

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: Colin

Last Name: Heinzmann

Mailing Address: 820 Vista Grande Ave

City: Los Altos

Country: United States

State or Province: CA

ZIP/Postal Code: 94024

Email Address: cheinzmann3@gmail.com

Organization Name:

Comment: Please do not block the ability for users to modify the software on their wireless 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 block the ability for users to modify the software on their wireless 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: Gordon

Last Name: Dexter

Mailing Address: 9072 Canterbury Riding

City: Laurel

Country: United States

State or Province: MD

ZIP/Postal Code: 20723

Email Address: kmpuerguy@gmail.com

Organization Name:

Comment: I am extremely concerned about the proposed change in regulations. I use free, open source software on nearly all my computing devices. This includes my laptop, which has wifi and runs Linux, my networking equipment, which run OpenWRT and DD-WRT. This software substantially increases the devices' reliability, and allows me to take full advantage of the hardware, patch security holes that the original hardware vendor hasn't released patches for, and ensure that the device respects my privacy and doesn't send information about my browsing habits to the manufacturer. I am worried that the new regulations could make open source projects like this impossible because it would force manufacturers to lock down their hardware. With all the modern security and privacy issues, having a device in my house that I don't have full control over is disturbing.

Manufacturers have already done things like automatically installed updates that locked out the routers configuration options and required you to make a cloud account and agree to a restrictive terms of service (<http://arstechnica.com/gadgets/2012/07/cisco-backpedals-after-uproar-drops-cloud-from-default-router-setting/>). Rules like those proposed could make this sort of thing the norm, harming everyone through decreased privacy and making home routers less capable and more locked-down.

I am extremely concerned about the proposed change in regulations. I use free, open source software on nearly all my computing devices. This includes my laptop, which has wifi and runs Linux, my networking equipment, which run OpenWRT and DD-WRT. This software substantially increases the devices' reliability, and allows me to take full advantage of the hardware, patch security holes that the original hardware vendor hasn't released patches for, and ensure that the device respects my privacy and doesn't send information about my browsing habits to the manufacturer. I am worried that the new regulations could make open source projects like this impossible because it would force manufacturers to lock down their hardware. With all the modern security and privacy issues, having a device in my house that I don't have full control over is disturbing.

Manufacturers have already done things like automatically installed updates that locked out the routers configuration options and required you to make a cloud account and agree to a restrictive terms of service (<http://arstechnica.com/gadgets/2012/07/cisco-backpedals-after-uproar-drops-cloud-from-default-router-setting/>). Rules like those proposed could make this sort of thing the norm, harming everyone through decreased privacy and making home routers less capable and more locked-down.

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: Mohamed Thalib

Last Name: H

Mailing Address: 11, North Raja St,

City: Chennai

Country: India

State or Province: TN

ZIP/Postal Code: 600016

Email Address:

Organization Name:

Comment: I request FCC and its board

DONT 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 request FCC and its board

DONT 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: Igor

Last Name: Chelnokov

Mailing Address: some street, random number, some appartment

City: Zhytomyr

Country: Ukraine

State or Province: Zhytomyr Oblast

ZIP/Postal Code: 18101

Email Address:

Organization Name:

Comment: Regulation about devices that operate in U-NII range will impact all devices that use Wi-Fi.

Depending on severity of laws and regulations this might render people unable to install Linux or flash a custom ROM for their mobile or router.

This is unacceptable.

Regulation about devices that operate in U-NII range will impact all devices that use Wi-Fi.

Depending on severity of laws and regulations this might render people unable to install Linux or flash a custom ROM for their mobile or router.

This is unacceptable.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Chris

Last Name: Marsh

Mailing Address: 15450 FM 112

City: Thrall

Country: United States

State or Province: TX

ZIP/Postal Code: 76578

Email Address: chris78664@gmail.com

Organization Name:

Comment: I am respectfully asking the FCC to not implement rules that take away the ability of owners or future owners to install the software of their choosing on their computing devices, this would be like requiring users that received retail Windows XP on their computer with a wireless card to stay with retail Windows XP (no Service Pack) because changing the OS to say Linux or just installing a Service Pack including the drivers could modify the how the wireless card operates as the drivers would have changed. Without the choice to load the software of the owners choice you will be exposing the owners to major security holes that the owners need the ability to fix in their devices when the manufacturer chooses to not do so, like when manufactures only give you only WEP WiFi encryption and decide to not provide WPA or WPA2 encryption, be replacing that software or firmware with another like DD-WRT you breathe new life and security into a device that otherwise would run insecurely waiting to become part of someone's botnet or ends up another piece of trash to end up in the landfill when it is a perfectly usable product still. Manufacturers trying to force early obsolescence of product by not updating them is sadly a common problem in the consumer and enterprise space when it comes to computing devices from the smallest wi-fi device to the largest computer with a wi-fi interfaces. To that end wireless networking research depends on the ability of researchers to investigate and modify their devices to find and fix issues before they begin to be exploited not after the owner is infected. Owners of these devices have in the past fixed serious bugs in wifi drivers provided by the manufacturers and shared those fixes with others including the original manufacturers, 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 owners and companies to install the software of their choosing on their computing devices the NPRM will stall innovation and lower the quality and security of the products put out by the manufacturers further because the owner no longer has ability to breathe new life into their computing product by installing 3rd party firmware, drivers or OS such as DD-WRT or Open-WRT and solely reliant on the manufacturer You defended Net Neutrality now you need to defend Neutrality of choice.

I am respectfully asking the FCC to not implement rules that take away the ability of owners or future owners to install the software of their choosing on their computing devices, this would be like requiring users that received retail Windows XP on their computer with a wireless card to stay with retail Windows XP (no Service Pack) because changing the OS to say Linux or just installing a Service Pack including the drivers could modify the how the wireless card operates as the drivers would have changed. Without the choice to load the software of the owners choice you will be exposing the owners to major security holes that the owners need the ability to fix in their devices when the manufacturer chooses to not do so, like when manufactures only give you only WEP WiFi encryption and decide to not provide WPA or WPA2 encryption, be replacing that software or firmware with another like DD-WRT you breathe new life and security into a device that otherwise would run insecurely waiting to become part of someone's botnet or ends up another piece of trash to end up in the landfill when it is a perfectly usable product still. Manufacturers trying to force early obsolescence of product by not updating them is sadly a common problem in the consumer and enterprise space when it comes to computing devices from the smallest wi-fi device to the largest computer with a wi-fi interfaces.

To that end wireless networking research depends on the ability of researchers to investigate and modify their devices to find and fix issues before they begin to be exploited not after the owner is infected. Owners of these devices have in the past fixed serious bugs in wifi drivers provided by the manufacturers and shared those fixes with others including the original manufacturers, 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 owners and companies to install the software of their choosing on their computing devices the NPRM will stall innovation and lower the quality and security of the products put out by the manufacturers further because the owner no longer has ability to breathe new life into their computing product by installing 3rd party firmware, drivers or OS such as DD-WRT or Open-WRT and solely reliant on the manufacturer You defended Net Neutrality now you need to defend Neutrality of 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: Pavel

Last Name: Astashonok

Mailing Address: p.astashonok@gmail.com

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: 125195

Email Address: p.astashonok@gmail.com

Organization Name:

Comment: The prohibition to change firmware of Wi-Fi transmitters is awful. It violates freedom of expression.

The prohibition to change firmware of Wi-Fi transmitters is awful. It violates freedom of expression.

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: Andrey

Last Name: Lopuha

Mailing Address: exlecknk@10mail.org

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: 111123

Email Address:

Organization Name:

Comment: Don't restrain our freedom to use the free OpenSource software!

Don't restrain our freedom to use the free OpenSource 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: Nico

Last Name: Vijlbrief

Mailing Address: bierbrouwershorst 10

City: apeldoorn

Country: Netherlands

State or Province: gelderland

ZIP/Postal Code: 7328na

Email Address: nico.vijlbrief@outlook.com

Organization Name:

Comment: As a european citizen i do feel very concerned by the proposal that is stated here. Altho i cannot express myself entirely english correct and living under diferent rules and laws, i am deeply concerned by the effects on the global market that this proposal could have, and if made enforced will have on the international scale.

First of all, it will limit comercial companies inside and outside the us for either the american or international markets big effects in such a way that i believe would enforce them all to close down any posible way for customisation, research or protoction of a customers own hardware. It will harm the public privacy, freedom of information and freedom to own a product. Instead a customers device will be on loan, not owned and one cannot proof its inocense, security and protection againts foreign countries, terrosist groups or (bad/black) hackers (crackers).

As a member of multiple freedom fighter groups and advocate of free speech, privacy and security im deeply concernrd that this legislation will make the hardware effected by this help for instance the nsa with backdoors but even worse, help the bad guys get a permanent fix on bacldoors aswell. This bill will prevent your US persons of protecting themselvss. Including us foreigners but keep in mind that it will close the door shut for your own people. It will create a police state inside someones home internet. But quite posible not convermed by their goverment. In example, a chinese router that you, the us cannot moddify so china cannot spy, in said example a openwrt or other "free" firmware would remove such a limit and give freedom to your people.

Dont close those doors, it will harm you and the country harder than you imaginee.

Please ignore any spelling mistakes or potencial wrong wording. My deepest wish is that my concern is comming accross and you see that its a bad idea to close down the open free firmware potentials and lockin any of your US regulations within hardware. It will destroy your freedom, economics and let others spy on you without you having the tools to fix it.

As a european citizen i do feel very concerned by the proposal that is stated here. Altho i cannot express myself entirely english correct and living under diferent rules and laws, i am deeply concerned by the effects on the global market that this proposal could have, and if made enforced will have on the international scale.

First of all, it will limit comercial companies inside and outside the us for either the american or international markets big effects in such a way that i believe would enforce them all to close down any posible way for customisation, research or protoction of a customers own hardware. It will harm the public privacy, freedom of information and freedom to own a product. Instead a customers device will be on loan, not owned and one cannot proof its inocense, security and protection againts foreign countries, terrosist groups or (bad/black) hackers (crackers).

As a member of multiple freedom fighter groups and advocate of free speech, privacy and security im deeply concernd that this legislation will make the hardware effected by this help for instance the nsa with backdoors but even worse, help the bad guys get a permanent fix on bacldoors aswell. This bill will prevent your US persons of protecting themselvss. Including us foreigners but keep in mind that it will close the door shut for your own people. It will create a police state inside someones home internet. But quite posible not convermed by their goverment. In example, a chinese router that you, the us cannot moddifly so china cannot spy, in said example a openwrt or other "free" firmware would remove such a limit and give freedom to your people.

Dont close those doors, it will harm you and the country harder than you imaginge.

Please ignore any spelling mistakes or potencial wrong wording. My deepest wish is that my concern is comming accross and you see that its a bad idea to close down the open free firmware potencials and lockin any of your US regulations within hardware. It will destroy your freedom, economics and let others spy on you without you having the tools to fix 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: James

Last Name: Brock

Mailing Address: 8 Fieldstone drive

City: KIngston

Country: United States

State or Province: NH

ZIP/Postal Code: 03848

Email Address: jamesbrock@livefreeordienh.com

Organization Name:

Comment: These rules are a gross over-reach of federal authority to citizens' personal property that provide no real advantage or benefit to the citizenry as a whole. The only entities that this could possibly benefit are large private corporations and government espionage against private citizens, both of which are largely detrimental to freedom, free speech, and innovation. The following points outline how these changes will negatively impact both individuals and businesses.

These rules are a gross over-reach of federal authority to citizens' personal property that provide no real advantage or benefit to the citizenry as a whole. The only entities that this could possibly benefit are large private corporations and government espionage against private citizens, both of which are largely detrimental to freedom, free speech, and innovation. The following points outline how these changes will negatively impact both individuals and businesses.

These rules are a gross over-reach of federal authority to citizens' personal property that provide no real advantage or benefit to the citizenry as a whole. The only entities that this could possibly benefit are large private corporations and government espionage against private citizens, both of which are largely detrimental to freedom, free speech, and innovation. The following points outline how these changes will negatively impact both individuals and businesses.

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 user's 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 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.

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

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: Lukasz

Last Name: Blaszczyk

Mailing Address: 6814 Donerail Trail

City: Tallahassee

Country: United States

State or Province: FL

ZIP/Postal Code: 32309

Email Address: lblaszczyk@gmail.com

Organization Name:

Comment: For almost the past decade I have been using Open Source router firmware software for connecting and securing my family's access to the internet from home. In the same way I can purchase a car and replace the radio, or purchase a laptop and replace the hard disk I expect to be able to purchase a router and replace the software.

Wonderful and dramatic leaps of innovation have occurred because of the ability for people with talent and great interest to understand and better the devices around them, not to mention new business models.

It would be a travesty to take away our rights to the very hardware we purchase with our own money. At that point we would not truly own the router, we would own a magical box that makes data move in and out.

In summary, it's my damn router, keep your damn hands out of it.

-- Thank you.

For almost the past decade I have been using Open Source router firmware software for connecting and securing my family's access to the internet from home. In the same way I can purchase a car and replace the radio, or purchase a laptop and replace the hard disk I expect to be able to purchase a router and replace the software.

Wonderful and dramatic leaps of innovation have occurred because of the ability for people with talent and great interest to understand and better the devices around them, not to mention new business models.

It would be a travesty to take away our rights to the very hardware we purchase with our own money. At that point we would not truly own the router, we would own a magical box that makes data move in and out.

In summary, it's my damn router, keep your damn hands out of it.

-- 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: Michael

Last Name: Di Domenico

Mailing Address: 2 Cambria Court

City: Hamilton

Country: United States

State or Province: NJ

ZIP/Postal Code: 08690

Email Address: mdidomenico@gmail.com

Organization Name: kc2ykj

Comment: Hacking of Wifi routers isn't really my business, so I don't have time to read through the lengthy reports below or around the web to verify the statements being circulated. However, I'm a little dismayed that the fcc would take such action against the hardware hacking community, amateur radio operators, and others. We should be encouraging hardware hacking not restricting it. Children of today and tomorrow need to be encouraged to take their devices farther then the original manufacturers intended. This action promotes eduction and reduces e-waste through reuse. To do otherwise sends a message to the next generation that electronics are basically throw away devices that are not intended to be touched and can only provide functionality that someone else claims is all you need. I would strongly urge the fcc to rethink any policies or legislation it plans to put forth now or in the furture which would restrict the rights of people to "hack" their devices.

Hacking of Wifi routers isn't really my business, so I don't have time to read through the lengthy reports below or around the web to verify the statements being circulated. However, I'm a little dismayed that the fcc would take such action against the hardware hacking community, amateur radio operators, and others. We should be encouraging hardware hacking not restricting it. Children of today and tomorrow need to be encouraged to take their devices farther then the original manufacturers intended. This action promotes eduction and reduces e-waste through reuse. To do otherwise sends a message to the next generation that electronics are basically throw away devices that are not intended to be touched and can only provide functionality that someone else claims is all you need. I would strongly urge the fcc to rethink any policies or legislation it plans to put forth now or in the furture which would restrict the rights of people to "hack" their 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: Alexey

Last Name: Vecheria

Mailing Address: 601 SSSR 63\57

City: Horlivka

Country: Ukraine

State or Province: Donetska obl

ZIP/Postal Code: 84607

Email Address: mr.a.vecheria@gmail.com

Organization Name:

Comment: Hey, what are you doing? , ?

Hey, what are you doing? , ?

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: Laurent

Last Name: M

Mailing Address: 24 alle Germinal

City: Chauconin-Neufmontiers

Country: France

State or Province: Ile-de-France

ZIP/Postal Code: 77124

Email Address: federalregister@lolomin.net

Organization Name:

Comment: I asked 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 the FCC should consider :

- 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.

Thanks for you reading.

Regards.

I asked 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 the FCC should consider :

- 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.

Thanks for you reading.

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: Francesco

Last Name: Zanini

Mailing Address: Via C. Roda 52

City: Curtatone

Country: Italy

State or Province: MN

ZIP/Postal Code: 46010

Email Address: francesco@zanini.me

Organization Name: zanini.me di Zanini Francesco

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

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

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

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

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

Thanks for reading.

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

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

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

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

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

Thanks for reading.

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: Eamon

Last Name: Ho

Mailing Address: 38 Walnut Ave

City: Atherton

Country: United States

State or Province: CA

ZIP/Postal Code: 94027

Email Address: eamon.ho@gmail.com

Organization Name:

Comment: This is an incredibly shortsighted ruling. Some of the best wifi platforms were developed as open source firmware that runs on commodity hardware (and were adopted in commercial products). Disallowing the modification of existing hardware forces these communities to build custom hardware, which is both cost prohibitive and would have crippled the development of these open source solutions which rely on large communities providing their free time and labor with minimal financial commitment. Alternatively, such development will simply go overseas, and we will effectively legislate ourselves out of this and similar evolving avenues and potential commercial derivatives. This establishes a poor precedent for similar projects which in aggregate have had significant net positive outcome in the engineering and scientific communities.

This is an incredibly shortsighted ruling. Some of the best wifi platforms were developed as open source firmware that runs on commodity hardware (and were adopted in commercial products). Disallowing the modification of existing hardware forces these communities to build custom hardware, which is both cost prohibitive and would have crippled the development of these open source solutions which rely on large communities providing their free time and labor with minimal financial commitment. Alternatively, such development will simply go overseas, and we will effectively legislate ourselves out of this and similar evolving avenues and potential commercial derivatives. This establishes a poor precedent for similar projects which in aggregate have had significant net positive outcome in the engineering and scientific communities.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Alex

Last Name: Temp

Mailing Address: tempalex@inbox.uz

City: Tashkent

Country: Uzbekistan

State or Province: Tash

ZIP/Postal Code: 114477

Email Address:

Organization Name:

Comment: . . . , !

. . . , !

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: Gerasimov

Mailing Address: Mozhaiskoe shosse, 42, 154

City: Odintsovo

Country: Russia

State or Province: Moskovskaya oblast

ZIP/Postal Code: 143007

Email Address: gr.evocatus@gmail.com

Organization Name:

Comment: I ask the members of FCC to refuse locking down computer devices with modular wireless radio. It would be a huge strike on freedom of speech all over the world.

I ask the members of FCC to refuse locking down computer devices with modular wireless radio. It would be a huge strike on freedom of speech all over the world.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: Davis

Mailing Address: 1180 Pascal Place

City: Norfolk

Country: United States

State or Province: VA

ZIP/Postal Code: 23502

Email Address:

Organization Name: Personal *AND* Lake Taylor Transitional Care Hospital

Comment: I am opposed to ANY proposal that would prevent or limit users from installing open-source firmware on WiFi routers. I do exactly that at home and at work and it is extremely important in both places. Open source firmware:

- 1) Prevents vendor lock-in and planned obsolescence
- 2) Gives me *MUCH* better security
- 3) Allows me to control the all features of my devices
- 4) Gives me a consistent user-interface across devices
- 5) Makes management of the devices easier and less costly
- 6) Provides updates with reasonable time periods
- 7) Ensures I can use the devices for much longer before they go obsolete
- 8) Makes the devices work faster
- 9) Gives far better logging, troubleshooting, and other features
- 10) Helps prevent corporate and government spying and back-doors, which should not only be illegal and unconstitutional, but are also extremely dangerous.

Please do not enact any type of regulation that would harm the ability for the open source community to extend their software and support to WiFi routers. Thank You!

-Mark A. Davis

Charter Director, TideWater Unix/Linux User's Group

Director of Information Systems, Lake Taylor Transitional Care Hospital

I am opposed to ANY proposal that would prevent or limit users from installing open-source firmware on WiFi routers.

I do exactly that at home and at work and it is extremely important in both places. Open source firmware:

- 1) Prevents vendor lock-in and planned obsolescence
- 2) Gives me *MUCH* better security
- 3) Allows me to control the all features of my devices
- 4) Gives me a consistent user-interface across devices
- 5) Makes management of the devices easier and less costly
- 6) Provides updates with reasonable time periods
- 7) Ensures I can use the devices for much longer before they go obsolete
- 8) Makes the devices work faster
- 9) Gives far better logging, troubleshooting, and other features

10) Helps prevent corporate and government spying and back-doors, which should not only be illegal and unconstitutional, but are also extremely dangerous.

Please do not enact any type of regulation that would harm the ability for the open source community to extend their software and support to WiFi routers. Thank You!

-Mark A. Davis

Charter Director, TideWater Unix/Linux User's Group

Director of Information Systems, Lake Taylor Transitional Care Hospital

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: Bill

Last Name: Harwell

Mailing Address: 404 Edgecrest Dr.

City: Birmingham

Country: United States

State or Province: AL

ZIP/Postal Code: 35209

Email Address:

Organization Name:

Comment: Please do not implement policy that would prevent the public from installing and modifying software on the computing devices that we own.

The appropriate way to deal with those who operate wireless equipment in bad faith is to seek out and fine those operators, not to impede the proper functioning of any radio-equipped computing equipment.

Such policy would leave all wireless network operators and users helpless to correct unpatched software vulnerabilities.

Please do not implement policy that would prevent the public from installing and modifying software on the computing devices that we own.

The appropriate way to deal with those who operate wireless equipment in bad faith is to seek out and fine those operators, not to impede the proper functioning of any radio-equipped computing equipment.

Such policy would leave all wireless network operators and users helpless to correct unpatched software vulnerabilities.

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: Kolichenkov

Mailing Address: noneedto

City: Lappeenranta

Country: Finland

State or Province: Etela-savo

ZIP/Postal Code: 222222222

Email Address: noneedto@enter.this

Organization Name: Computer science society

Comment: I am, as many other developers/users/companies, ask to not enforce rules that take away the ability of users to install the software of their choosing on their computing devices.

This makes order of magnitude more problems than any benefits.

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, as many other developers/users/companies, ask to not enforce rules that take away the ability of users to install the software of their choosing on their computing devices.

This makes order of magnitude more problems than any benefits.

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: Kermes

Last Name: Persialainen

Mailing Address: Main Street

City: Quebec

Country: Canada

State or Province: Nova Scotia

ZIP/Postal Code: 56780

Email Address:

Organization Name:

Comment: I often find that a wireless routed purchased has a bug or vulnerability and there just is no new firmware for older devices. Therefore open source firmware can be used for these devices to fix bugs and vulnerabilities.

I often find that a wireless routed purchased has a bug or vulnerability and there just is no new firmware for older devices. Therefore open source firmware can be used for these devices to fix bugs and vulnerabilities.

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: Timothy

Last Name: Rios

Mailing Address: 495 chestnut st.

City: ashland

Country: United States

State or Province: OR

ZIP/Postal Code: 97520

Email Address:

Organization Name:

Comment: Hello Sirs and Madams,

Please reconsider the inclusion of rules that bans the ability of users to make changes to the software of device that contain radio equipment.

This only effects the FCC's security of controlling rules. This will greatly effect the security of our nations communication resources (due to the slowness and unwillingness for manufactures to support "obsolete" devices).

This will also limit the development of new technologies to those large corporations that have no interest in improve our culture and emergency response. Devices like OpenBTS (an adaptable, improvisational cell phone tower), technique like mesh networks (ad hoc communication, especially useful in emergency situations) and operating systems like Linux and CyogenMod (that gives user the freedom over their data) would be greatly hindered in development and flexibility.

Thank you for your time and your service and please keep the citizens that will be effected by these decisions in mind.

Yours truly,

Timothy Rios

Hello Sirs and Madams,

Please reconsider the inclusion of rules that bans the ability of users to make changes to the software of device that contain radio equipment.

This only effects the FCC's security of controlling rules. This will greatly effect the security of our nations communication resources (due to the slowness and unwillingness for manufactures to support "obsolete" devices).

This will also limit the development of new technologies to those large corporations that have no interest in improve our culture and emergency response. Devices like OpenBTS (an adaptable, improvisational cell phone tower), technique like mesh networks (ad hoc communication, especially useful in emergency situations) and operating systems like Linux and CyogenMod (that gives user the freedom over their data) would be greatly hindered in development and flexibility.

Thank you for your time and your service and please keep the citizens that will be effected by these decisions in mind.

Yours truly,

Timothy Rios

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: Igor

Last Name: Sazonov

Mailing Address: 76-1-22 Garybaldy str.

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: 117393

Email Address: igor.g.sazonov@yandex.ru

Organization Name: MAMSY

Comment: Please do not do it!

Please do not do 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: Don

Last Name: Mahurin

Mailing Address: 732 Layton Ct

City: Santa Clara

Country: United States

State or Province: CA

ZIP/Postal Code: 95051

Email Address: dm@openright.org

Organization Name:

Comment: "A grantee must obtain an updated grant of certification for the addition of new device capabilities through software changes."

Hello,

I am concerned that such rules may prevent fair use of devices such as routers, which are commonly modified to have more software functionality, security or stability than originally shipped. As an engineer, I learned years ago, that factory software on routers is inadequate, and that open source replacement software such as OpenWRT provides a reasonable alternative to the factory software that may enhance the functionality, stability and security of the device.

Please consider the effect on of users of such devices who wish to make software changes to the device to utilize the full potential of such devices. If such modifications are disallowed, this will potentially reduce the usefulness and security of such devices, and increase waste due to discarded hardware.

If software modifications are disallowed, this follows a dangerous and wasteful trend of the consumer being locked out of software on consumer purchased computing devices. This trend is counterproductive, and does not benefit the consumer or society. Instead this trend encourages vendor hardware/software bundling, reduces competition and encourages disposable hardware.

"A grantee must obtain an updated grant of certification for the addition of new device capabilities through software changes."

Hello,

I am concerned that such rules may prevent fair use of devices such as routers, which are commonly modified to have more software functionality, security or stability than originally shipped. As an engineer, I learned years ago, that factory software on routers is inadequate, and that open source replacement software such as OpenWRT provides a reasonable alternative to the factory software that may enhance the functionality, stability and security of the device.

Please consider the effect on of users of such devices who wish to make software changes to the device to utilize the full potential of such devices. If such modifications are disallowed, this will potentially reduce the usefulness and security of such devices, and increase waste due to discarded hardware.

If software modifications are disallowed, this follows a dangerous and wasteful trend of the consumer being locked out of software on consumer purchased computing devices. This trend is counterproductive, and does not benefit the consumer or society. Instead this trend encourages vendor hardware/software bundling, reduces competition and encourages disposable hardware.

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: Matt

Last Name: Adams

Mailing Address: 2271 Marion St

City: North Bend

Country: United States

State or Province: OR

ZIP/Postal Code: 97459

Email Address: theseconddarkage@yahoo.com

Organization Name:

Comment: The proposed rules to prevent modification to devices if they have a "modular wireless radio" are disastrous. They would potentially:

Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes

Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

Discourage the development of alternative free and open source WiFi firmware, like OpenWrt

Ban installation of custom firmware on your Android phone

Prevent resellers from installing firmware or customizing routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

Thank you for considering these points.

The proposed rules to prevent modification to devices if they have a "modular wireless radio" are disastrous. They would potentially:

Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes

Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

Discourage the development of alternative free and open source WiFi firmware, like OpenWrt

Ban installation of custom firmware on your Android phone

Prevent resellers from installing firmware or customizing routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

Thank you for considering these points.

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: Sheppard

Mailing Address: 4624 N Huson St

City: Tacoma

Country: United States

State or Province: WA

ZIP/Postal Code: 98407

Email Address:

Organization Name:

Comment: This regulation would stifle innovation, make us less secure, and set back innovation in the United States decades.

This regulation would stifle innovation, make us less secure, and set back innovation in the United States decades.

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: Daniela

Last Name: Trinidad

Mailing Address: 3007 W 53RD ST

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60632

Email Address:

Organization Name:

Comment: Please do not do this. I like to modify my phone for more freedom to do what I want with it. Are you against freedom? Are you a communist?

Please do not do this. I like to modify my phone for more freedom to do what I want with it. Are you against freedom?
Are you a communist?

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: Jimmy

Last Name: Boone

Mailing Address: 10712 Buck Road

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32817

Email Address: ooberchicken@gmail.com

Organization Name:

Comment: Good morning,

I would Like to voice my disapproval of the proposed mandate to prevent the flashing of any device that contains a modular wireless radio. I feel that not only is this un-american, it is stifling to innovation and good ole tinkering around.

If I want to buy a router and flash it with a firmware of my choosing that is my right and choice, not yours.

Good morning,

I would Like to voice my disapproval of the proposed mandate to prevent the flashing of any device that contains a modular wireless radio. I feel that not only is this un-american, it is stifling to innovation and good ole tinkering around.

If I want to buy a router and flash it with a firmware of my choosing that is my right and choice, not yours.

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: Ivan

Last Name: Ivanov

Mailing Address: Russia

City: Russia

Country: Russia

State or Province: Russia

ZIP/Postal Code: 0000123456

Email Address:

Organization Name:

Comment: This is not good for geeks and software developers.

This is not good for geeks and software developers.

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: Lee

Last Name: Burt

Mailing Address: 1430 Woodside Glen Way

City: Sacramento

Country: United States

State or Province: CA

ZIP/Postal Code: 95833

Email Address: lburt@aperio.cc

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their own computing devices. Additional points of emphasis you should consider:

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

Please do not implement rules that take away the ability of users to install the software of their choosing on their own computing devices. Additional points of emphasis you should consider:

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: SHAUN

Last Name: St John

Mailing Address: 10373 North Sam Houston Pkwy E apt 815

City: Humble

Country: United States

State or Province: TX

ZIP/Postal Code: 77396

Email Address: aikman1890@yahoo.com

Organization Name:

Comment: Hello,

I need the ability to control my wireless network and the operating system at home. I work in an industry that is forever changing and need the ability to learn new technologies and be able to patch the new technologies if I find security holes. You can't prevent me from doing this on a device that I purchase for my personal use per the USA constitution. I have the right to install anything I want on computer hardware that I purchase.

Hello,

I need the ability to control my wireless network and the operating system at home. I work in an industry that is forever changing and need the ability to learn new technologies and be able to patch the new technologies if I find security holes. You can't prevent me from doing this on a device that I purchase for my personal use per the USA constitution. I have the right to install anything I want on computer hardware that I purchase.

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: Giovanni

Last Name: Hernandez

Mailing Address: 9027 SW 211th Lane

City: Miami

Country: United States

State or Province: FL

ZIP/Postal Code: 33189

Email Address:

Organization Name:

Comment: These are OUR DEVICES! Please do not limit what we can or can't do on them. Flashing custom firmware is a very common practice for just about any device you can think of. Custom firmware on our devices not only allows savvy consumers to increase the performance but it also increases the longevity of said items. It allows us to tinker with our devices, learn new ways to code/program, and teaches us the fundamental skills needed so supplement our growing need for technology in our day to day lives. The FCC should take notice of every time some proposal like this comes out into the light, it won't win. Even if it goes through, tinkerers and hobbyist WILL FIND A WAY to bypass whatever security crap is implemented. All you are going to have on your hands is angry citizens.

Please consider the above, from a hobbyist-tinkerer-college-student/grad-business owner. Thanks.

These are OUR DEVICES! Please do not limit what we can or can't do on them. Flashing custom firmware is a very common practice for just about any device you can think of. Custom firmware on our devices not only allows savvy consumers to increase the performance but it also increases the longevity of said items. It allows us to tinker with our devices, learn new ways to code/program, and teaches us the fundamental skills needed so supplement our growing need for technology in our day to day lives. The FCC should take notice of every time some proposal like this comes out into the light, it won't win. Even if it goes through, tinkerers and hobbyist WILL FIND A WAY to bypass whatever security crap is implemented. All you are going to have on your hands is angry citizens.

Please consider the above, from a hobbyist-tinkerer-college-student/grad-business owner. Thanks.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jordan

Last Name: Stewart

Mailing Address: jstewart0718@gmail.com

City: Ottawa

Country: Canada

State or Province: Ontario

ZIP/Postal Code: K2E 6J5

Email Address:

Organization Name:

Comment: Hello,

I am commenting to ask why a person should not be able to modify a device that they own, in their own home, when it does not seem to negatively affect anyone else. It seems like these rules would unjustly affect the open-source community, and would unjustly regulate the actions of the individual. Unless there is something about using open-source firmware that somehow negatively affects the community then what meaning is there in regulating it? If it negatively affects business somehow we should remember that there is no reason why business should take precedence, or have any special privileges, over anyone else.

I would really appreciate hearing why the FCC feels it is their duty to regulate this activity.

J.S.

Hello,

I am commenting to ask why a person should not be able to modify a device that they own, in their own home, when it does not seem to negatively affect anyone else. It seems like these rules would unjustly affect the open-source community, and would unjustly regulate the actions of the individual. Unless there is something about using open-source firmware that somehow negatively affects the community then what meaning is there in regulating it? If it negatively affects business somehow we should remember that there is no reason why business should take precedence, or have any special privileges, over anyone else.

I would really appreciate hearing why the FCC feels it is their duty to regulate this activity.

J.S.

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: Zych

Mailing Address: 205 Calvin

City: Savoy

Country: United States

State or Province: IL

ZIP/Postal Code: 61874

Email Address:

Organization Name:

Comment: Please do not implement rules that would deny users the right to install and run the software of their choosing (including and especially free software) on their computing devices.

Please do not implement rules that would deny users the right to install and run the software of their choosing (including and especially free software) on their computing 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: Elatia

Last Name: Grimshaw

Mailing Address: 1317 Butternut Ave

City: Royal Oak

Country: United States

State or Province: MI

ZIP/Postal Code: 48073

Email Address:

Organization Name:

Comment: Why do you want to have a rule against people modifying the routers that they purchased and installing open source firmware on them? Open source firmware does no harm.

Why do you want to have a rule against people modifying the routers that they purchased and installing open source firmware on them? Open source firmware does no harm.

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: Kirill

Last Name: Timofeev

Mailing Address: 4257 181st Pl SE

City: Issaquah

Country: United States

State or Province: WA

ZIP/Postal Code: 98027

Email Address:

Organization Name:

Comment: To whom it may concern.

This proposal if approved would have extremely negative effect on open source projects. In particular you wouldn't be able to install alternative open source operating systems (Linux, FreeBSD etc) on computers with wireless capabilities.

Please decline this proposal.

Thank you.

To whom it may concern.

This proposal if approved would have extremely negative effect on open source projects. In particular you wouldn't be able to install alternative open source operating systems (Linux, FreeBSD etc) on computers with wireless capabilities.

Please decline this proposal.

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: N/A

Last Name: N/A

Mailing Address: N/A

City: N/A

Country: United States

State or Province: IL

ZIP/Postal Code: 62234

Email Address:

Organization Name:

Comment: As an owner of a tech start up, I think this regulation restricts innovation from individuals while catering to existing big companies. This can promote anti-competitive behavior.

As an owner of a tech start up, I think this regulation restricts innovation from individuals while catering to existing big companies. This can promote anti-competitive behavior.

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: Morris

Mailing Address: 5036 25th St N

City: Arlington

Country: United States

State or Province: VA

ZIP/Postal Code: 22207

Email Address: dmorri17@masonlive.gmu.edu

Organization Name: null

Comment: First off, the summary should describe the changes to law proposed. As a citizen, I find the summary evasive. I hope Bernie gets elected.

Second, I feel I should be able to pull apart my electronics as long as I don't create interference. Why shouldn't I be allowed to turn my web-connected lightbulb into a propane-powered cheese grater?

If modification of Internet Of Things objects is restricted, it will stifle industry. Where would George Foreman be if he wasn't allowed to take a hammer to a waffle iron? A parkinsons clinic, that's where.

First off, the summary should describe the changes to law proposed. As a citizen, I find the summary evasive. I hope Bernie gets elected.

Second, I feel I should be able to pull apart my electronics as long as I don't create interference. Why shouldn't I be allowed to turn my web-connected lightbulb into a propane-powered cheese grater?

If modification of Internet Of Things objects is restricted, it will stifle industry. Where would George Foreman be if he wasn't allowed to take a hammer to a waffle iron? A parkinsons clinic, that's where.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nick

Last Name: Vitse

Mailing Address: 1677 2nd Ave

City: Grafton

Country: United States

State or Province: WI

ZIP/Postal Code: 53024

Email Address:

Organization Name:

Comment: With all due respect, I would ask that all rules be dropped from the proposed regulation that restrict the user's ability to modify firmware and software on radio-equipped devices.

Manufactures of such devices have consistently shown that they have no particular interest in providing actual support, bug fixes, or real updates to devices once they are sold. Consumers need the ability to manage such updates and fixes. In my opinion, the existence of aftermarket firmware such as DD-WRT is the only thing that even makes consumer-grade routers functional at all.

It seems the FCC's real concern is over user modification of radio power levels beyond legal limits. If this is the case, there should be much more elegant solutions available that would satisfy the FCC.

With all due respect, I would ask that all rules be dropped from the proposed regulation that restrict the user's ability to modify firmware and software on radio-equipped devices.

Manufactures of such devices have consistently shown that they have no particular interest in providing actual support, bug fixes, or real updates to devices once they are sold. Consumers need the ability to manage such updates and fixes. In my opinion, the existence of aftermarket firmware such as DD-WRT is the only thing that even makes consumer-grade routers functional at all.

It seems the FCC's real concern is over user modification of radio power levels beyond legal limits. If this is the case, there should be much more elegant solutions available that would satisfy the FCC.

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: Perriello

Mailing Address: Envisage

City: Ithaca

Country: United States

State or Province: NY

ZIP/Postal Code: 14850

Email Address:

Organization Name:

Comment: Without the ability to modify wireless device firmwares, I'm quite concerned this will lead to an insecure web. Without security updates, all flaws that are found will remain exploitable indefinitely.

Without the ability to modify wireless device firmwares, I'm quite concerned this will lead to an insecure web. Without security updates, all flaws that are found will remain exploitable indefinitely.