

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: Sage

Last Name: Driskell

Mailing Address: 6720 Sweetwater Dr

City: Plano

Country: United States

State or Province: TX

ZIP/Postal Code: 75023

Email Address:

Organization Name:

Comment: Please do not restrict the ability of users to modify software in their radio hardware. Businesses as well as individuals depend on secure wireless communications which depend on suitable hardware as well as suitable software on said hardware.

Plenty of manufacturers develop hardware but do not develop decent software or will abandon it as soon as possible. I personally have had to use alternative firmware on multiple WiFi cards and routers due to the manufacturer not caring enough to fix gaping security holes or to patch critical bugs. Legitimate businesses and users will suffer the most from these restrictions since they will either have to depend on manufacturers to properly patch the drivers or else they will have to constantly upgrade when a simple patch to the drivers would have sufficed. Open source drivers help to offload the work from manufacturers while allowing users to have updated and secure drivers. Open source drivers also allow more knowledgeable people to audit code for the driver or firmware.

Open source technologies are able to breathe new life into old devices and hardware and make them able to be useful rather than rotting away in a landfill. These restrictions would make people unable to patch broken firmware on an otherwise good router, to patch broken networking drivers on an otherwise functional laptop, or to remove a bloated, insecure firmware and replace it with something updated and functional on an Android device.

These restrictions will do virtually nothing in the long run to stop illegitimate radio usage. They'll at most be a minor hindrance since cheap radios can just be sourced from outside the US and smuggled or shipped in. Customs may catch some, but will never catch them all. While doing something would be better than nothing if these measures only affected illegitimate usage; this will overwhelmingly negatively affect legitimate users and be at most a minor hindrance to the groups of people this measure seeks to stop.

Please do not restrict the ability of users to modify software in their radio hardware. Businesses as well as individuals depend on secure wireless communications which depend on suitable hardware as well as suitable software on said hardware.

Plenty of manufacturers develop hardware but do not develop decent software or will abandon it as soon as possible. I personally have had to use alternative firmware on multiple WiFi cards and routers due to the manufacturer not caring enough to fix gaping security holes or to patch critical bugs. Legitimate businesses and users will suffer the most from these restrictions since they will either have to depend on manufacturers to properly patch the drivers or else they will have to constantly upgrade when a simple patch to the drivers would have sufficed. Open source drivers help to offload the work from manufacturers while allowing users to have updated and secure drivers. Open source drivers also allow more knowledgeable people to audit code for the driver or firmware.

Open source technologies are able to breathe new life into old devices and hardware and make them able to be useful rather than rotting away in a landfill. These restrictions would make people unable to patch broken firmware on an otherwise good router, to patch broken networking drivers on an otherwise functional laptop, or to remove a bloated, insecure firmware and replace it with something updated and functional on an Android device.

These restrictions will do virtually nothing in the long run to stop illegitimate radio usage. They'll at most be a minor hindrance since cheap radios can just be sourced from outside the US and smuggled or shipped in. Customs may catch some, but will never catch them all. While doing something would be better than nothing if these measures only affected illegitimate usage; this will overwhelmingly negatively affect legitimate users and be at most a minor hindrance to the groups of people this measure seeks to stop.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ryan

Last Name: Morency

Mailing Address: 703 Hartz Ct

City: Le Claire

Country: United States

State or Province: IA

ZIP/Postal Code: 52753

Email Address:

Organization Name:

Comment: Preventing end users from modifying the firmware of their home routers should not be something the FCC should be meddling with. The companies which produce routers are notorious for releasing firmware with numerous security flaws, and denying the end user the ability to modify something they have purchased, which is THEIRS, will only create more security problems for the end user and consumers in general. Does the FCC really want to be held responsible when consumers have their personal information stolen due to faulty router firmware, and the inability of the end user to protect their private information by using a more secure third-party firmware? More importantly, does the FCC want to be seen as yet another government organization which has too much authority and should receive less funding? These are important points which need to be considered. The majority of Americans are fed up with big government intervention, and taking away the freedom to put your own firmware on your own router is going to be a PR nightmare for an organization which is already treading a very thin line when it comes to public opinion. Give the people the freedom they deserve. Being a bureaucratic authoritarian, and restricting what people can do with their own property will only reinforced the belief that government is the problem. Make the right choice. Say NO to this proposal.

Preventing end users from modifying the firmware of their home routers should not be something the FCC should be meddling with. The companies which produce routers are notorious for releasing firmware with numerous security flaws, and denying the end user the ability to modify something they have purchased, which is THEIRS, will only create more security problems for the end user and consumers in general. Does the FCC really want to be held responsible when consumers have their personal information stolen due to faulty router firmware, and the inability of the end user to protect their private information by using a more secure third-party firmware? More importantly, does the FCC want to be seen as yet another government organization which has too much authority and should receive less funding? These are important points which need to be considered. The majority of Americans are fed up with big government intervention, and taking away the freedom to put your own firmware on your own router is going to be a PR nightmare for an organization which is already treading a very thin line when it comes to public opinion. Give the people the freedom they deserve. Being a bureaucratic authoritarian, and restricting what people can do with their own property will only reinforced the belief that government is the problem. Make the right choice. Say NO to this proposal.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Justin

Last Name: Bilyj

Mailing Address: 1171 Virginia Ave

City: Lakewood

Country: United States

State or Province: OH

ZIP/Postal Code: 44107

Email Address:

Organization Name:

Comment: I am against this proposed rule, and will only enforce monopolies while putting down competition.

Just say no to fascism...

I am against this proposed rule, and will only enforce monopolies while putting down competition.

Just say no to fascism...

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: Nathan

Last Name: Kryger

Mailing Address: PO Box 1547

City: Snoqualmie

Country: United States

State or Province: WA

ZIP/Postal Code: 98065

Email Address: natex@yahoo.com

Organization Name:

Comment: I would like the FCC to please refrain from implementing rules that would prevent users from installing software of their choosing, including firmware, onto their computing devices including phones, wireless routers, and any other consumer computing device that uses radio. The currently proposed rules would completely inhibit the development of innovative new technologies as well as create potential security risks by not allowing users to correct faulty or insecure software on their own devices by themselves.

I would like the FCC to please refrain from implementing rules that would prevent users from installing software of their choosing, including firmware, onto their computing devices including phones, wireless routers, and any other consumer computing device that uses radio. The currently proposed rules would completely inhibit the development of innovative new technologies as well as create potential security risks by not allowing users to correct faulty or insecure software on their own devices by themselves.

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: Mogenson

Mailing Address: 18 Clary Street

City: Cambridge

Country: United States

State or Province: MA

ZIP/Postal Code: 02139

Email Address:

Organization Name:

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

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

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ross

Last Name: Whenmouth

Mailing Address: 116 Willowpark Road South

City: Hastings

Country: New Zealand

State or Province: Hawkes Bay

ZIP/Postal Code: 4122

Email Address:

Organization Name:

Comment: Statement of bias: I am the holder of a New Zealand amateur radio license, my callsign is ZL2WRW.

With respect to IEEE802.11 compatible "WiFi" part.15 radio equipment such as "wireless access points", preventing "unauthorised firmware modifications" such as the installation of "OpenWRT" and variants there of will greatly reduce the usefulness of said radio equipment [<http://wiki.openwrt.org/start>].

Indeed, the FCC's own "SamKnows" whiteboxes, which are used to survey broadband performance, utilise commodity part.15 WiFi radio equipment running modified firmware [<https://www.samknows.com/>]. Were these modifications actually authorised by the original device manufacturer?

The holders of amateur radio licenses are entitled to take part.15 devices and modify them for operation under part.97 - an example of this is the "flashing" of WiFi equipment with modified firmware for "High Speed Multimedia Mesh" networking. Two volunteer groups in the United States which are actively pursuing this are the "Broad Band Ham Net" group and the "Amateur Radio Emergency Data Network" group [<http://www.broadband-hamnet.org/>] [<http://www.aredn.org/>]. Preventing the modification of WiFi device firmware will hinder efforts to build a robust network which is available for use in an emergency when other communication networks have failed.

The manufacturers of part.15 WiFi equipment often stop releasing firmware updates a few short years after the device was sold. The problem is that many users keep using their "old" WiFi equipment for years after manufacturer support ends, and new security flaws in digital devices are constantly being discovered. Thus preventing firmware modification will prevent the patching of security flaws in devices that are no-longer supported by their manufacturer, increasing the risk of cybercrime. Generally speaking, OpenWRT and the like continue to provide "unauthorised" security updates for devices long after the original manufacturer has stopped supporting the product.

Most WiFi "access points" are actually miniature computers, typically running a variant of Linux or QNX. The freedom to modify the device firmware is effectively the same as the freedom to change the operating system on your PC. Indeed, if your PC has a WiFi adaptor, when you change the operating system on your PC, you are also changing the driver for the WiFi adaptor - typically this driver is what controls the operating frequency, TX power level and DFS (aka radar avoidance). For example, see the source code for the Atheros 9k series radio chip driver for Linux

[<https://github.com/torvalds/linux/tree/master/drivers/net/wireless/ath/ath9k>].

On the subject of radar and interference from 5 GHz part.15 devices, there is a lot to be said for replacing old-fashioned pulse radar with broadband "compressed pulse" radar [https://en.wikipedia.org/wiki/Pulse_compression]. With respect to "Homeland Security", if "flea power" WiFi equipment causes interference problems with radar equipment, I hate to think of the effect that deliberate high-power electronic counter measures from an adversary in wartime would have on those radars.

Thank you for your time.

Statement of bias: I am the holder of a New Zealand amateur radio license, my callsign is ZL2WRW.

With respect to IEEE802.11 compatible "WiFi" part.15 radio equipment such as "wireless access points", preventing "unauthorised firmware modifications" such as the installation of "OpenWRT" and variants there of will greatly reduce the usefulness of said radio equipment [<http://wiki.openwrt.org/start>].

Indeed, the FCC's own "SamKnows" whiteboxes, which are used to survey broadband performance, utilise commodity part.15 WiFi radio equipment running modified firmware [<https://www.samknows.com/>]. Were these modifications actually authorised by the original device manufacturer?

The holders of amateur radio licenses are entitled to take part.15 devices and modify them for operation under part.97 - an example of this is the "flashing" of WiFi equipment with modified firmware for "High Speed Multimedia Mesh" networking. Two volunteer groups in the United States which are actively pursuing this are the "Broad Band Ham Net" group and the "Amateur Radio Emergency Data Network" group [<http://www.broadband-hamnet.org/>] [<http://www.aredn.org/>]. Preventing the modification of WiFi device firmware will hinder efforts to build a robust network which is available for use in an emergency when other communication networks have failed.

The manufacturers of part.15 WiFi equipment often stop releasing firmware updates a few short years after the device was sold. The problem is that many users keep using their "old" WiFi equipment for years after manufacturer support ends, and new security flaws in digital devices are constantly being discovered. Thus preventing firmware modification will prevent the patching of security flaws in devices that are no-longer supported by their manufacturer, increasing the risk of cybercrime. Generally speaking, OpenWRT and the like continue to provide "unauthorised" security updates for devices long after the original manufacturer has stopped supporting the product.

Most WiFi "access points" are actually miniature computers, typically running a variant of Linux or QNX. The freedom to modify the device firmware is effectively the same as the freedom to change the operating system on your PC. Indeed, if your PC has a WiFi adaptor, when you change the operating system on your PC, you are also changing the driver for the WiFi adaptor - typically this driver is what controls the operating frequency, TX power level and DFS (aka radar avoidance). For example, see the source code for the Atheros 9k series radio chip driver for Linux [<https://github.com/torvalds/linux/tree/master/drivers/net/wireless/ath/ath9k>].

On the subject of radar and interference from 5 GHz part.15 devices, there is a lot to be said for replacing old-fashioned pulse radar with broadband "compressed pulse" radar [https://en.wikipedia.org/wiki/Pulse_compression]. With respect to "Homeland Security", if "flea power" WiFi equipment causes interference problems with radar equipment, I hate to think of the effect that deliberate high-power electronic counter measures from an adversary in wartime would have on

those radars.

Thank you for your time.

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: Emiel

Last Name: Kosse

Mailing Address: Langewijk 27

City: Dedemsvaart

Country: Netherlands

State or Province: Overijssel

ZIP/Postal Code: 7701AA NL

Email Address: emielkosse@hotmail.com

Organization Name:

Comment: Dear Sir/Madam,

Please do not implement rules that take away the ability of users to install costum firmware/software on their electronics computer devices.

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

Americans and individuals around the world 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.

Dear Sir/Madam,

Please do not implement rules that take away the ability of users to install costum firmware/software on their electronics computer devices.

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

Americans and individuals around the world 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: Sergey

Last Name: Yaglov

Mailing Address: Molodezhnaya st, 19-47

City: Chekhov

Country: Russia

State or Province: Moscow region

ZIP/Postal Code: 142300

Email Address: sergey@yaglov.ru

Organization Name:

Comment: it is not necessary to limit the progress that occurs naturally

#SaveWifi

it is not necessary to limit the progress that occurs naturally

#SaveWifi

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: Stanislav

Last Name: Panasik

Mailing Address: Obkhodnoi 2, 36

City: Orenburg

Country: Russia

State or Province: Orenburg

ZIP/Postal Code: 460004

Email Address: spanasik@gmail.com

Organization Name:

Comment: Hello,

I think this document is a bullshit.

Best regards

Hello,

I think this document is a bullshit.

Best regards

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Serena

Last Name: Cummings

Mailing Address: 19296 hwy 170

City: westfork

Country: United States

State or Province: AR

ZIP/Postal Code: 72774

Email Address: serenaisaaceric@gmail.com

Organization Name:

Comment: Please do not pass this rule..I like to change things on what I buy...I want to be able to put better upgrades on my stuff then what will ever be offered...

Please do not pass this rule..I like to change things on what I buy...I want to be able to put better upgrades on my stuff then what will ever be offered...

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: Jamie

Last Name: Taylor

Mailing Address: Flat 12, Windsor Court

City: London

Country: United Kingdom

State or Province: London

ZIP/Postal Code: SW11 3LA

Email Address: jamieolivertaylor@gmail.com

Organization Name: null

Comment: I strongly object to this proposal on the grounds of user choice.

I strongly object to this proposal on the grounds of user choice.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Vladimir

Last Name: Smirnov

Mailing Address: Zeussingel 33

City: Almere

Country: Netherlands

State or Province: Almere

ZIP/Postal Code: 1363TM

Email Address: civil.over@gmail.com

Organization Name:

Comment: In my opinion, this rule will have negative impact on the IT sector all over the world.

Reasons behind this:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices. This will decrease security of the devices and networks, will make it easier for hackers to live in this world.
2. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. This rule will make it impossible to fix them legally
3. 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.
4. IT sector relay on installing custom OS on corporate notebooks, desktop PCs, etc. - this rule will force them to use what vendor installed, which will hurt all IT business sector.

In my opinion, this rule will have negative impact on the IT sector all over the world.

Reasons behind this:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices. This will decrease security of the devices and networks, will make it easier for hackers to live in this world.
2. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. This rule will make it impossible to fix them legally
3. 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.
4. IT sector relay on installing custom OS on corporate notebooks, desktop PCs, etc. - this rule will force them to use what vendor installed, which will hurt all IT business sector.

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: Wesley

Last Name: Deglise

Mailing Address: 8 place saint martin

City: metz

Country: France

State or Province: moselle

ZIP/Postal Code: 57000

Email Address:

Organization Name:

Comment: Hi,

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

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

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

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

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

Hi,

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

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

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

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

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

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: Mathew

Last Name: Myers

Mailing Address: 1020 south rova ct.

City: visalia

Country: United States

State or Province: CA

ZIP/Postal Code: 93277

Email Address: mathewcmymers@gmail.com

Organization Name:

Comment: This is a very bad idea.

This is a very bad idea.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: john

Last Name: culver

Mailing Address: 3524 n. labarre rd

City: metairie

Country: United States

State or Province: LA

ZIP/Postal Code: 70002

Email Address:

Organization Name:

Comment: To whom it may concern:

I am highly concerned that the FCC is proposing to ban the running of custom software on what is basically a computer system used as a home/office router. This would be a poor decision from a technical standpoint.

These "routers" are really just small computers, most of which run a customized version of an operating system called Linux? These customizations are created by the manufacturers with various features and capabilities in mind. What history has born out is that many of these *official* firmware installations are fraught with bugs, back doors, security holes and are lacking in features.

What these non-manufacturer generated software images bring to the table are new and exciting features and timely bug fixes and inventiveness that the manufacturers are unable or unwilling to provide as it perhaps doesn't fit with their business models.

Would the FCC care to create rules about what Operating system I should be running on my desktop or laptop computer? If the answer is no, why not? At its basic level, the router is no different than my desktop. It is a computer that runs software. I can install Linux on my router and I can install Linux on my desktop. I can even configure my desktop to function as a router. Then would the FCC then decide what software I could run on my desktop?

To whom it may concern:

I am highly concerned that the FCC is proposing to ban the running of custom software on what is basically a computer system used as a home/office router. This would be a poor decision from a technical standpoint.

These "routers" are really just small computers, most of which run a customized version of an operating system called Linux? These customizations are created by the manufacturers with various features and capabilities in mind. What history has born out is that many of these *official* firmware installations are fraught with bugs, back doors, security holes and are lacking in features.

What these non-manufacturer generated software images bring to the table are new and exciting features and timely bug fixes and inventiveness that the manufacturers are unable or unwilling to provide as it perhaps doesn't fit with their business models.

Would the FCC care to create rules about what Operating system I should be running on my desktop or laptop computer? If the answer is no, why not? At its basic level, the router is no different than my desktop. It is a computer that runs software. I can install Linux on my router and I can install Linux on my desktop. I can even configure my desktop to function as a router. Then would the FCC then decide what software I could run on my desktop?

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: Gavin

Last Name: Li

Mailing Address: 2520 Channing Way

City: Berkeley

Country: United States

State or Province: CA

ZIP/Postal Code: 94720

Email Address:

Organization Name:

Comment: Please revise provision 2.1033 by removing the ban on third-party modifications to wireless devices operating in the 5 GHz band. The ability of third-parties (particularly hobbyists) to modify the operation of wireless devices spurs innovation and is often a learning opportunity for many curious individuals. Banning modification (and consequently inspection) of these devices might actually work to harm the security of these devices; many products that have been historically locked-down have been "hacked" due to security vulnerabilities which may have been found and mitigated if the firmware were open source.

Please revise provision 2.1033 by removing the ban on third-party modifications to wireless devices operating in the 5 GHz band. The ability of third-parties (particularly hobbyists) to modify the operation of wireless devices spurs innovation and is often a learning opportunity for many curious individuals. Banning modification (and consequently inspection) of these devices might actually work to harm the security of these devices; many products that have been historically locked-down have been "hacked" due to security vulnerabilities which may have been found and mitigated if the firmware were open source.

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: Oleg

Last Name: Shevchenko

Mailing Address: Peremohy Ave. 78a

City: Kharkiv

Country: Ukraine

State or Province: Kharkivska

ZIP/Postal Code: 61000

Email Address: sheva-gitara@mail.ru

Organization Name:

Comment: It's unfair to the user! When I bought this gadget, I should have the right to do with it whatever I want. Replace firmware to the other so as to have the right to choose an operating system other than Windows. Or then it is necessary to prohibit the use of all GNU/Linux systems, or other consolidated software?

It's unfair to the user! When I bought this gadget, I should have the right to do with it whatever I want. Replace firmware to the other so as to have the right to choose an operating system other than Windows. Or then it is necessary to prohibit the use of all GNU/Linux systems, or other consolidated software?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Parker

Last Name: Richardson

Mailing Address: 104 Lake Reba Dr.

City: Richmond

Country: United States

State or Province: KY

ZIP/Postal Code: 40475

Email Address:

Organization Name:

Comment: As a citizen of the United States, I am formally requesting that you not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I request this because 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. Additionally, billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I hope that you will take this into consideration when making your decision. Freedom of choice when it comes to software, firmware, and hardware, are core values that would have been considered by the founding fathers, had the technology existed at the time. Considering their view on freedom, I think they would be opposed to restricting the choices of citizens, as you should.

Thank you for taking the time to read this.

As a citizen of the United States, I am formally requesting that you not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I request this because 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. Additionally, billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I hope that you will take this into consideration when making your decision. Freedom of choice when it comes to software, firmware, and hardware, are core values that would have been considered by the founding fathers, had the technology existed at the time. Considering their view on freedom, I think they would be opposed to restricting the choices of citizens, as you should.

Thank you for taking the time to read this.

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: Moses

Mailing Address: 7064 Cottontail St.

City: Ventura

Country: United States

State or Province: CA

ZIP/Postal Code: 93003

Email Address: james.moses@navy.mil

Organization Name:

Comment:

FCC,

With respect to your proposed rulemaking, I have the following feedback:

1. I do not trust government meddling of large companies (like Cisco or Linksys). I believe that consumers have a right to be able to replace proprietary firmware with Open source, open reviewed firmware.
2. As an Electrical Engineer, I desire the right to be able to program radio wifi equipment WITHOUT government restrictions. You should regulate power/transmit freqs/geolocations of transmissions, but not what I propose to do in a lab environment.
3. Proposed rulemaking stifles innovation and education.

FCC,

With respect to your proposed rulemaking, I have the following feedback:

1. I do not trust government meddling of large companies (like Cisco or Linksys). I believe that consumers have a right to be able to replace proprietary firmware with Open source, open reviewed firmware.
2. As an Electrical Engineer, I desire the right to be able to program radio wifi equipment WITHOUT government restrictions. You should regulate power/transmit freqs/geolocations of transmissions, but not what I propose to do in a lab environment.
3. Proposed rulemaking stifles innovation and education.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Scott

Last Name: Reece

Mailing Address: 1347 S. Owl Dr.

City: Gilbert

Country: United States

State or Province: AZ

ZIP/Postal Code: 85296

Email Address:

Organization Name:

Comment: I think this legislation would be a huge blow to innovation in our nation, and I think it should be stopped. People should have the right and ability to modify their equipment, both hardware and software, as long as they're not breaking the FCC rules.

Thank you for your time.

I think this legislation would be a huge blow to innovation in our nation, and I think it should be stopped. People should have the right and ability to modify their equipment, both hardware and software, as long as they're not breaking the FCC rules.

Thank you for your time.

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: zachary

Last Name: luft

Mailing Address: 2825 w porter ct.

City: visalia

Country: United States

State or Province: CA

ZIP/Postal Code: 93291

Email Address:

Organization Name:

Comment: Restricting the flashing of firmware is insane. It should be at the discretion of the maker to allow or disallow flashing of firmware.

Restricting the flashing of firmware is insane. It should be at the discretion of the maker to allow or disallow flashing of firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Douglas

Last Name: Wilson

Mailing Address: 652 Scronce Creek Rd

City: Burnsville

Country: United States

State or Province: NC

ZIP/Postal Code: 28714

Email Address: dbreezew@gmail.com

Organization Name: United States Citizenry

Comment: Dear Sirs,

Please reconsider this effort to lock out hobbyist and open systems enthusiasts. Probably one of the best sources available to those voting on this decision would be the technology blog website Slashdot:

<http://tech.slashdot.org/story/15/09/02/1513259/new-fcc-rules-could-ban-wifi-router-firmware-modification>

Here are a few snippets of the arguments already posted to this forum concerning this issue:

"I was just thinking that. This is so broad as to be unusable.

And mature products like DD-WRT are what make consumer-grade routers fly. It's pretty much the only reason I'll buy an ASUS, because the stock firmware doesn't have the feature set needed for latency sensitive hardware."

"Based on 18 years of professional experience in network security, in both the private sector and government, the proposed rule causes significant concern for information security posture. There are three primary reasons. The legitimate goals of the FCC could be achieved in an alternate manner which does not cause the same widespread security vulnerabilities, by instead requiring that output power levels and any other critical parameters be limited to legal levels by a separate chip. This approach would be far superior to effectively banning proper security practice for the ENTIRE operating system and all utilities on the device, as the current proposal does."

"Yes, this is the answer. If commodity Wifi routers become lock boxes, make non-commodity non-firmware Wifi routers. The more you tighten your grip, FCC, the more general-purpose computing systems will slip through your fingers."

And, there is much more to be considered available at the above linked forum page. I personally just want government agencies to refrain from locking out individual freedom and choice as much as possible. When lack of regulation on usage of FCC governed equipment becomes a noticeable problem then there may be need for action. I've been in the technology industry for 30+ years and have yet to encounter a problem that these proposed restrictions would address. It is, however, readily apparent that these rules would be of benefit to large-scale manufacturers in stifling "open systems" competition and forcing consumers into purchases that otherwise wouldn't be required. Don't force us to "follow the money" to see who's really driving this proposal.

Dear Sirs,

Please reconsider this effort to lock out hobbyist and open systems enthusiasts. Probably one of the best sources available to those voting on this decision would be the technology blog website Slashdot:

<http://tech.slashdot.org/story/15/09/02/1513259/new-fcc-rules-could-ban-wifi-router-firmware-modification>

Here are a few snippets of the arguments already posted to this forum concerning this issue:

"I was just thinking that. This is so broad as to be unusable.

And mature products like DD-WRT are what make consumer-grade routers fly. It's pretty much the only reason I'll buy an ASUS, because the stock firmware doesn't have the feature set needed for latency sensitive hardware."

"Based on 18 years of professional experience in network security, in both the private sector and government, the proposed rule causes significant concern for information security posture. There are three primary reasons. The legitimate goals of the FCC could be achieved in an alternate manner which does not cause the same widespread security vulnerabilities, by instead requiring that output power levels and any other critical parameters be limited to legal levels by a separate chip. This approach would be far superior to effectively banning proper security practice for the ENTIRE operating system and all utilities on the device, as the current proposal does."

"Yes, this is the answer. If commodity Wifi routers become lock boxes, make non-commodity non-firmware Wifi routers. The more you tighten your grip, FCC, the more general-purpose computing systems will slip through your fingers."

And, there is much more to be considered available at the above linked forum page. I personally just want government agencies to refrain from locking out individual freedom and choice as much as possible. When lack of regulation on usage of FCC governed equipment becomes a noticeable problem then there may be need for action. I've been in the technology industry for 30+ years and have yet to encounter a problem that these proposed restrictions would address. It is, however, readily apparent that these rules would be of benefit to large-scale manufacturers in stifling "open systems" competition and forcing consumers into purchases that otherwise wouldn't be required. Don't force us to "follow the money" to see who's really driving this proposal.

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: Ashley

Mailing Address: 1173 Hester Ave

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95126

Email Address: Daniel.r.ashley@gmail.com

Organization Name: pro open source

Comment: This is anti-Open Source. As a network engineer, I need to experiment on experimental and/or edge case platforms. This type of proposed law is no different than HP breaking someone down through legal fees for edging into the ink cartridge market.

If this proposed law is passed, I will break it. Openly. Fuck you FCC for even going there.

Daniel Ashley

This is anti-Open Source. As a network engineer, I need to experiment on experimental and/or edge case platforms. This type of proposed law is no different than HP breaking someone down through legal fees for edging into the ink cartridge market.

If this proposed law is passed, I will break it. Openly. Fuck you FCC for even going there.

Daniel Ashley

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: Longenecker

Mailing Address: 41 Laurel Hill

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78737

Email Address: david@securityforrealpeople.com

Organization Name: www.securityforrealpeople.com

Comment: The rules proposed by the FCC could have significant unintended consequences for end users and security researchers.

For the most part, the proposed rules do make sense - but with a few significant caveats. Those caveats could lead to significant restrictions on what citizens can do with our devices. While we are a minority of consumers, there are a great many individuals like myself that enjoy tinkering with technology, configuring devices to work together in novel ways, and customizing products to suit our tastes.

Equally important, there are a smaller number of people that, like me, investigate products for security flaws. In many cases, we experiment with products that we have purchased and use personally. When we find something that could be abused by a malicious actor, we often come up with solutions and report our findings to the manufacturer. Our "hacking" leads to security fixes that benefit millions of consumers using the same devices.

Much of this could be impossible if interpretation of the rules leads to manufacturers blocking access to device firmware and software.

More detailed comments are attached, as well as published at <http://www.securityforrealpeople.com/2015/09/comments-on-proposed-fcc-rules.html>

The rules proposed by the FCC could have significant unintended consequences for end users and security researchers.

For the most part, the proposed rules do make sense - but with a few significant caveats. Those caveats could lead to significant restrictions on what citizens can do with our devices. While we are a minority of consumers, there are a great many individuals like myself that enjoy tinkering with technology, configuring devices to work together in novel ways, and customizing products to suit our tastes.

Equally important, there are a smaller number of people that, like me, investigate products for security flaws. In many cases, we experiment with products that we have purchased and use personally. When we find something that could be abused by a malicious actor, we often come up with solutions and report our findings to the manufacturer. Our "hacking" leads to security fixes that benefit millions of consumers using the same devices.

Much of this could be impossible if interpretation of the rules leads to manufacturers blocking access to device firmware and software.

More detailed comments are attached, as well as published at <http://www.securityforrealpeople.com/2015/09/comments-on-proposed-fcc-rules.html>

The rules proposed by the FCC for regulating RF-emitting devices could have significant unintended consequences for end users and security researchers. For the most part, the proposed rules do make sense - but with a few significant caveats.

Those caveats could lead to significant restrictions on what we as citizens can do with our devices. While we are a minority of consumers, there are a great many individuals like myself that enjoy tinkering with technology, configuring devices to work together in novel ways, and customizing products to suit our tastes. If you've ever seen a Christmas display where the lights are set to music, you've seen our tinkering at work.

Equally important, there are a smaller number of people that, like me, investigate products for security flaws. In many cases, we experiment with products that we have purchased and use personally. When we find something that could be abused by a malicious actor, we often come up with solutions and report our findings to the manufacturer. Our "hacking" leads to security fixes that benefit millions of consumers using the same devices.

A few examples from my own work follow. These are security issues fixed, and highly useful configuration tweaks, that could be impossible if the device software were locked down in accordance with the proposed rules.

A configuration error on ASUS servers prevented all ASUS wireless routers worldwide from recognizing that a critical security update was available. <http://www.securityforrealpeople.com/2014/02/breaking-down-asus-router-bug.html>

CVE-2014-2719: Certain wireless routers disclosed the administrator password in such a way that the password could be stolen and used to access the device without authorization. <http://www.securityforrealpeople.com/CVE-2014-2719>

CVE-2014-2718: Certain wireless routers did not properly verify that an automatically-downloaded update was genuine. An attacker could supply a malicious update, which the router would install, potentially granting the attacker complete control over the network. <http://www.securityforrealpeople.com/CVE-2014-2719>

A networked device provided a way to share a storage drive with users of the network, but with very limited functionality. I wrote a script that greatly enhanced the functionality. <http://www.securityforrealpeople.com/2014/12/customizing-samba-on-asuswrt-wireless.html>

CVE-2014-9584: Discovered by another researcher, this flaw allowed an attacker with access to the local network, to take full control of the network router. <http://www.securityforrealpeople.com/2015/01/asus-bug-lets-those-on-your-local.html>

I demonstrated a project using a wireless router, and a Raspberry Pi running snort, to monitor network traffic and alert the owner to potential malicious or undesirable network behavior. <http://www.securityforrealpeople.com/snort-dns>

These are just a few examples of my own work; there are many others like myself, that have similar examples.

Below are what I consider to be the most important parts of the proposed rules.

13. Updating Certification Procedures

...manufacturers are increasingly designing transmitters that use software to set the operating parameters. Such RF-controlling software can allow adjustment of individual parameters or enable a device to operate in different modes, and the manufacturer may provide software upgrades in the field to enable new capabilities. We need to be assured that such devices only operate consistent with their certification. Also, software may be designed to only be modified by the grantee of certification or may be designed to permit third parties to enable new functions or frequency bands. Such trends are testing the limits of the Commission's existing certification rules, and formed the basis for the NPRM's proposals.

>>This is the foundation for the following sections. On the surface it sounds reasonable. The FCC is charged with regulating radio bands; to do so, they need assurance that a device will not behave differently in operation than when

tested. A few paragraphs later though is the central problem

18. Devices with Software-Based Capabilities

The SDR rules were intended to allow manufacturers to obtain approval for changes to the RF operating parameters of a radio resulting from software changes without the need to physically re-label a device with a new FCC ID number in the field. For a device to be certified as an SDR, in addition to demonstrating that the device complies with the applicable technical requirements, the applicant must also demonstrate that the device contains security features to prevent the loading of software that would allow the radio to operate in violation of the Commission's rules. The applicant generally has the option of whether to declare a device an SDR. Once the grantee of a device that is classified as an SDR makes any hardware modifications that require approval, the rules do not permit any subsequent software changes absent the filing of an application to obtain a new FCC ID.

>>In theory a manufacturer can "prevent the loading of software that would allow the radio to operate in violation of the Commission's rules" while still permitting an end user to load custom firmware. It is entirely possible to separate radio control firmware from device operating software. Using a WiFi router as an example, the software to route network packets, or to encrypt wireless transmissions, or to impose firewall protections, can be separated from the firmware that operates the actual radio transmissions.

>>In practice, few manufacturers have proven willing to separate the functions. It is far more likely that manufacturers will chose the easier route of locking down firmware to only the manufacturer's own programs, thus putting an end to the sort of novel inventions and security improvements I described earlier.

38-39. Modification of Certified Equipment by Third Parties

The Commission proposed to eliminate exceptions to the principle that certified devices could not be modified by third parties unless the third party receives its own certification. It proposed to revise § 2.909(d), which allows a new party that performs device modifications without the consent of the original grantee to become responsible for the compliance by labeling the device with a statement indicating it was modified, with the requirement that the party obtain a new grant of certification. It would have to specify a new FCC ID unless the consent of the original is obtained. The Commission asked whether the new procedure should also apply to parties that currently market devices with modified certification labels.

The Commission proposed, for certified device operating under all rule parts, to require that any party making changes without the authorization of the original grantee of certification must obtain a new grant of certification and a new FCC ID. This would codify a uniform application process for instances where parties other than the original grantee wish to make changes to certified devices, and would remove the current distinctions in § 2.1043(d) and (f) of the rules.

>>Does this mean an end user making software changes is obligated to seek certification himself or herself? What constitutes "modified" in the context of this rule?

74. Devices Imported for Personal UseThe Commission proposed to expand its exception on devices imported for personal use by modifying its existing personal use exception for up to three devices to encompass devices that use both licensed and unlicensed frequencies. It asked if there are targeted exceptions within the Commission's existing rules that should also be updated or removed. It asked whether the three-device limit is still appropriate, and if a different limit would provide adequate protection against harmful interference without unduly restricting individuals' personal use importation.

>>An exemption for personal use could potentially alleviate the earlier concerns, if broadened considerably. A technology-savvy household could easily include two or three wireless routers; four or more cell phones; multiple mobile computers and laptops; a wireless television; a wireless video player; one or more game consoles; and a wireless thermostat. It is not unreasonable that a household might include a wireless refrigerator, laundry appliances, door locks, and alarm system.

>>To be meaningful, an exemption for personal use would have to allow for dozens of 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: Jacob

Last Name: Rasiel

Mailing Address: 225 River Street apt 2403

City: Hoboken

Country: United States

State or Province: NJ

ZIP/Postal Code: 07030

Email Address: JSR694@mac.com

Organization Name:

Comment: Hello,

I am writing in protest of the Equipment Authorization and Electronic Labeling for Wireless Devices Rule currently being proposed by the FCC. I hold dear my right to modify within reasonable limitations the functionality of wireless network hardware which I own. I also understand the intent of the FCC to protect consumers and infrastructure from the abuse of radio equipment... However the current proposal goes too far. It threatens to snuff out a vibrant community of wireless network developers and tinkerers, the loss of which would be a great blow to wireless network security. For furtger reasons why I disagree with the proposed rule, I include below objections raised by the SaveWifi campaign:

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.

Thanks for your consideration.

Hello,

I am writing in protest of the Equipment Authorization and Electronic Labeling for Wireless Devices Rule currently being proposed by the FCC. I hold dear my right to modify within reasonable limitations the functionality of wireless network hardware which I own. I also understand the intent of the FCC to protect consumers and infrastructure from the abuse of radio equipment... However the current proposal goes too far. It threatens to snuff out a vibrant community of wireless network developers and tinkerers, the loss of which would be a great blow to wireless network security. For furtger reasons why I disagree with the proposed rule, I include below objections raised by the SaveWifi campaign:

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.

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: Nathaniel

Last Name: DeSimone

Mailing Address: 6242 NW 159Th Pl

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97229

Email Address: nateman1352@gmail.com

Organization Name:

Comment: This new regulation could potentially ban the use, creation and distribution of alternative open source firmware for consumer WiFi routers. Examples of potentially impacted projects include www.dd-wrt.com and www.polarcloud.com/tomato

These projects give the technically inclined computer user the ability add capabilities to WiFi routers that were not originally provided by the manufacturer. In some cases, they also make the routers more robust and able to operate for longer periods of time without being reset. Generally, they do not modify the actual WiFi radio's RF parameters in any way, they only modify the networking software.

I recommend that the regulation be modified to allow these firmware projects to continue to be used, created, and distributed as long as they use the exact same radio RF parameters as the original firmware which the device was certified with.

This new regulation could potentially ban the use, creation and distribution of alternative open source firmware for consumer WiFi routers. Examples of potentially impacted projects include www.dd-wrt.com and www.polarcloud.com/tomato

These projects give the technically inclined computer user the ability add capabilities to WiFi routers that were not originally provided by the manufacturer. In some cases, they also make the routers more robust and able to operate for longer periods of time without being reset. Generally, they do not modify the actual WiFi radio's RF parameters in any way, they only modify the networking software.

I recommend that the regulation be modified to allow these firmware projects to continue to be used, created, and distributed as long as they use the exact same radio RF parameters as the original firmware which the device was certified with.

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: George V.

Last Name: Reilly

Mailing Address: 4322 13th Ave S

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98108

Email Address: george@reilly.org

Organization Name:

Comment: As a professional software developer and an open source advocate, I know the importance of the freedom to experiment and the freedom to modify software. The proposed legislation goes too far.

As a professional software developer and an open source advocate, I know the importance of the freedom to experiment and the freedom to modify software. The proposed legislation goes too far.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Steven

Last Name: Dubnoff

Mailing Address: 1712 Lakeside Ave. S.

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98144

Email Address: sdubnoff@circlesys.com

Organization Name: Circle Systems

Comment: This is a really bad idea, that will restrict innovation and prohibit the installation of proven firmware such as dd-wrt on routers. This firmware, I have found, is clearly superior to that which is shipped by the manufacturer.

This is a really bad idea, that will restrict innovation and prohibit the installation of proven firmware such as dd-wrt on routers. This firmware, I have found, is clearly superior to that which is shipped by 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: Robert

Last Name: Taylor

Mailing Address: 304 NW Wade St

City: Estacada

Country: United States

State or Province: OR

ZIP/Postal Code: 97023

Email Address: mscompuserv@gmail.com

Organization Name:

Comment: As consumers, we have the right to our own private property. If I procure a wireless devices such as a WiFi router; I then ought to be able to have control over that property--with in the bounds of the law of course. I have a dual band 2.4 and 5.8 Ghz router with an open source firmware from Tomato Shibby. The software is a GNU free and open source firmware with the source code available to the public. This firmware utilizes and open source driver for the Atheros baseband for both radios. This driver was written so that I could install additional functionality on my router and still use it for WiFi purposes. Implementing this rule change will force manufactures to lock down the baseband with a property driver thus blocking support for open source software. Not to mention, this will drive up the cost of manufacturing. Companies like Cisco, Netgear and so on will be forced to pay for additional patent licensing and prolong development of new products. This rule change is nothing but a big loss for everybody. The FCC can still maintain authority over the proper use of the 5.8 Ghz band. These rules can be posted and enforced on the respective domains of various open source firmware home pages. I would rather see a cease and deist for improper band usage by the FCC versus an outright ban on open source router firmware.

As consumers, we have the right to our own private property. If I procure a wireless devices such as a WiFi router; I then ought to be able to have control over that property--with in the bounds of the law of course. I have a dual band 2.4 and 5.8 Ghz router with an open source firmware from Tomato Shibby. The software is a GNU free and open source firmware with the source code available to the public. This firmware utilizes and open source driver for the Atheros baseband for both radios. This driver was written so that I could install additional functionality on my router and still use it for WiFi purposes. Implementing this rule change will force manufactures to lock down the baseband with a property driver thus blocking support for open source software. Not to mention, this will drive up the cost of manufacturing. Companies like Cisco, Netgear and so on will be forced to pay for additional patent licensing and prolong development of new products. This rule change is nothing but a big loss for everybody. The FCC can still maintain authority over the proper use of the 5.8 Ghz band. These rules can be posted and enforced on the respective domains of various open source firmware home pages. I would rather see a cease and deist for improper band usage by the FCC versus an outright ban on open source router firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ben

Last Name: Griffith

Mailing Address: 7098 N Marais Dr

City: Coeur d Alene

Country: United States

State or Province: ID

ZIP/Postal Code: 83815-0436

Email Address:

Organization Name:

Comment: I respectfully ask the FCC to not implement rules that take away the ability of users/consumers to install the software of their choosing on their computing devices. Specifically, do not restrict the ability to install custom firmware into wireless routers. As a consumer, I feel that I should have the right to alter the equipment that I have purchased. If the equipment is insecure, or not performing optimally, or abandoned by the manufacturer, I should be able to upgrade/patch/flash the device in order to make it work better and continue to be useful to me. Furthermore, wireless networking research depends on the ability of researchers to investigate and modify their devices. Taking away their ability to legally conduct research will stifle innovation and leave consumers unaware of potential problems or enhancements to their equipment that could be fixed/applied. Not to mention the security of the device. Many devices are sold and used in homes/small businesses for years - but the manufacturers move on and do not continue to develop or support these older devices. Having the ability to upgrade their firmware makes them more secure and longer lasting. This proposed rule is unnecessary and overreaching. Please do not take away people's choice.

I respectfully ask the FCC to not implement rules that take away the ability of users/consumers to install the software of their choosing on their computing devices. Specifically, do not restrict the ability to install custom firmware into wireless routers. As a consumer, I feel that I should have the right to alter the equipment that I have purchased. If the equipment is insecure, or not performing optimally, or abandoned by the manufacturer, I should be able to upgrade/patch/flash the device in order to make it work better and continue to be useful to me. Furthermore, wireless networking research depends on the ability of researchers to investigate and modify their devices. Taking away their ability to legally conduct research will stifle innovation and leave consumers unaware of potential problems or enhancements to their equipment that could be fixed/applied. Not to mention the security of the device. Many devices are sold and used in homes/small businesses for years - but the manufacturers move on and do not continue to develop or support these older devices. Having the ability to upgrade their firmware makes them more secure and longer lasting. This proposed rule is unnecessary and overreaching. Please do not take away people's choice.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Mallia

Mailing Address: 12431 Cotton Creek

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78253

Email Address:

Organization Name:

Comment: No... The spectrum belongs to the world and let us run custom firmware on "our" devices... Otherwise it will happen with or without FCC support. My router, my freqs!

No... The spectrum belongs to the world and let us run custom firmware on "our" devices... Otherwise it will happen with or without FCC support. My router, my freqs!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Wong

Mailing Address: 8124 Spring Valley Ln

City: Plano

Country: United States

State or Province: TX

ZIP/Postal Code: 75025

Email Address: rwong@alumni.rice.edu

Organization Name: self

Comment: Please do not implement rules that prohibit users from installing software (of their own design) on their own computing devices. I believe this capability promotes advancement (and knowledge) in our American tech industry, because average users (like myself) can learn how things work, which can lead to inevitable improvements. There is a large community of technically-inclined users who are interested in experimenting with new features added to customized software. Many of these features are not supported by the commercial industries. Commercial products are only interested in making money, not innovating (unless it can make more money).

I believe the DIY movement in this country has re-energized the US tech future, which is necessary if our country is to survive international competition in high-tech products. Already, countries like China (makers of our iPhones) is quickly advancing to technical parity with the US, especially through out-sourcing our technical manufacturing. We need to encourage our domestic young engineers and designers to engage in experimentation and innovation (more than other countries is doing for theirs).

I also agree with the following ideas:

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

Thanks for your attention.

Best Regards,

Robert Wong

Please do not implement rules that prohibit users from installing software (of their own design) on their own computing devices. I believe this capability promotes advancement (and knowledge) in our American tech industry, because average users (like myself) can learn how things work, which can lead to inevitable improvements. There is a large community of technically-inclined users who are interested in experimenting with new features added to customized software. Many of these features are not supported by the commercial industries. Commercial products are only

interested in making money, not innovating (unless it can make more money).

I believe the DIY movement in this country has re-energized the US tech future, which is necessary if our country is to survive international competition in high-tech products. Already, countries like China (makers of our iPhones) is quickly advancing to technical parity with the US, especially through out-sourcing our technical manufacturing. We need to encourage our domestic young engineers and designers to engage in experimentation and innovation (more than other countries is doing for theirs).

I also agree with the following ideas:

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

Thanks for your attention.

Best Regards,

Robert Wong

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kevin

Last Name: H

Mailing Address: Somewhere.

City: Not telling you.

Country: Zimbabwe

State or Province: 1234567890

ZIP/Postal Code: 1231231231

Email Address:

Organization Name:

Comment: Hello FCC,

The Equipment Authorization and Electronic Labelling for Wireless Devices proposal is completely infringing on the concepts of being able to audit the code for software the end users install, the ability for developers to improve on existing systems by means of independent research and not corporate interest-based software development. End users are buying into a world where our devices are being made based on the interests of corporate conglomerates instead of being able to develop for themselves technology made for the people, by the people.

I hope this reaction from people around the world within the United States and elsewhere will convince you not to forever change the future of free, independent software.

Hello FCC,

The Equipment Authorization and Electronic Labelling for Wireless Devices proposal is completely infringing on the concepts of being able to audit the code for software the end users install, the ability for developers to improve on existing systems by means of independent research and not corporate interest-based software development. End users are buying into a world where our devices are being made based on the interests of corporate conglomerates instead of being able to develop for themselves technology made for the people, by the people.

I hope this reaction from people around the world within the United States and elsewhere will convince you not to forever change the future of free, independent software.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Evan

Last Name: Sternberg

Mailing Address: 1241 Vassar Drive NE

City: Albuquerque

Country: United States

State or Province: NM

ZIP/Postal Code: 87106

Email Address:

Organization Name:

Comment: This is a horrible idea. Re law of unintended consequences, see

https://libreplanet.org/wiki/Save_WiFi/Individual_Comments

<http://hackaday.com/2015/08/31/fcc-introduces-rules-banning-wifi-router-firmware-modification/>

The freedom to tinker with something is valuable. Even if you do not agree with this concept, closed systems tend to become less secure than open systems. See Window PCs and CAN bus.

This is a bad idea.

This is a horrible idea. Re law of unintended consequences, see

https://libreplanet.org/wiki/Save_WiFi/Individual_Comments

<http://hackaday.com/2015/08/31/fcc-introduces-rules-banning-wifi-router-firmware-modification/>

The freedom to tinker with something is valuable. Even if you do not agree with this concept, closed systems tend to become less secure than open systems. See Window PCs and CAN bus.

This is a bad idea.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Boyle

Mailing Address: 6240 Welcome Home Dr

City: Columbia

Country: United States

State or Province: MD

ZIP/Postal Code: 21045

Email Address: n3lpt@canonic.net

Organization Name:

Comment: In the way that Amateur radio operators and hobbyists have done for years, modifying a device should not be made illegal.

The FCC is already authorized to sanction those responsible for illegal RF emissions.

Easing the FCC's burden of enforcement should not come at the expense of the personal freedom create or modify one's possessions.

In the way that Amateur radio operators and hobbyists have done for years, modifying a device should not be made illegal.

The FCC is already authorized to sanction those responsible for illegal RF emissions.

Easing the FCC's burden of enforcement should not come at the expense of the personal freedom create or modify one's possessions.

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: Jo3

Last Name: McCarthy

Mailing Address: 316 Lugonis St

City: Newport Beach

Country: United States

State or Province: CA

ZIP/Postal Code: 92663

Email Address: jo3@brats.com

Organization Name: null

Comment: I am a Computer Scientist. I have worked at companies developing these very devices. I have developed code that actually runs in millions of these devices. However, I and all of my colleagues are only human. We will not get everything right the first time -- that is impossible. We do not design the devices to be immutable. We design them with modification in mind. It is of vital importance that users be permitted to modify the equipment they own.

Changing rules to prohibit customers from exercising their freedom to modify their own equipment will have a profoundly deleterious effect on the progress of technological innovation in the wireless sphere. It is often through the efforts of private citizens working on their own equipment that the security and reliability of these devices are improved.

In this light, I urge you not to approve a rule change to prohibit the modification of wireless equipment.

I am a Computer Scientist. I have worked at companies developing these very devices. I have developed code that actually runs in millions of these devices. However, I and all of my colleagues are only human. We will not get everything right the first time -- that is impossible. We do not design the devices to be immutable. We design them with modification in mind. It is of vital importance that users be permitted to modify the equipment they own.

Changing rules to prohibit customers from exercising their freedom to modify their own equipment will have a profoundly deleterious effect on the progress of technological innovation in the wireless sphere. It is often through the efforts of private citizens working on their own equipment that the security and reliability of these devices are improved.

In this light, I urge you not to approve a rule change to prohibit the modification of wireless equipment.

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: GERARDO

Last Name: Espinoza

Mailing Address: Street 2, road 112

City: San Pablo

Country: Costa Rica

State or Province: Heredia

ZIP/Postal Code: 41900

Email Address: gerardo.espinoza@gmail.com

Organization Name: None

Comment: Hi. I am against this new act. I should be allowed to be able to modify my devise firmware as I like. I am the owner of the hardware once I have it, I should be free to change the software if the default version don't fulfill my needs or it gets unsupported.

Hi. I am against this new act. I should be allowed to be able to modify my devise firmware as I like. I am the owner of the hardware once I have it, I should be free to change the software if the default version don't fulfill my needs or it gets unsupported.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Anonymous

Mailing Address: S Chase Dr

City: Crown Point

Country: United States

State or Province: IN

ZIP/Postal Code: 46307

Email Address: null

Organization Name: null

Comment: Please don't force manufacturers to lockdown their firmware. This will kill off projects like OpenWrt which I regularly use to keep my router secure. Manufacturers of routers don't fix bugs or security issues. Most don't provide support after six months. These routers are going to be in service for years. Without projects like OpenWrt routers would have to be replaced every year or two because the manufacturer won't fix a security issue. That is a lot of waste.

Please don't force manufacturers to lockdown their firmware. This will kill off projects like OpenWrt which I regularly use to keep my router secure. Manufacturers of routers don't fix bugs or security issues. Most don't provide support after six months. These routers are going to be in service for years. Without projects like OpenWrt routers would have to be replaced every year or two because the manufacturer won't fix a security issue. That is a lot of waste.

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: Brenda

Last Name: Make

Mailing Address: 808 Gale Drive

City: Campbell

Country: United States

State or Province: CA

ZIP/Postal Code: 95008

Email Address: brendieellen@yahoo.com

Organization Name:

Comment: Please, do not needlessly restrict the modification of device communication software!

The proposed rule is bad legislation which dis-empowers people to use their devices.

The proposed also represents an anti-competitive legislation, that will stifles innovation.

Would our government also restrict the use of a hammer, or a washing machine, or tell us that our car cannot be painted blue?

Respectfully,

Brenda Make

Please, do not needlessly restrict the modification of device communication software!

The proposed rule is bad legislation which dis-empowers people to use their devices.

The proposed also represents an anti-competitive legislation, that will stifles innovation.

Would our government also restrict the use of a hammer, or a washing machine, or tell us that our car cannot be painted blue?

Respectfully,

Brenda Make

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: Don

Last Name: Quon, Jr.

Mailing Address: 44 Lynn Fells PKWY

City: Melrose

Country: United States

State or Province: MA

ZIP/Postal Code: 02176

Email Address:

Organization Name:

Comment: Restrictions on software or firmware modifications for consumer RF devices, mainly WiFi devices, would place a major hindrance on the consumers' experience and value for their devices. Some WiFi devices are severely limited out of the box due to poor and sub-standard firmware. Open-source WiFi firmware such as DD-WRT are known to provide WiFi device owners with much more flexibility and potentially fixes the issues that plagued the original firmware.

Any kind of restriction on modifying or replacing the firmware used for WiFi devices would prove disastrous. It's akin to telling the cell phone service providers to lock the phones (and thus the device be forever stuck on that provider's network).

Please reconsider making progress on this rule. I do not know what the intention of this rule is for. But unfortunately, such a rule being put in place would affect WiFi devices that are everywhere nowadays.

Restrictions on software or firmware modifications for consumer RF devices, mainly WiFi devices, would place a major hindrance on the consumers' experience and value for their devices. Some WiFi devices are severely limited out of the box due to poor and sub-standard firmware. Open-source WiFi firmware such as DD-WRT are known to provide WiFi device owners with much more flexibility and potentially fixes the issues that plagued the original firmware.

Any kind of restriction on modifying or replacing the firmware used for WiFi devices would prove disastrous. It's akin to telling the cell phone service providers to lock the phones (and thus the device be forever stuck on that provider's network).

Please reconsider making progress on this rule. I do not know what the intention of this rule is for. But unfortunately, such a rule being put in place would affect WiFi devices that are everywhere nowadays.