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: Maxim
Last Name: Cherkasov
Mailing Address: RF, Novosibirsk
City: Novosibirsk
Country: Russia
State or Province: Novosibirsk
ZIP/Postal Code: 630126
Email Address:
Organization Name:
Comment: save wi-fi

save wi-fi

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: Randy
Last Name: Saunders
Mailing Address: 7052 River Oak Ct
City: Clarksville
Country: United States
State or Province: MD
ZIP/Postal Code: 21029
Email Address: R.Saunders@ieee.org
Organization Name: null
Comment: As written, the rules and recommendations of the commission will prevent the installation of available free and open source wireless firmware such as DD-WRT and OpenWrt, both of which I use. This firmware better fits the my needs, which are not the same as my ISP. My ISP wants to use my router to provide WiFi to their customers, without regard for the security and bandwidth congestion impacts that would have on my facility. I need to be able to tailor the device to my needs. I set up a tightly constrained guest wireless network, just as I would allow an Amish carriage to water their horse from by garden hose. I consider this part of being civil in the community, and since I pay for the service, the ISP shouldn't be able to leverage the FCC's regulation of radio space to mandate their business practices. The emerging Internet of Things will make further demands of WiFi routers, and there is no reason it should put predatory ISPs in a position to further expand their leverage over their users. Where strong net neutrality is needed, these rules mandate DRM to further entrench the world's advocates against net neutrality. The changes proposed will make my needed changes difficult and, in some cases, impossible.

As written, the rules and recommendations of the commission will prevent the installation of available free and open source wireless firmware such as DD-WRT and OpenWrt, both of which I use. This firmware better fits the my needs, which are not the same as my ISP. My ISP wants to use my router to provide WiFi to their customers, without regard for the security and bandwidth congestion impacts that would have on my facility. I need to be able to tailor the device to my needs. I set up a tightly constrained guest wireless network, just as I would allow an Amish carriage to water their horse from by garden hose. I consider this part of being civil in the community, and since I pay for the service, the ISP shouldn't be able to leverage the FCC's regulation of radio space to mandate their business practices. The emerging Internet of Things will make further demands of WiFi routers, and there is no reason it should put predatory ISPs in a position to further expand their leverage over their users. Where strong net neutrality is needed, these rules mandate DRM to further entrench the world's advocates against net neutrality. The changes proposed will make my needed changes difficult and, in some cases, impossible.

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: Frisvold
Mailing Address: 119 Fairview St.
City: Lehighton
Country: United States
State or Province: PA
ZIP/Postal Code: 18235-2812
Email Address: friz@godshell.com
Organization Name:
Comment: Making this change will greatly impact the open source community. There are incredible open source project such as DD-WRT, SDR#, and others that significantly enhance existing equipment by providing a stable codebase and features that vendors are unwilling to provide. A vendor is typically motivated by sales and is more interested in building new hardware that can be sold rather than updating firmware with new features. Additionally, open source has a proven track record of resolving security issues in a timely manner.

I oppose this change in the rules.

Making this change will greatly impact the open source community. There are incredible open source project such as DD-WRT, SDR#, and others that significantly enhance existing equipment by providing a stable codebase and features that vendors are unwilling to provide. A vendor is typically motivated by sales and is more interested in building new hardware that can be sold rather than updating firmware with new features. Additionally, open source has a proven track record of resolving security issues in a timely manner.

I oppose this change in the 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: Matthew
Last Name: Miller
Mailing Address: 11 Cameron Ave. #2
City: Somerville
Country: United States
State or Province: MA
ZIP/Postal Code: 02144
Email Address:
Organization Name: Fedora Project
Comment: Please do not implement any rules which take away the ability for citizens to install software of their choosing on their own computing devices. This is essential to freedom in the broad sense in the digital era.

Please do not implement any rules which take away the ability for citizens to install software of their choosing on their own computing devices. This is essential to freedom in the broad sense in the digital era.

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: Philip
Last Name: McClure
Mailing Address: 16767 W College St
City: Pulaski
Country: United States
State or Province: TN
ZIP/Postal Code: 38478
Email Address: philip.mcclure@gmail.com
Organization Name: none
Comment: I should be able to control the software that is installed in the devices I own.

I should be able to control the software that is installed in the devices I own.

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: Sullivan
Mailing Address: 60 Farquhar Ave
City: Yonkers
Country: United States
State or Province: NY
ZIP/Postal Code: 10701
Email Address:
Organization Name:
Comment: This rule has been poorly thought out. Open source router firmware such as DD-WRT was created to address the problem of manufacturers not releasing functional and secure firmware. If this rule goes into effect then many people will be forced to run bug riddled and vulnerable software that's easily exploited. Information security is already a huge concern and this would greatly exacerbate the problem. What are you addressing that you're willing to sacrifice the security of millions of people? There must be a better way because preventing us from using current up-to-date and secure software will be an absolute disaster. I am strongly against this attack on well maintained, secure open source firmware that is much, much better than anything a manufacturer ever will or has provided.

This rule has been poorly thought out. Open source router firmware such as DD-WRT was created to address the problem of manufacturers not releasing functional and secure firmware. If this rule goes into effect then many people will be forced to run bug riddled and vulnerable software that's easily exploited. Information security is already a huge concern and this would greatly exacerbate the problem. What are you addressing that you're willing to sacrifice the security of millions of people? There must be a better way because preventing us from using current up-to-date and secure software will be an absolute disaster. I am strongly against this attack on well maintained, secure open source firmware that is much, much better than anything a manufacturer ever will or has provided.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Mark
Last Name: McKeen
Mailing Address: 424 Wood Street
City: Fort Collins
Country: United States
State or Province: CO
ZIP/Postal Code: 80521
Email Address:
Organization Name:
Comment: The law steps on yet another foundation of education and hobbies. The inability to use custom software on hardware I own is like putting me in chains. We already have far too many laws with DRM. Common sense says if I own it is can do whatever I want to it. What's next? I won't be able to use aftermarket parts on my car? Corporate interests are systematically targeting creativity and innovation. This needs to stop. Our fundamental rights as US citizens are being constrained every time a law like this passes. Our ability to customize the things we own is part of our freedom of speech and expression. Don't let these companies that are pushing this bill step on our rights, your rights, to own something we bought.

Either way we will break the DRM and take back control of the devices we own. This law is a waste of money and only furthers the interests of corporate wallets - not the people.

The law steps on yet another foundation of education and hobbies. The inability to use custom software on hardware I own is like putting me in chains. We already have far too many laws with DRM. Common sense says if I own it is can do whatever I want to it. What's next? I won't be able to use aftermarket parts on my car? Corporate interests are systematically targeting creativity and innovation. This needs to stop. Our fundamental rights as US citizens are being constrained every time a law like this passes. Our ability to customize the things we own is part of our freedom of speech and expression. Don't let these companies that are pushing this bill step on our rights, your rights, to own something we bought.

Either way we will break the DRM and take back control of the devices we own. This law is a waste of money and only furthers the interests of corporate wallets - not the people.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Christopher
Last Name: Schultz
Mailing Address: 805 S Veitch St
City: Arlington
Country: United States
State or Province: VA
ZIP/Postal Code: 22204
Email Address: chris@christopherschultz.net
Organization Name:
Comment: Please do not prohibit the modification of a device by either its owner or an agent of the owner (e.g. A contractor or repair technician). Leaving this prohibition in these rules makes it impossible for owners to repair or replace components (especially the software) of a device that is failing to protect security and/or privacy of its owner.

Companies who make these devices do not always support them past some arbitrary window of time (e.g. 90 days, 1 year, etc.) even though the device may continue to perform its primary function (e.g. Broadband router) well beyond that window of time. After that window of time ends, the device is completely unsupported and can contribute to the insecurity of the Internet or whichever environment the device operates.

The ability of owners to modify these devices is critical to a safe Internet and not just for an individual owner; a compromised device also represents a risk to any other network user that may communicate with the owner of an otherwise unsupported (and therefore potentially vulnerable device).

If the concern is that unauthorized parties will modify these devices, please make an allowance specifically for device owners or their designated agents.

Please do not prohibit the modification of a device by either its owner or an agent of the owner (e.g. A contractor or repair technician). Leaving this prohibition in these rules makes it impossible for owners to repair or replace components (especially the software) of a device that is failing to protect security and/or privacy of its owner.

Companies who make these devices do not always support them past some arbitrary window of time (e.g. 90 days, 1 year, etc.) even though the device may continue to perform its primary function (e.g. Broadband router) well beyond that window of time. After that window of time ends, the device is completely unsupported and can contribute to the insecurity of the Internet or whichever environment the device operates.

The ability of owners to modify these devices is critical to a safe Internet and not just for an individual owner; a compromised device also represents a risk to any other network user that may communicate with the owner of an otherwise unsupported (and therefore potentially vulnerable device).

If the concern is that unauthorized parties will modify these devices, please make an allowance specifically for device owners or their designated agents.

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: Derrek
Last Name: Benesh
Mailing Address: PO Box 12456
City: Durham
Country: United States
State or Province: NC
ZIP/Postal Code: 27709
Email Address:
Organization Name:
Comment: 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.
Please consider the following facts: Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
Thank you.

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

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: Stefan
Last Name: Koerner
Mailing Address: Alfred-Herrhausen-Allee 16-24
City: Eschborn
Country: Germany
State or Province: Hessen
ZIP/Postal Code: 65760
Email Address: stefan.koerner@db.com
Organization Name:
Comment: the default software provided with most WiFi routers is extremely broken at delivery, most miss critical functions.
also most manufacturers stop providing critical patches after some time or take extremely long to fix bugs,
where the experience with open source firmware has been mostly good.

allowing only the manufacturer firmware where we currently can use e.g. DD-WRT or OpenWRT
to work around limitations will likely lead to avoiding hardware with limited firmware alltogether.
if necessary this means not providing the WIFI service at all to protect the network and data.

PS: after the recent revealment of firmware-bugs installed by order of the US government n american products, this FCC rule is a measure that completely undermines trust in WiFi routers with a FCC seal. frankly speaking it is a reason not to buy a product.

the default software provided with most WiFi routers is extremely broken at delivery, most miss critical functions.
also most manufacturers stop providing critical patches after some time or take extremely long to fix bugs,
where the experience with open source firmware has been mostly good.

allowing only the manufacturer firmware where we currently can use e.g. DD-WRT or OpenWRT
to work around limitations will likely lead to avoiding hardware with limited firmware alltogether.
if necessary this means not providing the WIFI service at all to protect the network and data.

PS: after the recent revealment of firmware-bugs installed by order of the US government n american products, this FCC rule is a measure that completely undermines trust in WiFi routers with a FCC seal. frankly speaking it is a reason not to buy a product.

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: Travis
Last Name: Hardiman
Mailing Address: 235 Pemberton Rd
City: Rochester
Country: United States
State or Province: NY
ZIP/Postal Code: 14622-1807
Email Address: travis.hardiman@gmail.com
Organization Name:
Comment: Please do not prohibit me (or anyone) from flashing the firmware of my routers, phones, and other wireless devices. This would stifle innovation by preventing great third-party firmware from being installed, and make the devices less secure due to the inability to fix bugs.

Please do not prohibit me (or anyone) from flashing the firmware of my routers, phones, and other wireless devices. This would stifle innovation by preventing great third-party firmware from being installed, and make the devices less secure due to the inability to fix bugs.

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: McClain
Mailing Address: 8278 Pawtucket ct
City: Indianapolis
Country: United States
State or Province: IN
ZIP/Postal Code: 46256
Email Address: jacob.mcclain@gmail.com
Organization Name:
Comment: Please do not pass the proposal for device manufacturers having to implement security to prevent flashing of custom firmware. I would like to see a hardware limitation of the radio before I saw a software limitation that may have far reaching consequences. I purchase some/most devices with the sole intention of putting custom firmware on it to make it better.

Please do not pass the proposal for device manufacturers having to implement security to prevent flashing of custom firmware. I would like to see a hardware limitation of the radio before I saw a software limitation that may have far reaching consequences. I purchase some/most devices with the sole intention of putting custom firmware on it to make it better.

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: Schaible
Mailing Address: 619 Parkview Avenue
City: Braddock
Country: United States
State or Province: PA
ZIP/Postal Code: 15104
Email Address:
Organization Name:
Comment: I enjoy being able to modify the firmware of my router to ensure it fits in to my local wireless spectrum, between the noise of other routers. I'd like to continue owning the things I purchase and not having the open source nature of my devices ruined.

I enjoy being able to modify the firmware of my router to ensure it fits in to my local wireless spectrum, between the noise of other routers. I'd like to continue owning the things I purchase and not having the open source nature of my devices ruined.

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: Graham
Last Name: Hutchinson
Mailing Address: 233 Crown Point Mdws
City: Centerville
Country: United States
State or Province: OH
ZIP/Postal Code: 45458
Email Address:
Organization Name:
Comment: I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:
Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:
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: Jorg
Last Name: Kewisch
Mailing Address: 115 Broadview Circle
City: Wading River
Country: United States
State or Province: NY
ZIP/Postal Code: 11792
Email Address: jorg@optonline.net
Organization Name:
Comment: I oppose ANY proposal that would prevent or limit users from
installing open-source firmware on WiFi routers. Appart from concerns about the safety of preinstalled firmware such ruling would stifle innovation. The Linux system (which is used in a large number of web servers and nearly all scientific computing as well as Apple and Microsoft started by user written software.

I oppose ANY proposal that would prevent or limit users from
installing open-source firmware on WiFi routers. Appart from concerns about the safety of preinstalled firmware such ruling would stifle innovation. The Linux system (which is used in a large number of web servers and nearly all scientific computing as well as Apple and Microsoft started by user written 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: Andrew
Last Name: Shur
Mailing Address: 604 Hillcrest Ave.
City: Wilmington
Country: United States
State or Province: DE
ZIP/Postal Code: 19809
Email Address: andrew.shur@gmail.com
Organization Name:
Comment: To whom it may concern,

The ability to modify or "make better" technology that companies have decided to stop supporting should never be banned. We are dealing with a worse version of this currently with companies like John Deer not wanting you to be able to repair your own farm equipment; instead you would have to go to them where they could charge a monopoly service charge to fix every part. Where else could you go?

With the amount of spying from different governments these days, the ability to wipe and install my own software on any piece of hardware is essential. I should not be forced to use old, never updated software that barley works when there are people out there passionate in trying to make equipment work better and faster.

In conclusion, all this rule would do is allow companies to create inadequate software since they will never have to worry about competition from some kids in their garage, and all of our best technology has come from kids in their garages.

To whom it may concern,

The ability to modify or "make better" technology that companies have decided to stop supporting should never be banned. We are dealing with a worse version of this currently with companies like John Deer not wanting you to be able to repair your own farm equipment; instead you would have to go to them where they could charge a monopoly service charge to fix every part. Where else could you go?

With the amount of spying from different governments these days, the ability to wipe and install my own software on any piece of hardware is essential. I should not be forced to use old, never updated software that barley works when there are people out there passionate in trying to make equipment work better and faster.

In conclusion, all this rule would do is allow companies to create inadequate software since they will never have to worry about competition from some kids in their garage, and all of our best technology has come from kids in their garages.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Josh
Last Name: Harding
Mailing Address: 1615 Fox Run Dr
City: Arlington Heights
Country: United States
State or Province: IL
ZIP/Postal Code: 60004
Email Address:
Organization Name:
Comment: Your proposed rules prohibit me from fixing buggy and/or insecure software shipped by a WiFi router manufacturer.

Manufacturers have little incentive to be quick to fix security holes in their products (they already got paid). As an end consumer, I'm the one suffering from the problems with the software. The open source community can much more quickly deploy software fixes if you let them.

Your proposed rules prohibit me from fixing buggy and/or insecure software shipped by a WiFi router manufacturer.

Manufacturers have little incentive to be quick to fix security holes in their products (they already got paid). As an end consumer, I'm the one suffering from the problems with the software. The open source community can much more quickly deploy software fixes if you let them.

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: Nadeem
Last Name: Azhar
Mailing Address: 5315B Cypress Creek Pkwy
City: Houston
Country: United States
State or Province: TX
ZIP/Postal Code: 77069
Email Address:
Organization Name:
Comment: FCC a phone could be jail broken/rooted but you want to restrict custom firmware on devices? One step forward two steps back anyone?
We use custom firmware to fix issues/vulnerabilities that most manufacturers not not nimble enough to fix on time.
Custom firmware allows us to add options specific customers need.
Custom firmware even helps us identify underlying hardware problems quickly and efficiently.

FCC a phone could be jail broken/rooted but you want to restrict custom firmware on devices? One step forward two steps back anyone?
We use custom firmware to fix issues/vulnerabilities that most manufacturers not not nimble enough to fix on time.
Custom firmware allows us to add options specific customers need.
Custom firmware even helps us identify underlying hardware problems quickly and efficiently.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Andrew
Last Name: Fenuk
Mailing Address: Derbentskaya 77
City: Krasnodar
Country: Russia
State or Province: KRD
ZIP/Postal Code: 350042
Email Address: fenyukandrew@gmail.com
Organization Name:
Comment: Wireless networking research depends on the ability of researchers to investigate and modify their devices. 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.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. 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: Korn
Last Name: De Sand
Mailing Address: Naturstr. 1
City: Neufeld
Country: Germany
State or Province: Bayern
ZIP/Postal Code: 95326
Email Address:
Organization Name:
Comment: User Freedom

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

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.
Economic Impact

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

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for

small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

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

Security

User Freedom

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

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

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

Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for

small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

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

Security

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: james michael
Last Name: dupont
Mailing Address: 2527 belle crest dr
City: lawrence
Country: United States
State or Province: KS
ZIP/Postal Code: 66047
Email Address: jamesmikedupont@gmail.com
Organization Name: free/libre open source and open knowledge association of kansas
Comment: Dear Sirs,
I would like to respectfully ask that you do not limit the usage of devices to software that is purchased but allow for the open source community to be able to come up with solutions.

I understand the need to regulate the spectrum, a long time ago I got my technicians license and my family has a large number of licensed radio operators.

Authorization of software is the wrong step in my opinion, going back to the time of home made radios it is like saying that only authorized brands of radios may be used. We need to look at the problems and say that certain illegal usage of spectrum are illegal not mandating software.

The creation of licensed software will stifle creativity and hurt our open source community.

Respectfully,

James Michael DuPont

Dear Sirs,
I would like to respectfully ask that you do not limit the usage of devices to software that is purchased but allow for the open source community to be able to come up with solutions.

I understand the need to regulate the spectrum, a long time ago I got my technicians license and my family has a large number of licensed radio operators.

Authorization of software is the wrong step in my opinion, going back to the time of home made radios it is like saying that only authorized brands of radios may be used. We need to look at the problems and say that certain illegal usage of spectrum are illegal not mandating software.

The creation of licensed software will stifle creativity and hurt our open source community.

Respectfully,

James Michael DuPont

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: Dadash
Last Name: Mukhtarov
Mailing Address: 10, Mirjalal St., Apt. 90
City: Baku
Country: Azerbaijan
State or Province: 1134
ZIP/Postal Code: 1134
Email Address: rapatar@gmail.com
Organization Name:
Comment: Freedom!

Freedom!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Roman
Last Name: Valeyev
Mailing Address: 7a semashko st
City: simferopol
Country: Russia
State or Province: Crimea
ZIP/Postal Code: 395026
Email Address:
Organization Name:
Comment: don't, pls

don't, pls

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: Gogolev
Mailing Address: Lezhnevskaya st., 128, 1
City: Ivanovo
Country: Russia
State or Province: Ivanovskaya
ZIP/Postal Code: 155000
Email Address: gogolev.sergey@gmail.com
Organization Name:
Comment: Dear FCC, it is not fair.

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.

Dear FCC, it is not fair.

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: Nolan
Last Name: S
Mailing Address: E Olive Way
City: Seattle
Country: United States
State or Province: WA
ZIP/Postal Code: 98102
Email Address:
Organization Name:
Comment: Please do not implement the proposed ban upon radio modification in wireless devices. To stifle the creative and ingenius community surrounding open source software development, which hinges on the ability to tweak wireless devices including the radios inside them, would negatively impact the overall software development ecosystem. The open source community is a fragile yet critical structure in software development and has led to some of the most important and accessible software advances in the world, including, in a way, the entire Android operating system. Please reconsider before taking the creative process out of the hands of tinkerers all over the country.

Please do not implement the proposed ban upon radio modification in wireless devices. To stifle the creative and ingenius community surrounding open source software development, which hinges on the ability to tweak wireless devices including the radios inside them, would negatively impact the overall software development ecosystem. The open source community is a fragile yet critical structure in software development and has led to some of the most important and accessible software advances in the world, including, in a way, the entire Android operating system. Please reconsider before taking the creative process out of the hands of tinkerers all over the country.

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: Baryshnikov
Mailing Address: TSQ
City: Moscow
Country: Russia
State or Province: RF
ZIP/Postal Code: 123456
Email Address: brr@zmail.ru
Organization Name:
Comment: This new regulation is absolute crap! It closes possibilities for development of free software and enhancements which could be done by users and independent software companies.

This new regulation is absolute crap! It closes possibilities for development of free software and enhancements which could be done by users and independent software companies.

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: Artem
Last Name: Andrushko
Mailing Address: 165 Amboy Road Unit 710 for 1090
City: Morganville
Country: United States
State or Province: NJ
ZIP/Postal Code: 07751
Email Address: lbicbiy@gmail.com
Organization Name:
Comment: It is very strange. I am developer and my work is to optimise firmware for special requirments. Don't deprive me of work.

It is very strange. I am developer and my work is to optimise firmware for special requirments. Don't deprive me of work.

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: Maxim
Last Name: Usok
Mailing Address: Bulgakova str., 5
City: Kiev
Country: Ukraine
State or Province: Kyivskaya obl
ZIP/Postal Code: 03134
Email Address: max.usok@gmail.com
Organization Name:
Comment: In fact, the new regulations FCC puts an end to the use of available firmware. The ban on the modification relates to personal computers, laptops and mobile phones with built-chip Wi-Fi.

If the new regulation enters into force, it can lead to the following: a ban on the installation of a computer alternative operating system (GNU / Linux, OpenBSD, FreeBSD, and others.); Frozen research in the field of advanced wireless technologies, such as mesh-network; a ban on the installation of third-party firmware on Android-smartphone; vague prospects of the free firmware for routers as OpenWrt.

In fact, the new regulations FCC puts an end to the use of available firmware. The ban on the modification relates to personal computers, laptops and mobile phones with built-chip Wi-Fi.

If the new regulation enters into force, it can lead to the following: a ban on the installation of a computer alternative operating system (GNU / Linux, OpenBSD, FreeBSD, and others.); Frozen research in the field of advanced wireless technologies, such as mesh-network; a ban on the installation of third-party firmware on Android-smartphone; vague prospects of the free firmware for routers as OpenWrt.

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: Darrik
Last Name: Marion
Mailing Address: 2124 E. Sanson
City: Spokane
Country: United States
State or Province: WA
ZIP/Postal Code: 99207
Email Address: darrikmarion@outlook.com
Organization Name:
Comment: Regulation and the locking down of wireless firmware is a major blow to the Free and Open Source Software community. By closing the source of many routers and wireless cards, many users will not be able to access the internet as we see it.

Regulation and the locking down of wireless firmware is a major blow to the Free and Open Source Software community. By closing the source of many routers and wireless cards, many users will not be able to access the internet as we see it.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Dionisii
Last Name: Vergasov
Mailing Address: antisocial4tr@gmail.com
City: Prague
Country: Czech Republic
State or Province: Bohemia
ZIP/Postal Code: 2500533456
Email Address:
Organization Name:
Comment: If the new regulation enters into force, it can lead to the following: a ban on the installation of a computer alternative operating system (GNU / Linux, OpenBSD, FreeBSD, and others.); Frozen research in the field of advanced wireless technologies, such as mesh-network; a ban on the installation of third-party firmware on Android-smartphone; vague prospects of the free firmware for routers as OpenWrt.

It would ban free firmware - it's only an American problem as well as a ban on jailbreaking "iPhones". Like, let forbid there at anything we what?

But the decision of the US regulator will inevitably affect us - Europe, Asia, etc. It should be understood that the Chinese producers are unlikely to want to make two models of the router: one for US and one for the rest of the world. No, we also get the gadgets of locked stitching. So the FCC decision a blow across the world.

And it worries me.

If the new regulation enters into force, it can lead to the following: a ban on the installation of a computer alternative operating system (GNU / Linux, OpenBSD, FreeBSD, and others.); Frozen research in the field of advanced wireless technologies, such as mesh-network; a ban on the installation of third-party firmware on Android-smartphone; vague prospects of the free firmware for routers as OpenWrt.

It would ban free firmware - it's only an American problem as well as a ban on jailbreaking "iPhones". Like, let forbid there at anything we what?

But the decision of the US regulator will inevitably affect us - Europe, Asia, etc. It should be understood that the Chinese producers are unlikely to want to make two models of the router: one for US and one for the rest of the world. No, we also get the gadgets of locked stitching. So the FCC decision a blow across the world.

And it worries me.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Kevin
Last Name: Lee
Mailing Address: 177 W. 200 N.
City: Hyrum
Country: United States
State or Province: UT
ZIP/Postal Code: 84319
Email Address:
Organization Name:
Comment: I stand against certain aspects of this proposal. I highly believe that users should freely be able to modify devices with "modular wireless radio" capability's, such as networking routers, computer systems and cell phones.

This proposal set forth, although with good intention, will do more harm than good, by restricting and/or discouraging open source router and cell phone firmware, alternative operating systems, research and development of wireless technologies, and amateur radio mesh networks for emergency communication.

As a licensed amateur radio technician, i am passionate about the responsible use of frequencies for communication of all types, and see no reason to put into action the restrictions set forth, as it will only hinder advancements, security, and options in the tech industry at large.

Thank you for your efforts in managing the radio frequency and wireless spectrum, and for the opportunity to voice my opinions in this matter.

Kevin Lee - N7ERV

I stand against certain aspects of this proposal. I highly believe that users should freely be able to modify devices with "modular wireless radio" capability's, such as networking routers, computer systems and cell phones.

This proposal set forth, although with good intention, will do more harm than good, by restricting and/or discouraging open source router and cell phone firmware, alternative operating systems, research and development of wireless technologies, and amateur radio mesh networks for emergency communication.

As a licensed amateur radio technician, i am passionate about the responsible use of frequencies for communication of all types, and see no reason to put into action the restrictions set forth, as it will only hinder advancements, security, and options in the tech industry at large.

Thank you for your efforts in managing the radio frequency and wireless spectrum, and for the opportunity to voice my opinions in this matter.

Kevin Lee - N7ERV

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: Dmitriy
Last Name: Dzhuriy
Mailing Address: Freedom st 74
City: Krasnodar
Country: Russia
State or Province: Krasnodar region
ZIP/Postal Code: 357000
Email Address: lonfas@lonfas.ru
Organization Name:
Comment: Hello guys!
Your decisions affects the whole world. Please approach them more deliberately
Best regards

Hello guys!
Your decisions affects the whole world. Please approach them more deliberately
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: richard
Last Name: Lough
Mailing Address: 9 Windslow heights
City: Carrickfergus
Country: United Kingdom
State or Province: Co Antrim
ZIP/Postal Code: BT38 9AT
Email Address: ralough@iee.org
Organization Name:
Comment: RE para 26. The change seems to unduly broad, and once implemented will be difficult to reverse even if found to be totally inappropriate. It is expected that the law of unforseen consequences will eventually apply: the design will break in the worst possible way at the worst possible time.

RE para 26. The change seems to unduly broad, and once implemented will be difficult to reverse even if found to be totally inappropriate. It is expected that the law of unforseen consequences will eventually apply: the design will break in the worst possible way at the worst possible 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: philip jh
Last Name: jh
Mailing Address: wsidxyz@exemail.com.au
City: melbourne
Country: Australia
State or Province: vic
ZIP/Postal Code: 3003
Email Address: wsidxyz@exemail.com.au
Organization Name: wsid
Comment: hello to the fcc

i have learned that you intend to take the following actions
please refer to http://slashdot.org/?page=1

Hackaday reports that the FCC is introducing new rules which ban firmware modifications for the radio systems in WiFi routers and other wireless devices operating in the 5 GHz range. The vast majority of routers are manufactured as System on Chip devices, with the radio module and CPU integrated in a single package. The new rules have the potential to effectively ban the installation of proven Open Source firmware on any WiFi router.

i strongly disagree with this intent and suggest you dont go forward with these actions
my arguments are based on this information. https://libreplanet.org/wiki/Save_WiFi

quote
"
Save WiFi
The FCC wants to require device makers to lock down the software and firmware on computers with radio devices (wifi, bluetooth, etc) ...stop them.

FCC Notice of Proposed Rulemaking (NPRM):
http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0722/FCC-15-92A1.pdf
Federal Register comment page:
https://www.federalregister.gov/articles/2015/08/06/2015-18402/equipment-authorization-and-electronic-labeling-for-wireless-devices

Here are the proposed rules from the NPRM that we are going to comment on: Save_WiFi/Rules
Here is the list of all specific request for comment the FCC has made in this NPRM: Save_WiFi/RFC
Here is where we are drafting specific language for our letters and comments to the FCC: Save_WiFi_letter_language
Here is joint letter we're creating to submit to the FCC on the NPRM: Joint Letter
Send your comments to the FCC. Prepared questions for meeting with the FCC (tentative date: second week of September).
More info
The FCC has proposed rules (ET Docket No. 15-170) that will require device makers with WiFi and other Radio Frequency (RF) devices to cryptographically lock down the RF-controlling software on those devices so as to prevent

users from installing the software of their choice. This means not only routers, but also many phones, tablets, laptops, and any number of new devices that are wifi capable would now be required to implement a low level DRM system that prevents users from re-flashing or modifying the operating system and/or firmware on those devices.

We have been fighting for years the unjust laws that serve to protect companies that use DRM to restrict users. This new regulation goes beyond protecting those who use DRM, this would be a law requiring device makers to implement low level DRM technology to restrict users from upgrading the operating system and/or firmware of many devices.
"

you can read the full detail here. https://libreplanet.org/wiki/Save_WiFi

philip jh
wsidxyz@exemail.com.au
australia

hello to the fcc

i have learned that you intend to take the following actions
please refer to http://slashdot.org/?page=1

Hackaday reports that the FCC is introducing new rules which ban firmware modifications for the radio systems in WiFi routers and other wireless devices operating in the 5 GHz range. The vast majority of routers are manufactured as System on Chip devices, with the radio module and CPU integrated in a single package. The new rules have the potential to effectively ban the installation of proven Open Source firmware on any WiFi router.

i strongly disagree with this intent and suggest you dont go forward with these actions
my arguments are based on this information. https://libreplanet.org/wiki/Save_WiFi

quote
"
Save WiFi
The FCC wants to require device makers to lock down the software and firmware on computers with radio devices (wifi, bluetooth, etc) ...stop them.

FCC Notice of Proposed Rulemaking (NPRM):
http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0722/FCC-15-92A1.pdf
Federal Register comment page:
https://www.federalregister.gov/articles/2015/08/06/2015-18402/equipment-authorization-and-electronic-labeling-for-wireless-devices

Here are the proposed rules from the NPRM that we are going to comment on: Save_WiFi/Rules
Here is the list of all specific request for comment the FCC has made in this NPRM: Save_WiFi/RFC
Here is where we are drafting specific language for our letters and comments to the FCC: Save_WiFi_letter_language
Here is joint letter we're creating to submit to the FCC on the NPRM: Joint Letter
Send your comments to the FCC. Prepared questions for meeting with the FCC (tentative date: second week of September).
More info
The FCC has proposed rules (ET Docket No. 15-170) that will require device makers with WiFi and other Radio Frequency (RF) devices to cryptographically lock down the RF-controlling software on those devices so as to prevent users from installing the software of their choice. This means not only routers, but also many phones, tablets, laptops, and any number of new devices that are wifi capable would now be required to implement a low level DRM system that prevents users from re-flashing or modifying the operating system and/or firmware on those devices.

We have been fighting for years the unjust laws that serve to protect companies that use DRM to restrict users. This new

regulation goes beyond protecting those who use DRM, this would be a law requiring device makers to implement low level DRM technology to restrict users from upgrading the operating system and/or firmware of many devices.
"

you can read the full detail here. https://libreplanet.org/wiki/Save_WiFi

philip jh
wsidxyz@exemail.com.au
australia

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: Alexander
Last Name: Waldmann
Mailing Address: 41 North Terrace
City: Port Elliot
Country: Australia
State or Province: South Australia
ZIP/Postal Code: 5212
Email Address: melchior@tfwno.gf
Organization Name:
Comment: I am very strongly opposed to restricting software that controls radio hardware. Firstly, when there are security holes or backdoors or regular bugs in such software, it needs to be discoverable and fixable by anyone, because there is no guarantee the original manufacturer will do so. I personally have benefitted from more reliable third-party router firmware and custom Android distributions, and I am also loathe to trust closed software. More importantly, innovation depends on being able to modify and build off of existing tools, and there are much greater possibilities for wireless than what we use them for now.

I am very strongly opposed to restricting software that controls radio hardware. Firstly, when there are security holes or backdoors or regular bugs in such software, it needs to be discoverable and fixable by anyone, because there is no guarantee the original manufacturer will do so. I personally have benefitted from more reliable third-party router firmware and custom Android distributions, and I am also loathe to trust closed software. More importantly, innovation depends on being able to modify and build off of existing tools, and there are much greater possibilities for wireless than what we use them for now.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Jay
Last Name: Libove
Mailing Address: 1876 Hartland Ct
City: Bowling Green
Country: United States
State or Province: KY
ZIP/Postal Code: 42103
Email Address: libove@felines.org
Organization Name:
Comment: I support the libreplanet.org concerns about the proposed rules restricting the ability of users to modify devices with a 'modular wireless radio'.

In addition to the libreplanet comments (which I reproduce in full below) I point out that, simply, this proposed rule and proposed restriction is like prohibiting iron foundries from existing because they could be used to make or modify weapons.
Effectively, the proposed rule is a blunt instrument which will bludgeon innovation, freedom, creativity, reasonable use, and even security, in the name of preventing people from misusing technology.
Overly broad technological prohibitions never work, and they always have major unintended, undesirable consequences.
Please, go back to the drawing board, and rely much more on detection and correction than on short-sighted, damaging prevention in this case.

thank you,
Jay Libove, CISSP, CIPP/US, CIPT, CISM

I support the libreplanet.org concerns about the proposed rules restricting the ability of users to modify devices with a 'modular wireless radio'.

In addition to the libreplanet comments (which I reproduce in full below) I point out that, simply, this proposed rule and proposed restriction is like prohibiting iron foundries from existing because they could be used to make or modify weapons.
Effectively, the proposed rule is a blunt instrument which will bludgeon innovation, freedom, creativity, reasonable use, and even security, in the name of preventing people from misusing technology.
Overly broad technological prohibitions never work, and they always have major unintended, undesirable consequences.
Please, go back to the drawing board, and rely much more on detection and correction than on short-sighted, damaging prevention in this case.

thank you,
Jay Libove, CISSP, CIPP/US, CIPT, CISM

User Freedom
As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the userâ€™s needs. Each user is better able to tailor the device to their needs. The changes proposed will make such changes difficult and, in some cases, impossible.

Innovation
Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

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

Guest Wifi hotspots businesses
Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses
Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

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

Security
Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users

replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

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: matteo
Last Name: Arlotti
Mailing Address: Viale Ugo Foscolo 29
City: Italy
Country: Italy
State or Province: Italy
ZIP/Postal Code: 47900
Email Address:
Organization Name:
Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Dimitrii
Last Name: Ystinov
Mailing Address: 87 Gvardeyskay 77 8
City: Volzhsky
Country: Russia
State or Province: Volgogradskay
ZIP/Postal Code: 404118
Email Address: naugron@gmail.com
Organization Name: -
Comment: This law is stupid. It hinders the development of wireless technologies

This law is stupid. It hinders the development of wireless technologies

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: Boris
Last Name: Sinitsyn
Mailing Address: app 63, Soni Krivoy st 69
City: Chelyabinsk
Country: Russia
State or Province: Chelyabinsk region
ZIP/Postal Code: 454080
Email Address: borisskin@gmail.com
Organization Name:
Comment: Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

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

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: Salishev
Mailing Address: Malaya Balkanskaya 58-361
City: Saint-Petersburg
Country: Russia
State or Province: Saint-Petersburg
ZIP/Postal Code: 198328
Email Address: sergey.i.salishev@gmail.com
Organization Name:
Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Users 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.
Users in other countries depend on your decisions due to globalization.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Users 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.
Users in other countries depend on your decisions due to globalization.

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: Schaefer
Mailing Address: 805 Tinkerbell Rd.
City: Chapel Hill
Country: United States
State or Province: NC
ZIP/Postal Code: 27517
Email Address: sschaefer@acm.org
Organization Name:
Comment: As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.
Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

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

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so

chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

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

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

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

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

Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users