

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Kyle
Last Name: Tinker
Mailing Address: 4268 SW Averio Ln
City: Lees Summit
Country: United States
State or Province: MO
ZIP/Postal Code: 64082
Email Address: shamrock.computing@gmail.com
Organization Name:

Comment: As a developer of the open-source Tomato firmware, please refrain from implementing rules that take away from the ability of end users to install the software of choosing on their computing devices.

Router vendors frequently fail to install security updates in their routers, leaving millions vulnerable. The rules, if implemented as written, would cause companies to lock down these devices, preventing end users and open-source developers from fixing those security holes, making the internet less safe for everyone.

In addition, consumer-grade routers often have bugs in their WiFi implementations. The rule, as written, would ban us open-source developers from fixing those bugs by updating the drivers when the original manufacturers fail to do so.

Americans need the ability to flash custom firmware, fix bugs, and update security holes in their devices when the manufacturer chooses not to do so. Researchers rely on the existence of open-source devices in many cases to develop new networks and network protocols.

while it is critically important to protect airports and

As a developer of the open-source Tomato firmware, please refrain from implementing rules that take away from the ability of end users to install the software of choosing on their computing devices.

Router vendors frequently fail to install security updates in their routers, leaving millions vulnerable. The rules, if implemented as written, would cause companies to lock down these devices, preventing end users and open-source developers from fixing those security holes, making the internet less safe for everyone.

In addition, consumer-grade routers often have bugs in their WiFi implementations. The rule, as written, would ban us open-source developers from fixing those bugs by updating the drivers when the original manufacturers fail to do so.

Americans need the ability to flash custom firmware, fix bugs, and update security holes in their devices when the manufacturer chooses not to do so. Researchers rely on the existence of open-source devices in many cases to develop new networks and network protocols.

while it is critically important to protect airports and

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Mike
Last Name: Chick
Mailing Address: 1407 Rock Road
City: De Soto
Country: United States
State or Province: MO
ZIP/Postal Code: 63020
Email Address: mike@computer-partners.com
Organization Name: Computer Partners

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.

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.

-Mike

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.

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.

Submitter Info.txt

-Mike

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: David
Last Name: Lawrence
Mailing Address: 1028 Avery St. Unit 1
City: Parkersburg
Country: United States
State or Province: WV
ZIP/Postal Code: 26101
Email Address: Fenir8@gmail.com
Organization Name:

Comment: The continued openness of firmware is critical to not only user choice but also security.

An alternative method such as "signing" third party firmware as being compliant, or hardware level enforcement (rather than locking down the entire SOC) is really needed for this solution to be practical and not have a negative impact.

The continued openness of firmware is critical to not only user choice but also security.

An alternative method such as "signing" third party firmware as being compliant, or hardware level enforcement (rather than locking down the entire SOC) is really needed for this solution to be practical and not have a negative impact.

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Tim
Last Name: Jowers
Mailing Address: 227 Traditions Garden Lane
City: Wake Forest
Country: United States
State or Province: NC
ZIP/Postal Code: 27587
Email Address: timjowers@gmail.com
Organization Name: President

Comment: This is a blatant anti-competition move. It has nothing to do with better products, nor freedom. It should not be done and whomever proposed it should be dismissed from filing any future proposals.

This is a blatant anti-competition move. It has nothing to do with better products, nor freedom. It should not be done and whomever proposed it should be dismissed from filing any future proposals.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Christine
Last Name: Gann
Mailing Address: 2800 St. Paul Dr.
City: Santa Rosa
Country: United States
State or Province: CA
ZIP/Postal Code: 95405
Email Address:

Organization Name:

Comment: This comment is in response to the proposed rules for Equipment Authorization and Electronic Labeling for wireless Devices.

while the new rule does not mandate that equipment manufactures completely lock down their devices -- IN ACTUALITY that will be the result. The cheapest way for manufactures to comply with the proposed rule will be to simply lock down their devices so that no modifications will be possible.

This in turn will have following unintended consequences:

- * It will cripple wireless networking research since there will be no way to modify devices to test new firmwares

- * It will lead to unpactched security holes since independent investigation and modification of wifi firmware will not be possible. Furthermore, manufactures can not be relied for security research since they have little interest in supporting their devices after they are sold.

- * It will prevent the legitimate use wifi devices such as laptops, cell phones, wireless printers, and routers since manufactures will simply lock the consumer out of new devices. Consumers will be prevented from running the software/firmware of their choice on the devices they own.

Therefore, I urge the commission to reject the proposed rule. Freedom leads to innovation, while restrictions lead to stagnation.

This comment is in response to the proposed rules for Equipment Authorization and Electronic Labeling for Wireless Devices.

while the new rule does not mandate that equipment manufactures completely lock down their devices -- IN ACTUALITY that will be the result. The cheapest way for manufactures to comply with the proposed rule will be to simply lock down their devices so that no modifications will be possible.

This in turn will have following unintended consequences:

- * It will cripple wireless networking research since there will be no way to modify devices to test new firmwares

- * It will lead to unpactched security holes since independent investigation and modification of wifi firmware will not be possible. Furthermore, manufactures can not be relied for security research since they have little interest in supporting

Submitter Info.txt

their devices after they are sold.

* It will prevent the legitimate use wifi devices such as laptops, cell phones, wireless printers, and routers since manufactures will simply lock the consumer out of new devices. Consumers will be prevented from running the software/firmware of their choice on the devices they own.

Therefore, I urge the commission to reject the proposed rule. Freedom leads to innovation, while restrictions lead to stagnation.

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: Philip
Last Name: Mally
Mailing Address: 14491 Talking Pines Rd
City: Grass Valley
Country: United States
State or Province: CA
ZIP/Postal Code: 95945
Email Address: pmally@gmail.com
Organization Name: null

Comment: These new rules would make it nearly impossible to re-purpose and customize wireless Routers among many devices. Effectively killing a community and industry that for the past 10 years has been developing open source firmware which enables enterprise level features be available on consumer level electronics, thus making the internet more accessible and safe.

Why is this so important?

Well personally, most of my education surrounding linux and wireless networking comes from modifying used hardware which would otherwise be discarded as its software becomes obsolete.

Please don't take this away from us.

In most cases companies are focused on producing new products with great new features! At the moment some manufactures are even catering to open firmware enthusiasts. This will all disappear if this new ruling is passed. Current hardware quickly becomes obsolete.

The average person will just buy a brand new router not knowing that their old router probably had all the capabilities of the brand new one. Just in a different case.

Here are some examples of amazing projects made possible by open firmware. (This is a very small list)

BibleBox - Share the bible via battery powered wifi hotspot.
<http://biblebox.org/about-2/>

Standalone WiFi Fadecandy server (LED Controller)

https://www.youtube.com/watch?feature=player_embedded&v=4yeCbKATf2I#t=104

Wireless DSLR Camera Monitor

<https://youtu.be/xn1Yzt6zcpw>

<http://www.ds1rfilmnoob.com/>

All made possible by

OpenWRT

<http://wiki.openwrt.org/about/start>

DD-WRT

<http://www.dd-wrt.com/site/index>

Please Take this into consideration as a young person I was unable to ever afford enterprise level equipment but wanted to learn how to use. It was made possible by these projects dd-wrt. There some things that you simply cannot learn from college, where hands on experience is required.

Submitter Info.txt

Thank You
- Phil
KG6RIQ - My Amateur Radio Licence

These new rules would make it nearly impossible to re-purpose and customize wireless Routers among many devices. Effectively killing a community and industry that for the past 10 years has been developing open source firmware which enables enterprise level features be available on consumer level electronics, thus making the internet more accessible and safe.

Why is this so important?
Well personally, most of my education surrounding linux and wireless networking comes from modifying used hardware which would otherwise be discarded as its software becomes obsolete.
Please don't take this away from us.

In most cases companies are focused on producing new products with great new features! At the moment some manufactures are even catering to open firmware enthusiasts. This will all disappear if this new ruling is passed. Current hardware quickly becomes obsolete.

The average person will just buy a brand new router not knowing that their old router probably had all the capabilities of the brand new one. Just in a different case.

Here are some examples of amazing projects made possible by open firmware. (This is a very small list)
BibleBox - Share the bible via battery powered wifi hotspot.
<http://biblebox.org/about-2/>

Standalone WiFi Fadecandy server (LED Controller)
https://www.youtube.com/watch?feature=player_embedded&v=4yeCbKAtf2I#t=104

Wireless DSLR Camera Monitor
<https://youtu.be/xn1Yzt6zcpw>
<http://www.ds1rfilmnoob.com/>

All made possible by
OpenWRT
<http://wiki.openwrt.org/about/start>
DD-WRT
<http://www.dd-wrt.com/site/index>

Please Take this into consideration as a young person I was unable to ever afford enterprise level equipment but wanted to learn how to use. It was made possible by these projects dd-wrt. There some things that you simply cannot learn from college, where hands on experience is required.

Thank You
- Phil
KG6RIQ - My Amateur Radio Licence

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Nick
Last Name: Congleton
Mailing Address: 6 Fourth Street
City: Pequannock
Country: United States
State or Province: NJ
ZIP/Postal Code: 07440
Email Address: nick.congleton@gmail.com
Organization Name:

Comment: The rules presented by ET. Docket No. 15-170 are dangerous and pose a real threat to the rights of American consumers as well as to innovation and technology education. By forcing the implementation of DRM on devices with wireless antennae, the FCC would be setting a precedent wherein the lawful owners of such devices would, in practice, not own those devices. Rather, the devices would be owned and controlled by their manufacturers and the United States government.

The implementation of DRM on devices with wireless antennae would severely violate the rights of lawful device owners. It is within the fundamental rights of ownership that the owner of a device be able to modify and repair a device as he or she needs or sees fit. It is the right of the American consumer to be able to purchase a device that they may personally maintain, or, in effect, they are not granted ownership at the time of purchase and are merely leasing the device from the manufacturer. Such an informal lease agreement is deliberately deceptive and directly results in the exploitation of the consumer. In this situation, the consumer is bound to the manufacturer for the duration of the device's life span as determined by the manufacturer and not afforded the right to choose repair and maintenance services as they see fit based upon the present market. Additionally, this opens up the functionality of the device to be modified by the manufacturer or authorized third parties without the knowledge or consent of the supposed owner. All of this, in any light, amounts to a clearly anti-consumer set of restrictions. There has been a strong push in this country in recent years towards STEM education.

This is a large step forward as there has been a lack of adequate technology education, which is clearly reflected in the lack of qualified employees needed to meet the demands of the technology job market. With such an emphasis on preparing future generations for the rapidly evolving technology field, it would only stand to reason that anything and everything would be done to encourage young Americans to experiment with and learn from the technology available to them. Locking down devices with DRM inhibits the ability for young people, or anyone, to explore and learn. Personal exploration and hands on learning are crucial to developing a broad interest in learning technology and doing so from an early age. Free and open source software is a large part of this picture. Open source software allows an individual to examine the inner workings of a piece of software and gain a greater understanding of it. Open source also allows for a low barrier to access the same software used by top technology companies, often at no cost. The low to non-existent cost of open source software, especially when used through the Linux operating system, is critical in making technology accessible to people of all socioeconomic backgrounds. ET. Docket No. 15-170 could severely inhibit or entirely remove the ability to install and benefit from open source software like Linux, a major setback in preparing the next generation for the technology industry. ET. Docket No. 15-170, if passed, will have a severely negative impact on this country. It will stifle the ability of individuals to learn from their own devices and impede the growth of the technology industry. It violates the rights of the American consumer and flies in the face of the American free market. Do not approve ET. Docket No. 15-170. There are other ways to regulate wireless frequencies.

Submitter Info.txt

The rules presented by ET. Docket No. 15-170 are dangerous and pose a real threat to the rights of American consumers as well as to innovation and technology education. By forcing the implementation of DRM on devices with wireless antennae, the FCC would be setting a precedent wherein the lawful owners of such devices would, in practice, not own those devices. Rather, the devices would be owned and controlled by their manufacturers and the United States government.

The implementation of DRM on devices with wireless antennae would severely violate the rights of lawful device owners. It is within the fundamental rights of ownership that the owner of a device be able to modify and repair a device as he or she needs or sees fit. It is the right of the American consumer to be able to purchase a device that they may personally maintain, or, in effect, they are not granted ownership at the time of purchase and are merely leasing the device from the manufacturer. Such an informal lease agreement is deliberately deceptive and directly results in the exploitation of the consumer. In this situation, the consumer is bound to the manufacturer for the duration of the device's life span as determined by the manufacturer and not afforded the right to choose repair and maintenance services as they see fit based upon the present market. Additionally, this opens up the functionality of the device to be modified by the manufacturer or authorized third parties without the knowledge or consent of the supposed owner. All of this, in any light, amounts to a clearly anti-consumer set of restrictions. There has been a strong push in this country in recent years towards STEM education.

This is a large step forward as there has been a lack of adequate technology education, which is clearly reflected in the lack of qualified employees needed to meet the demands of the technology job market. With such an emphasis on preparing future generations for the rapidly evolving technology field, it would only stand to reason that anything and everything would be done to encourage young Americans to experiment with and learn from the technology available to them. Locking down devices with DRM inhibits the ability for young people, or anyone, to explore and learn. Personal exploration and hands on learning are crucial to developing a broad interest in learning technology and doing so from an early age. Free and open source software is a large part of this picture. Open source software allows an individual to examine the inner workings of a piece of software and gain a greater understanding of it. Open source also allows for a low barrier to access the same software used by top technology companies, often at no cost. The low to non-existent cost of open source software, especially when used through the Linux operating system, is critical in making technology accessible to people of all socioeconomic backgrounds. ET. Docket No. 15-170 could severely inhibit or entirely remove the ability to install and benefit from open source software like Linux, a major setback in preparing the next generation for the technology industry. ET. Docket No. 15-170, if passed, will have a severely negative impact on this country. It will stifle the ability of individuals to learn from their own devices and impede the growth of the technology industry. It violates the rights of the American consumer and flies in the face of the American free market. Do not approve ET. Docket No. 15-170. There are other ways to regulate wireless frequencies.

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: John
Last Name: Madden
Mailing Address: 12118 E 75th St
City: Indianapolis
Country: United States
State or Province: IN
ZIP/Postal Code: 46236
Email Address: jmadden@freelists.org
Organization Name: FreeLists

Comment: Custom modifications, tinkering, hobbyist-level and in some cases professional-level modification of OEM-distributed hardware is at the very roots of the computing industry and rules that would prevent this would have a detrimental affect on technology in the United States. The proposed rules, as written, would have prevented me from installing Linux or any other non-OEM operating system on the very computer I'm using to submit this comment. That alone is a frightening thought. Please spare consumer control of the devices we purchase and help maintain the precarious balance that currently (and sometimes, barely) exists between consumers and hardware manufacturers.

Custom modifications, tinkering, hobbyist-level and in some cases professional-level modification of OEM-distributed hardware is at the very roots of the computing industry and rules that would prevent this would have a detrimental affect on technology in the United States. The proposed rules, as written, would have prevented me from installing Linux or any other non-OEM operating system on the very computer I'm using to submit this comment. That alone is a frightening thought. Please spare consumer control of the devices we purchase and help maintain the precarious balance that currently (and sometimes, barely) exists between consumers and hardware manufacturers.

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: Richard
Last Name: Zurita
Mailing Address: 3042 Koontz Lane Reseda, CA 91335
City: Reseda
Country: United States
State or Province: CA
ZIP/Postal Code: 91335
Email Address:

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.

As libreplanet states:

- 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 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 computing devices.

As libreplanet states:

- 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 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 Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Joachim
Last Name: Fenkes
Mailing Address: Beim Herbstenhof 48
City: Tuebingen
Country: Germany
State or Province: BW
ZIP/Postal Code: 72076
Email Address: fcclockdown@dojoe.net
Organization Name:

Comment: I am extremely worried about the proposed lockdown of wireless device firmware. While I understand the motivation to keep the spectrum clean, this would mean an end to free and open operating systems on wireless devices like internet routers.

Although the proposal only refers to the wireless device itself, leaving a possibility to have a locked-down wireless radio controlled by a FOSS operating system, there is very little reason to believe any manufacturer would be willing to take on the additional costs incurred by such an approach.

In Germany, for example, we have the Freifunk project, aiming to provide a free mesh network to anyone and already successfully covering a wide area of Germany, purely on volunteer work. The project is based on off-the-shelf wireless routers running a special version of the open firmware OpenWRT. If future routers were firmware-locked, projects like Freifunk would not be possible any longer.

Furthermore, power users like to replace the notoriously badly maintained router firmware with a FOSS firmware like OpenWRT that is independently maintained and receives regular security updates. In times where router-based botnets are a very real threat, it would be irresponsible to prevent people from caring about the security of their devices.

Although the FCC ruling only covers the USA, again it is unlikely in practice that manufacturers would produce different router models for the US and the rest of the world, and much more likely they would just lock down the firmware everywhere.

I agree that keeping the spectrum clean is a goal worth achieving, but in this day and age, requiring device manufacturers to prevent firmware modification is the wrong way to achieve that goal.

Best regards
Joachim Fenkes

I am extremely worried about the proposed lockdown of wireless device firmware. While I understand the motivation to keep the spectrum clean, this would mean an end to free and open operating systems on wireless devices like internet routers.

Although the proposal only refers to the wireless device itself, leaving a possibility to have a locked-down wireless radio controlled by a FOSS operating system, there is very little reason to believe any manufacturer would be willing to take on the additional costs incurred by such an approach.

In Germany, for example, we have the Freifunk project, aiming to provide a free mesh network to anyone and already successfully covering a wide area of Germany, purely

Submitter Info.txt

on volunteer work. The project is based on off-the-shelf wireless routers running a special version of the open firmware OpenWRT. If future routers were firmware-locked, projects like Freifunk would not be possible any longer.

Furthermore, power users like to replace the notoriously badly maintained router firmware with a FOSS firmware like OpenWRT that is independently maintained and receives regular security updates. In times where router-based botnets are a very real threat, it would be irresponsible to prevent people from caring about the security of their devices.

Although the FCC ruling only covers the USA, again it is unlikely in practice that manufacturers would produce different router models for the US and the rest of the world, and much more likely they would just lock down the firmware everywhere.

I agree that keeping the spectrum clean is a goal worth achieving, but in this day and age, requiring device manufacturers to prevent firmware modification is the wrong way to achieve that goal.

Best regards
Joachim Fenkes

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Shawne
Last Name: Perkins
Mailing Address: P.O. Box 117
City: Greenfield Center
Country: United States
State or Province: NY
ZIP/Postal Code: 12833
Email Address: yellnomore@me.com
Organization Name:
Comment: Dear FCC,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. These restrictions concern me for the following reasons:

1. Wireless networking research depends on the ability of researchers and students to investigate and modify devices they own.
2. Regular people need the ability to fix security holes in their devices when the manufacturer chooses to not do so. The lack of Android phone carrier supplied updates are a perfect example.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Not fixing vendor security holes fuels cyberthreats.
5. 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. This is simply a violation of our right to private property and our fourth amendment right to be secure in their persons, houses, papers, and effects.

Sincerely,
Shawne Perkins

Dear FCC,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. These restrictions concern me for the following reasons:

1. Wireless networking research depends on the ability of researchers and students to investigate and modify devices they own.
2. Regular people need the ability to fix security holes in their devices when the manufacturer chooses to not do so. The lack of Android phone carrier supplied updates are a perfect example.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Not fixing vendor security holes fuels cyberthreats.
5. 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. This is simply a violation of our right to private property and our fourth amendment right to be secure in their persons, houses, papers, and effects.

Sincerely,
Shawne Perkins

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: John

Last Name: Scott

Mailing Address: 547 Pratt Trlr. 77

City: Greenfield

Country: United States

State or Province: IN

ZIP/Postal Code: 46140

Email Address: lorenzo567@outlook.com

Organization Name:

Comment: This denies users freedom to run their software on their own hardware, and applying this set of rules to every Wi-Fi device in America is just wrong. This denies Americans freedom and puts unneeded restrictions on personal devices in the Land of the Free. Laws that create this much controversy shouldn't be considered, and it's best for everyone that you stop restricting devices thinking you're making the world safer. The NSA spies on Americans' devices, only for the NSA to later spy illegally. Broad, restrictive laws that apply to an enormous number of devices in a region as large as the United States should not be tolerated.

This denies users freedom to run their software on their own hardware, and applying this set of rules to every Wi-Fi device in America is just wrong. This denies Americans freedom and puts unneeded restrictions on personal devices in the Land of the Free. Laws that create this much controversy shouldn't be considered, and it's best for everyone that you stop restricting devices thinking you're making the world safer. The NSA spies on Americans' devices, only for the NSA to later spy illegally. Broad, restrictive laws that apply to an enormous number of devices in a region as large as the United States should not be tolerated.

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Christopher
Last Name: Flusche
Mailing Address: 3616 Silverado Trail
City: Roanoke
Country: United States
State or Province: TX
ZIP/Postal Code: 76262

Email Address:

Organization Name:

Comment: I completely disagree with the requirements of this rule. I DO NOT want these restrictions placed on my wireless devices, or any wireless devices. DO NOT adopt this rule.

I completely disagree with the requirements of this rule. I DO NOT want these restrictions placed on my wireless devices, or any wireless devices. DO NOT adopt this rule.

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Shashank
Last Name: Sabniveesu
Mailing Address: 2872 University Avenue, Apt# A
City: Morgantown
Country: United States
State or Province: WV
ZIP/Postal Code: 26505
Email Address: shashank@linux.com
Organization Name: West Virginia University
Comment: Dear FCC,

I'm Shashank Sabniveesu, a Graduate Research Assistant working in the field of Wireless Networking at university.

The principles of user choice and control are vitally important for a vibrant wireless ecosystem. But as written, the NPRM threatens to undermine these ideals by limiting what users can do with their devices. That's a concern, because I want to be able to modify (and/or update) my own wireless software not invest in specialized devices to let me work.

The draft rules could enable device manufacturers to forbid third-party software, which would keep me from using my custom wireless configuration.

The ability to modify the firmware let us study various untested protocols and standards using a normal wireless device. Preventing such modifications would seriously handicap our ability to experiment.

Apart from the research perspectives, as a normal user of a wireless device, I expect to do simple changes to my router's administration interface which the manufacturer didn't care to implement.

In either case, I am not intending any damage to other transmissions around me and hence I deserve the freedom to better my life with the knowledge I acquire.

Sincerely,
Shashank Sabniveesu
2872 University Avenue, Apt# A
Morgantown, WV 26505

Dear FCC,

I'm Shashank Sabniveesu, a Graduate Research Assistant working in the field of Wireless Networking at university.

The principles of user choice and control are vitally important for a vibrant wireless ecosystem. But as written, the NPRM threatens to undermine these ideals by limiting what users can do with their devices. That's a concern, because I want to be able to modify (and/or update) my own wireless software not invest in specialized devices to let me work.

The draft rules could enable device manufacturers to forbid third-party software, which would keep me from using my custom wireless configuration.

Submitter Info.txt

The ability to modify the firmware let us study various untested protocols and standards using a normal wireless device. Preventing such modifications would seriously handicap our ability to experiment.

Apart from the research perspectives, as a normal user of a wireless device, I expect to do simple changes to my router's administration interface which the manufacturer didn't care to implement.

In either case, I am not intending any damage to other transmissions around me and hence I deserve the freedom to better my life with the knowledge I acquire.

Sincerely,
Shashank Sabniveesu
2872 University Avenue, Apt# A
Morgantown, WV 26505

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: Zach
Last Name: Zitterkopf
Mailing Address: PO Box 95405
City: South Jordan
Country: United States
State or Province: UT
ZIP/Postal Code: 84095
Email Address:
Organization Name:

Comment:

Please reject the ,,Equipment Authorization and Electronic Labeling for Wireless Devices'' rule. Please do not impose additional rules and reductions of freedom on Americans which will prohibit consumers of equipment, which may or may not have an SDR (Software Defined Radio), to utilize their equipment for their needs and lawful purposes.

801.11 wifi router offerings are frequently refreshed by their Manufacturers, which renders units which may only be a few years old, obsolete. When consumers have the freedom to change the programming of their units, several positive things happen:

- Consumers have the freedom to use their units for as long as they need them, and are not being compelled by a manufacturer to upgrade on the manufacturer's schedule and terms.

- Consumers and Community have the ability to resolve bugs and security flaws which the manufacturer may be unable or unwilling to provide. Such patches and updates contribute to the electronic security of our nation.

- Permitting seasoned and aspiring engineers the ability to modify and study the operation of units with an SDR provides valuable learning opportunities and gives them freedom to create positive, inventive, and innovative uses which the manufacturer may have been unable or unwilling to provide.

I urge you strongly to reject the proposed ,,Equipment Authorization and Electronic Labeling for wireless Devices'' rule.

Please reject the ,,Equipment Authorization and Electronic Labeling for Wireless Devices'' rule. Please do not impose additional rules and reductions of freedom on Americans which will prohibit consumers of equipment, which may or may not have an SDR (Software Defined Radio), to utilize their equipment for their needs and lawful purposes.

801.11 wifi router offerings are frequently refreshed by their Manufacturers, which renders units which may only be a few years old, obsolete. When consumers have the freedom to change the programming of their units, several positive things happen:

- Consumers have the freedom to use their units for as long as they need them, and are not being compelled by a manufacturer to upgrade on the manufacturer's schedule and terms.

Submitter Info.txt

- Consumers and Community have the ability to resolve bugs and security flaws which the manufacturer may be unable or unwilling to provide. Such patches and updates contribute to the electronic security of our nation.

- Permitting seasoned and aspiring engineers the ability to modify and study the operation of units with an SDR provides valuable learning opportunities and gives them freedom to create positive, inventive, and innovative uses which the manufacturer may have been unable or unwilling to provide.

I urge you strongly to reject the proposed ,,Equipment Authorization and Electronic Labeling for Wireless Devices'' rule.

Submitter Info.txt

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: Reid
Last Name: Conti
Mailing Address: 3732 Page St
City: Redwood City
Country: United States
State or Province: CA
ZIP/Postal Code: 94063
Email Address:

Organization Name:

Comment: Please do not take any action which harms the ability of companies or users to install Free Software on wireless devices. I've been working with free software for 20 years, and have have built a career around open-source products.

True innovation is happening in the open source movement, and entire livelihoods, not to mention the bulk of innovation in the technology industry, revolve around Free and Open Source Software (FOSS).

Please do not take any action which harms the ability of companies or users to install Free Software on wireless devices. I've been working with free software for 20 years, and have have built a career around open-source products.

True innovation is happening in the open source movement, and entire livelihoods, not to mention the bulk of innovation in the technology industry, revolve around Free and Open Source Software (FOSS).

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Wayne
Last Name: Workman
Mailing Address: 1480 Mundy Dr.
City: Florissant
Country: United States
State or Province: MO
ZIP/Postal Code: 63031
Email Address: wayne.workman2012@gmail.com
Organization Name:

Comment: I am developing a specialized capture portal for flashable router/access points. This specialized software is to promote businesses to share their WiFi with customers and generate revenue from sharing.

The wifi is ad-based, requiring a user to watch an ad to use the guest WiFi, and every 30 minutes thereafter. This will generate revenue for businesses that already share free wifi with customers, and will lower the cost of businesses sharing wifi, therefore promoting free and open WiFi to the general public, and drawing in more customers for said businesses.

If the proposed rule by the FCC is implemented, this will destroy my business plans, it will destroy the potential for a business to easily generate revenue by sharing WiFi. It will destroy the low-entry-cost that I plan to make available to all businesses everywhere for free.

Do not pass this rule. It will inhibit technological advancements, stunt potential business models, slow the adoption of free WiFi among businesses, and raise the cost of a business implementing free guest WiFi.

This proposed rule is a terrible rule - and it will destroy all the work I've conducted in my private time over the past several months.

There are many, many other very valid and important reasons why this proposed rule is terrible, but these reasons listed here are what's most important to me.

I am developing a specialized capture portal for flashable router/access points. This specialized software is to promote businesses to share their WiFi with customers and generate revenue from sharing.

The wifi is ad-based, requiring a user to watch an ad to use the guest WiFi, and every 30 minutes thereafter. This will generate revenue for businesses that already share free wifi with customers, and will lower the cost of businesses sharing wifi, therefore promoting free and open WiFi to the general public, and drawing in more customers for said businesses.

If the proposed rule by the FCC is implemented, this will destroy my business plans, it will destroy the potential for a business to easily generate revenue by sharing WiFi. It will destroy the low-entry-cost that I plan to make available to all businesses everywhere for free.

Do not pass this rule. It will inhibit technological advancements, stunt potential business models, slow the adoption of free WiFi among businesses, and raise the cost of a business implementing free guest WiFi.

Submitter Info.txt

This proposed rule is a terrible rule - and it will destroy all the work I've conducted in my private time over the past several months.

There are many, many other very valid and important reasons why this proposed rule is terrible, but these reasons listed here are what's most important to me.