

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: Anonymoose

Last Name: checkyourrecordsnsa

Mailing Address: youknowitNSA

City: no

Country: Thailand

State or Province: never

ZIP/Postal Code: no

Email Address:

Organization Name:

Comment: You tried SOPA and all that garbage, please stop trying to take the freedoms of everyone on the planet, you and your privacy bombardment is bullshit, what will this accomplish huh? It will allow you cunts to monitor everyone on the planet, but restricting firmware updates? you think that will solve anything, just let the hackers get an easy backdoor since you can't update it without huge restrictions.

You think spying on people is really helping in any way? we all know you just want money, and you spy so you can advertise, please go fuck yourselves, i hope you and your shitty laws get overturned in the rest of the world, where money doesn't decide everything since there's people here ready to put others's needs over theirs.

Fuck your bullshit laws and your spying, it won't help you in any way.

You tried SOPA and all that garbage, please stop trying to take the freedoms of everyone on the planet, you and your privacy bombardment is bullshit, what will this accomplish huh? It will allow you cunts to monitor everyone on the planet, but restricting firmware updates? you think that will solve anything, just let the hackers get an easy backdoor since you can't update it without huge restrictions.

You think spying on people is really helping in any way? we all know you just want money, and you spy so you can advertise, please go fuck yourselves, i hope you and your shitty laws get overturned in the rest of the world, where money doesn't decide everything since there's people here ready to put others's needs over theirs.

Fuck your bullshit laws and your spying, it won't help you in any way.

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: Klaus

Last Name: Lichtenwalder

Mailing Address: Sedanstr. 3

City: Munich

Country: Germany

State or Province: BY

ZIP/Postal Code: 81667

Email Address: lichtenwalder@acm.org

Organization Name:

Comment: Ladies an Gentlemen,

I'm afraid the proposed ruling will have a very detrimental effect on security of users as well as innovation for the industry.

- If one isn't able to install alternative firmware on routers, the fixing of security holes is up to the mercy of the manufacturer, who might not be interested any longer in this device. So either people have glaring security holes, or are adding to the ever growing electronic waste, having to buy new equipment.
- This will hinder innovation, as new features can often only be added later, by other sources as the manufacturer (first, until he realizes this will be valuable)
- Not anticipated features might not be implemented, or the burden to get these features will be extremely high.
- manufacturers often use open source tools and operating systems to keep their costs down and so can sell these devices for an affordable price. Manufacturers will have to cease collaboration with the open source developers and have to spend real money for these devices. Which may lead to a shortage on new devices, as it might become too expensive for many manufacturers.

Ladies an Gentlemen,

I'm afraid the proposed ruling will have a very detrimental effect on security of users as well as innovation for the industry.

- If one isn't able to install alternative firmware on routers, the fixing of security holes is up to the mercy of the manufacturer, who might not be interested any longer in this device. So either people have glaring security holes, or are adding to the ever growing electronic waste, having to buy new equipment.
- This will hinder innovation, as new features can often only be added later, by other sources as the manufacturer (first, until he realizes this will be valuable)
- Not anticipated features might not be implemented, or the burden to get these features will be extremely high.
- manufacturers often use open source tools and operating systems to keep their costs down and so can sell these devices for an affordable price. Manufacturers will have to cease collaboration with the open source developers and have to spend real money for these devices. Which may lead to a shortage on new devices, as it might become too expensive for many manufacturers.

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: Relyea

Mailing Address: 416 Lola Ave

City: Pasadena

Country: United States

State or Province: CA

ZIP/Postal Code: 91107

Email Address: drrelyea@gmail.com

Organization Name:

Comment: Please verify that your proposed ruleset does not prevent researchers from loading Linux onto PCs. I am a lead data scientist but also publish research I've done on a PC at home running Linux. Nothing nefarious, and the furthest thing in the world from an attempt to broadcast in illegal (reserved) parts of the spectrum.

Your rules, as currently written, might be very broadly interpreted to prevent me from running Linux on a PC. (Specifically, they might prevent open source software installation in general.) This would be a terrible blow to research in the US.

Please rewrite your ruleset to cover very specific situations. Absolutely nobody will care if you continuously rewrite your ruleset to prevent jerks from broadcasting into reserved parts of the spectrum. Pretty much every researcher in the entire country will mind if you pass these rules as written.

Please verify that your proposed ruleset does not prevent researchers from loading Linux onto PCs. I am a lead data scientist but also publish research I've done on a PC at home running Linux. Nothing nefarious, and the furthest thing in the world from an attempt to broadcast in illegal (reserved) parts of the spectrum.

Your rules, as currently written, might be very broadly interpreted to prevent me from running Linux on a PC. (Specifically, they might prevent open source software installation in general.) This would be a terrible blow to research in the US.

Please rewrite your ruleset to cover very specific situations. Absolutely nobody will care if you continuously rewrite your ruleset to prevent jerks from broadcasting into reserved parts of the spectrum. Pretty much every researcher in the entire country will mind if you pass these rules as written.

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: Jake

Last Name: Buroker

Mailing Address: 226 W 16th St. Apt. E1

City: New York

Country: United States

State or Province: NY

ZIP/Postal Code: 10011

Email Address: jakeburoker@gmail.com

Organization Name: Sandbox Studio

Comment: I implore the FCC to abandon implementing rules that take away the ability of users to install the software of their choosing on their computing devices.

I've been employed in the private IT sector for 22 years, and, in that time, have frequently depended on my ability to flash custom firmware to all manner of devices--including many devices with radios, which are now being targeted for lock-down by this proposed rule. Hardware manufacturers are infamous for abandoning their equipment long before it has truly reached end of life. Modifying and/or flashing custom firmware to plug security holes left unpatched by the hardware manufacturer is vital to network security, and helps to keep devices in use instead of filling up landfills with toxic materials.

Additionally, 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. And 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. Examples of this can be found far and wide, with the most cursory of investigation into the OpenWRT / DD-WRT / Tomato firmware communities (as well as the commercialized offshoots of those open source projects.)

For the sake of consumer safety and security, to prevent gross electronic waste due to end-of-life by way of manufacturer-support abandonment, and to avoid stifling research and innovation, I again implore the FCC to abandon this proposed rule.

I implore the FCC to abandon implementing rules that take away the ability of users to install the software of their choosing on their computing devices.

I've been employed in the private IT sector for 22 years, and, in that time, have frequently depended on my ability to flash custom firmware to all manner of devices--including many devices with radios, which are now being targeted for lock-down by this proposed rule. Hardware manufacturers are infamous for abandoning their equipment long before it has truly reached end of life. Modifying and/or flashing custom firmware to plug security holes left unpatched by the hardware manufacturer is vital to network security, and helps to keep devices in use instead of filling up landfills with toxic materials.

Additionally, 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. And 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. Examples of this can be found far and wide, with the most cursory of investigation into the OpenWRT / DD-WRT / Tomato firmware communities (as well as the commercialized offshoots of those open source projects.)

For the sake of consumer safety and security, to prevent gross electronic waste due to end-of-life by way of manufacturer-support abandonment, and to avoid stifling research and innovation, I again implore the FCC to abandon this proposed rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Anonymous

Mailing Address: 921 Dewey

City: Ann Arbor

Country: United States

State or Province: MI

ZIP/Postal Code: 48102

Email Address: null

Organization Name: null

Comment: Its flabbergasting that someone could dream that in a world that is increasingly digitized it would be a good idea to prevent people from using safe systems, especially if they own it. In no ideal world should anyone be subject to such tyranny over their property. Freedom as the cost of protection is non freedom at all.

Its flabbergasting that someone could dream that in a world that is increasingly digitized it would be a good idea to prevent people from using safe systems, especially if they own it. In no ideal world should anyone be subject to such tyranny over their property. Freedom as the cost of protection is non freedom at all.

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: Barton

Last Name: Chittenden

Mailing Address: 3910 Handley Ave

City: Louisville

Country: United States

State or Province: KY

ZIP/Postal Code: 40218

Email Address: bartonski@gmail.com

Organization Name: null

Comment: Per a thread in the news aggregator Reddit

([https://www.reddit.com/r/technology/comments/3jsiex/the\\_fcc\\_wants\\_to\\_prevent\\_you\\_from\\_installing/](https://www.reddit.com/r/technology/comments/3jsiex/the_fcc_wants_to_prevent_you_from_installing/)), it seems that the FCC would like to enact rules to disable the ability to replace the firmware on wireless routers. As a blanket statement, I'm against this -- I use open source firmware (DD-WRT and OpenWRT) on several of my routers, and I would be very disappointed if this was no longer an option.

The commenter here

([https://www.reddit.com/r/technology/comments/3jsiex/the\\_fcc\\_wants\\_to\\_prevent\\_you\\_from\\_installing/cus9wt6](https://www.reddit.com/r/technology/comments/3jsiex/the_fcc_wants_to_prevent_you_from_installing/cus9wt6)) makes the following statement:

"Adding the ability to only verify the firmware itself in such an environment is something that would require additional hardware effort. Therefore, it is much more likely that router manufacturers start to tivoize the thing, signing the entire blob (firmware + OS). This is the problem. The FCC only put in some vague notes that DD-WRT and the like should still be usable. It must be explicitly requested that only the actual radio firmware itself is verified, and that the rest must not be part of the verification."

As such, I would like to ensure that this language is included. Having the FCC have control of the radio frequency is fine by me. Honestly, I would prefer to have a bit of discretion -- if I've got a wireless router in a barn, and I know that I'm not going to hurt anyone by boosting the power, I'd like to have the ability to do that, but I understand that wireless routers aren't smart enough to distinguish between when they're in the hands of someone who knows what they're doing in a barn and someone who is washing out other people's wifi signals in an apartment complex... so I'm willing to cede some control over the radio transmission to the FCC -- but blocking the installation of all firmware, even by virtue of giving router manufacturers the excuse to lock consumers out of the router is not an option. If the firmware controlling the radio is to be signed, this must be a separate sub-system, and I don't want to hear router manufacturers whining about it.

Per a thread in the news aggregator Reddit

([https://www.reddit.com/r/technology/comments/3jsiex/the\\_fcc\\_wants\\_to\\_prevent\\_you\\_from\\_installing/](https://www.reddit.com/r/technology/comments/3jsiex/the_fcc_wants_to_prevent_you_from_installing/)), it seems that the FCC would like to enact rules to disable the ability to replace the firmware on wireless routers. As a blanket statement, I'm against this -- I use open source firmware (DD-WRT and OpenWRT) on several of my routers, and I would be very disappointed if this was no longer an option.

The commenter here

([https://www.reddit.com/r/technology/comments/3jsiex/the\\_fcc\\_wants\\_to\\_prevent\\_you\\_from\\_installing/cus9wt6](https://www.reddit.com/r/technology/comments/3jsiex/the_fcc_wants_to_prevent_you_from_installing/cus9wt6))

makes the following statement:

"Adding the ability to only verify the firmware itself in such an environment is something that would require additional hardware effort. Therefore, it is much more likely that router manufacturers start to tivoize the thing, signing the entire blob (firmware + OS). This is the problem. The FCC only put in some vague notes that DD-WRT and the like should still be usable. It must be explicitly requested that only the actual radio firmware itself is verified, and that the rest must not be part of the verification."

As such, I would like to ensure that this language is included. Having the FCC have control of the radio frequency is fine by me. Honestly, I would prefer to have a bit of discretion -- if I've got a wireless router in a barn, and I know that I'm not going to hurt anyone by boosting the power, I'd like to have the ability to do that, but I understand that wireless routers aren't smart enough to distinguish between when they're in the hands of someone who knows what they're doing in a barn and someone who is washing out other people's wifi signals in an apartment complex... so I'm willing to cede some control over the radio transmission to the FCC -- but blocking the installation of all firmware, even by virtue of giving router manufacturers the excuse to lock consumers out of the router is not an option. If the firmware controlling the radio is to be signed, this must be a separate sub-system, and I don't want to hear router manufacturers whining about 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: Jonathan

Last Name: Kincade

Mailing Address: 838 Wisconsin Ave

City: St. Joseph

Country: United States

State or Province: MI

ZIP/Postal Code: 49085

Email Address:

Organization Name:

Comment: I urge the FCC to not adopt any rules that would prevent consumers from replacing the operating system or firmware of any electronic device the purchase. The ability to do this allows the consumer to:

1. Correct security holes in the stock software that the manufacture will not fix promptly or at all
2. Ensure their privacy by allowing the consumer to replace closed "black box" software with vetted open source alternatives
3. Extend the lifespan of older hardware that would no longer be supported, reducing waste

These are just a few of the reasons that the freedom of a consumer to modify or replace any or all of the software on a device they have purchased must be maintained

I urge the FCC to not adopt any rules that would prevent consumers from replacing the operating system or firmware of any electronic device the purchase. The ability to do this allows the consumer to:

1. Correct security holes in the stock software that the manufacture will not fix promptly or at all
2. Ensure their privacy by allowing the consumer to replace closed "black box" software with vetted open source alternatives
3. Extend the lifespan of older hardware that would no longer be supported, reducing waste

These are just a few of the reasons that the freedom of a consumer to modify or replace any or all of the software on a device they have purchased must be maintained

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: Gerson

Last Name: Rojas

Mailing Address: El Roble

City: El Roble

Country: Costa Rica

State or Province: Alajuela

ZIP/Postal Code: 20104

Email Address: rojas.soto.g@gmail.com

Organization Name: None

Comment: Hello,

As an user of Wi-Fi technologies, I formally ask you not to implement rules that take away the ability of users to install the software of their choosing on their computing devices. Some of the reasons for this are:

- 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 appreciate that you take into account this comment.

Hello,

As an user of Wi-Fi technologies, I formally ask you not to implement rules that take away the ability of users to install the software of their choosing on their computing devices. Some of the reasons for this are:

- 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 appreciate that you take into account this 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: Matthew

Last Name: Milam

Mailing Address: 5015 pandora place

City: Plant City

Country: United States

State or Province: FL

ZIP/Postal Code: 33566

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.

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.

To pass this would be of ill-mind,

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

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

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.

To pass this would be of ill-mind,

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: Magee

Mailing Address: 101 Lower Brookhaven Rd

City: Monticello

Country: United States

State or Province: MS

ZIP/Postal Code: 39654

Email Address: timothy@eastlincoln.net

Organization Name:

Comment: This proposal is a bad idea. To achieve maximum security in consumer hardware, all users must be able to upgrade their software at will. Many users continue to use the same router for years. This rule will make it impossible for a user to upgrade to a more secure version of the software without vendor permission. While it is understandable that the FEC wants to keep clear the airwaves, prohibiting users from using FSF software on their routers is not the way to do this.

This proposal is a bad idea. To achieve maximum security in consumer hardware, all users must be able to upgrade their software at will. Many users continue to use the same router for years. This rule will make it impossible for a user to upgrade to a more secure version of the software without vendor permission. While it is understandable that the FEC wants to keep clear the airwaves, prohibiting users from using FSF software on their routers is not the way to do this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Dan

Last Name: Rebney

Mailing Address: 5721 Scenic Cir

City: Minnetonka

Country: United States

State or Province: MN

ZIP/Postal Code: 55345

Email Address:

Organization Name:

Comment: I am opposed to mandating that wifi devices be only update-able by officially signed updates. Device manufacturers have a long history of providing slow updates, having unpatched security flaws, or flat out having terrible configurations. My home wifi router has absolutely terrible performance on the official firmware. Without the ability to install custom firmware my router would be worthless.

Additionally the vagueness of the proposal could be interpreted as being unable to modify a PC such as install a Linux operating system. I would also potentially be unable to customize my cell phone, which would be terrifying as my manufacturer does not update their phone in a timely manner. Between the phone manufacturer taking months to provide updates to Android OS and my cell phone provider having to "customize" it with all their terrible apps that take up a lot of my limited memory, and that process taking month if it ever comes out since the cell provider is in the business of selling phones I've had more than one phone that eventually gets manufacturer updates that the cell phone provider won't pass on to it's customers. Without being able to root my phone and install a custom rom, I would be at the mercy of someone deciding whether or not it's profitable to provide updates.

Thank you for reading my comment.

I am opposed to mandating that wifi devices be only update-able by officially signed updates. Device manufacturers have a long history of providing slow updates, having unpatched security flaws, or flat out having terrible configurations. My home wifi router has absolutely terrible performance on the official firmware. Without the ability to install custom firmware my router would be worthless.

Additionally the vagueness of the proposal could be interpreted as being unable to modify a PC such as install a Linux operating system. I would also potentially be unable to customize my cell phone, which would be terrifying as my manufacturer does not update their phone in a timely manner. Between the phone manufacturer taking months to provide updates to Android OS and my cell phone provider having to "customize" it with all their terrible apps that take up a lot of my limited memory, and that process taking month if it ever comes out since the cell provider is in the business of selling phones I've had more than one phone that eventually gets manufacturer updates that the cell phone provider won't pass on to it's customers. Without being able to root my phone and install a custom rom, I would be at the mercy of someone deciding whether or not it's profitable to provide updates.

Thank you for reading my 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: Alexander

Last Name: Hardt

Mailing Address: 46554 Cedarhurst Dr

City: Sterling

Country: United States

State or Province: VA

ZIP/Postal Code: 20165

Email Address:

Organization Name:

Comment: I believe we need to keep devices open to the people that purchase them. If you take a look a car or truck, for example, anyone with the knowledge can make repairs or any sort of modification to it. Shouldn't the same be applicable to electronic devices? If I purchase a cell phone, then it is mine to do what I please with it. That includes modifying the firmware or radios. If I were to do something unintended with the device's design by way of modification, say, broadcast a powerful signal or jam other wireless devices, then is it not my ability to do so? Obviously this would be illegal and immoral, but the choices are mine to make regardless of legal ramifications as opposed to prevented from doing so by the manufacturer. Let's look at a less extreme example. I purchase a wireless router designed for home use. Is it not well within my right to install a custom firmware such as "DD-WRT" to make better use of the hardware I purchased? I cannot see a valid reason to disallow it. There are no rules preventing me from adding performance parts to a standard car, and then re-writing or modifying the engine's computer to compensate, so why the rules on electronic devices? These sorts of real-world examples do not pass the "common sense" test.

Thank you for your time.

I believe we need to keep devices open to the people that purchase them. If you take a look a car or truck, for example, anyone with the knowledge can make repairs or any sort of modification to it. Shouldn't the same be applicable to electronic devices? If I purchase a cell phone, then it is mine to do what I please with it. That includes modifying the firmware or radios. If I were to do something unintended with the device's design by way of modification, say, broadcast a powerful signal or jam other wireless devices, then is it not my ability to do so? Obviously this would be illegal and immoral, but the choices are mine to make regardless of legal ramifications as opposed to prevented from doing so by the manufacturer. Let's look at a less extreme example. I purchase a wireless router designed for home use. Is it not well within my right to install a custom firmware such as "DD-WRT" to make better use of the hardware I purchased? I cannot see a valid reason to disallow it. There are no rules preventing me from adding performance parts to a standard car, and then re-writing or modifying the engine's computer to compensate, so why the rules on electronic devices? These sorts of real-world examples do not pass the "common sense" test.

Thank you for your time.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nel

Last Name: Ruffin

Mailing Address: 67 Quarter Horse Lane

City: Starkville

Country: United States

State or Province: MS

ZIP/Postal Code: 39759

Email Address: nelruffin@bellsouth.net

Organization Name:

Comment: I urge you, DO NOT PASS this rule. Please consider the revenge of unintended consequences. The intent is no doubt noble, but the result would be nightmarish.

"Locking down" the firmware of any electronic device containing a modular transceiver would cripple wifi as we know it, along with other wireless services. If passed, this proposed rule would make it impossible to install open source firmware on routers, reflash Android phones, and even to install Linux or any other open source operating system on many if not most general purpose computing devices.

Please understand that this proposed rule would have SEVERE and unintended consequences for our economy and for our freedom as American citizens and consumers, and DO NOT ENACT THIS RULE.

I urge you, DO NOT PASS this rule. Please consider the revenge of unintended consequences. The intent is no doubt noble, but the result would be nightmarish.

"Locking down" the firmware of any electronic device containing a modular transceiver would cripple wifi as we know it, along with other wireless services. If passed, this proposed rule would make it impossible to install open source firmware on routers, reflash Android phones, and even to install Linux or any other open source operating system on many if not most general purpose computing devices.

Please understand that this proposed rule would have SEVERE and unintended consequences for our economy and for our freedom as American citizens and consumers, and DO NOT ENACT THIS RULE.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brandon

Last Name: Hamann

Mailing Address: 16722 NE 20th ST

City: Bellevue

Country: United States

State or Province: WA

ZIP/Postal Code: 98008

Email Address:

Organization Name:

Comment: As someone who has always looked at the USA as a beacon of freedom, this is of great concern to me that you are trying to implement a law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Steps and laws like this, when passed one after another, eventually lead to a system as close and authoritarian as those in the Middle East or North Korea.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave ovens. So I find the negative impact on health an unreasonable argument.

Besides, many manufacturers are not updating their firmware fast enough and after a few years they totally abandon their old devices. Having third party open source options that we can rely on is extremely important for us end users. If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

As someone who has always looked at the USA as a beacon of freedom, this is of great concern to me that you are trying to implement a law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Steps and laws like this, when passed one after another, eventually lead to a system as close and authoritarian as those in the Middle East or North Korea.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave ovens. So I find the negative impact on health an unreasonable argument.

Besides, many manufacturers are not updating their firmware fast enough and after a few years they totally abandon their old devices. Having third party open source options that we can rely on is extremely important for us end users. If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mari

Last Name: Miniatt

Mailing Address: 520 Black River Blvd.

City: Rome

Country: United States

State or Province: NY

ZIP/Postal Code: 13440

Email Address: maribittersweet@mail.com

Organization Name:

Comment: The main issue I have with this proposal is that I use Linux as my main desktop. I know I am in the minority, but it serves my purposes well. The routers I use have all be easy to use with my system. I feel that locking down these devices would cause more problems for the end users than any problems that the lock down is supposed to solve.

Also, as a hobby, I enjoy taking older equipment and seeing if I can get it to work. This usually means installing Linux. Last year I picked up a router at a garage sale for a buck, installed a Linux, and have a new router. As a hobbyist, I feel that this would take away my ability to try to keep older equipment out of the landfill for as long as possible.

The main issue I have with this proposal is that I use Linux as my main desktop. I know I am in the minority, but it serves my purposes well. The routers I use have all be easy to use with my system. I feel that locking down these devices would cause more problems for the end users than any problems that the lock down is supposed to solve.

Also, as a hobby, I enjoy taking older equipment and seeing if I can get it to work. This usually means installing Linux. Last year I picked up a router at a garage sale for a buck, installed a Linux, and have a new router. As a hobbyist, I feel that this would take away my ability to try to keep older equipment out of the landfill for as long as possible.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Daniel

Last Name: Blanchard

Mailing Address: 407 5th St ne

City: Fort Payne

Country: United States

State or Province: AL

ZIP/Postal Code: 35967

Email Address: Danielblanchard09@gmail.com

Organization Name:

Comment: I do not agree that our devices should be on lock down from installing and firmware or is we see fit. With encryption and the peoples security in there persons and effects. I believe this to not be in the light of the Constitution. We need the people to be able to defend themselves from any and all threts to there security.

I do not agree that our devices should be on lock down from installing and firmware or is we see fit. With encryption and the peoples security in there persons and effects. I believe this to not be in the light of the Constitution. We need the people to be able to defend themselves from any and all threts to there security.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: McGregor

Last Name: Townley

Mailing Address: 55 Brownlow Ave APT 905

City: Toronto

Country: Canada

State or Province: Ontario

ZIP/Postal Code: M4S2L1

Email Address: mcgregor.townley@gmail.com

Organization Name:

Comment: Dear Sir/Madam,

I am submitting this comment to express my dissent of this proposal. It is my opinion that users shouldn't be stopped from the ability to change/modify/replace the operating system on their purchased devices. MY reasoning for this is because it will impact not just hobbyist users who require more from their devices but professionals in many fields.

Wireless network researches depend on the ability to modify their devices to run custom code. Mesh networking is an important system of networking used by first responders in emergency situations. This will become more difficult to implement if these rules are passed.

The security of networks will be compromised by these rules. It is frequent enough of an issue that end users must install a custom patch to close an unpatched vulnerability in an out of service life operating system this will leave users and businesses open to exploits and damages.

Custom patches to wireless drives will also be restricted meaning performance will be worse and bug patches that companies believe are unimportant will remain unfixed.

our ability to run fully open source software will be compromised. This impacts not just casual linux users but researches of all types. These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Possibly most important to the USA and the world is the billions of dollars of commerce such as secure WIFI vendors, and retail hotspot vendors rely on the ability of users to install software of their choosing.

And the most egregious folly of these rules are stopping people from truly owning their devices. If I am unable to install what I want on a device then I do not truly own it.

Thank You for reading.

Dear Sir/Madam,

I am submitting this comment to express my dissent of this proposal. It is my opinion that users shouldn't be stopped from the ability to change/modify/replace the operating system on their purchased devices. MY reasoning for this is

because it will impact not just hobbyist users who require more from their devices but professionals in many fields.

Wireless network researches depend on the ability to modify their devices to run custom code. Mesh networking is an important system of networking used by first responders in emergency situations. This will become more difficult to implement if these rules are passed.

The security of networks will be compromised by these rules. It is frequent enough of an issue that end users must install a custom patch to close an unpatched vulnerability in an out of service life operating system this will leave users and businesses open to exploits and damages.

Custom patches to wireless drives will also be restricted meaning performance will be worse and bug patches that companies believe are unimportant will remain unfixed.

our ability to run fully open source software will be compromised. This impacts not just casual linux users but researches of all types. These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Possibly most important to the USA and the world is the billions of dollars of commerce such as secure WIFI vendors, and retail hotspot vendors rely on the ability of users to install software of their choosing.

And the most egregious folly of these rules are stopping people from truly owning their devices. If I am unable to install what I want on a device then I do not truly own it.

Thank You 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: everett

Last Name: neucere

Mailing Address: 10318 minturn lane

City: houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77064

Email Address: neucere1@gmail.com

Organization Name:

Comment: Dear Sir/Madam,

As a person who has always looked at USA as a beacon of freedom, this is of great concern to me that you are trying to implement such a draconian law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Steps and laws like this, when passed one after another, eventually lead to a system as close and authoritarian as those in the Middle East or North Korea.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave ovens. So I find the negative impact on health an unreasonable argument.

Besides, many manufacturers are not updating their firmware fast enough and after a few years they totally abandon their old devices. Having third party open source options that we can rely on is extremely important for us end users. If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

Sincerely yours, A netizen

Dear Sir/Madam,

As a person who has always looked at USA as a beacon of freedom, this is of great concern to me that you are trying to implement such a draconian law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Steps and laws like this, when passed one after another, eventually lead to a system as close and authoritarian as those in the Middle East or North Korea.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave ovens. So I find the negative impact on health an unreasonable argument.

Besides, many manufacturers are not updating their firmware fast enough and after a few years they totally abandon their old devices. Having third party open source options that we can rely on is extremely important for us end users. If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

Sincerely yours, A netizen

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Scott

Last Name: Fox

Mailing Address: 11270 Roseberg Ave S

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98168

Email Address: scottf@fremontnetworks.com

Organization Name: null

Comment: Companies get it wrong, and they get it wrong often. Whether intentionally or not they leave security holes in essential internet equipment and devices. When we limit the uses of devices and and it's associated software (firmware) then we limit innovation and new forms of commerce. Essentially it is exactly the same as saying to the public, "Please let us limit the amount of encryption you are using so we can hack you easier". Neither of these methods are prudent or necessary. Companies and the Federal Government are getting LAZY when it comes to problems they are having with these devices, security holes, and encryption. Please do not pass this!

Companies get it wrong, and they get it wrong often. Whether intentionally or not they leave security holes in essential internet equipment and devices. When we limit the uses of devices and and it's associated software (firmware) then we limit innovation and new forms of commerce. Essentially it is exactly the same as saying to the public, "Please let us limit the amount of encryption you are using so we can hack you easier". Neither of these methods are prudent or necessary. Companies and the Federal Government are getting LAZY when it comes to problems they are having with these devices, security holes, and encryption. Please do not pass this!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ellis

Last Name: Harlan

Mailing Address: 313 Lenox Avenue

City: Norfolk

Country: United States

State or Province: VA

ZIP/Postal Code: 23503

Email Address: null

Organization Name: null

Comment: Dear FCC,

It has come to my attention that you are considering a proposal that will require manufacturers to lock down computing devices. Although you may be considering this to be beneficial in the long run, the concerning portion is that it is feared that it would inhibit or terminate the ability of individual peoples to choose what operating system that is installed on computers and other devices. This would not only lead to the growing number of people who tinker with operating systems, are learning how to build operating systems, or even those who just don't prefer Windows or Mac to feel abandoned, ultimately leading to the stagnation of the development of better, safer technologies in areas such as wireless technology. Therefore, in conclusion, when this proposition is being considered, don't inhibit the freedom for us, the people, to choose how our computing devices operate.

Dear FCC,

It has come to my attention that you are considering a proposal that will require manufacturers to lock down computing devices. Although you may be considering this to be beneficial in the long run, the concerning portion is that it is feared that it would inhibit or terminate the ability of individual peoples to choose what operating system that is installed on computers and other devices. This would not only lead to the growing number of people who tinker with operating systems, are learning how to build operating systems, or even those who just don't prefer Windows or Mac to feel abandoned, ultimately leading to the stagnation of the development of better, safer technologies in areas such as wireless technology. Therefore, in conclusion, when this proposition is being considered, don't inhibit the freedom for us, the people, to choose how our computing devices operate.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nathan

Last Name: Hartman

Mailing Address: 6 Granite Ridge Drive

City: Ottawa

Country: Canada

State or Province: Ontario

ZIP/Postal Code: K2S1Y2

Email Address: hnathan918@gmail.com

Organization Name: N/A

Comment: 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.

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: Samuel

Last Name: Webster

Mailing Address: 2110 Kittredge St.

City: Berkeley

Country: United States

State or Province: CA

ZIP/Postal Code: 94704

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely

bad" category of regulatory ideas.

Thank you for your time,

Samuel Webster

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Thank you for your time,

Samuel Webster

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: Shane

Last Name: Brauner

Mailing Address: 215 E 95th St Apt 32B

City: New York

Country: United States

State or Province: NY

ZIP/Postal Code: 10128

Email Address: shane.brauner@gmail.com

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install software of our choosing on our computing devices. Restricting our freedom in this manner not only impedes the ability of researchers looking at new technologies, it makes us vulnerable to cyber attacks and other security vulnerabilities which can go un-patched by manufacturers. These vulnerabilities and bugs can be patched or circumvented if consumers are not barred from this practice.

My career of more than 20 years working with technology - specifically in research computing - has given me expertise and perspective on the power of open technology. It has revolutionized computing and America has been at the forefront of this. Laws and regulations can not stop the advancement of technology - they can only slow it. If America does not continue to innovate and lead, other countries will.

America was founded on individual liberty and a "can-do" attitude. Please do not sacrifice what makes this country great by handing even more power to corporations at the expense of of our liberty.

Sincerely,

Shane Brauner

Please do not implement rules that take away the ability of users to install software of our choosing on our computing devices. Restricting our freedom in this manner not only impedes the ability of researchers looking at new technologies, it makes us vulnerable to cyber attacks and other security vulnerabilities which can go un-patched by manufacturers. These vulnerabilities and bugs can be patched or circumvented if consumers are not barred from this practice.

My career of more than 20 years working with technology - specifically in research computing - has given me expertise and perspective on the power of open technology. It has revolutionized computing and America has been at the forefront of this. Laws and regulations can not stop the advancement of technology - they can only slow it. If America does not continue to innovate and lead, other countries will.

America was founded on individual liberty and a "can-do" attitude. Please do not sacrifice what makes this country great by handing even more power to corporations at the expense of of our liberty.

Sincerely,



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: Allen

Last Name: Hansen

Mailing Address: 4808 E 12th St Apt 4

City: Cheyenne

Country: United States

State or Province: WY

ZIP/Postal Code: 82001

Email Address:

Organization Name:

Comment: This is a pretty terrible idea with pretty terrible consequences. If I own the device, I should have the right to install whatever I wish on it. Also, limiting what can be installed has the potential to limit the evolution of technology outside of mainstream industry. I urge you to consider the validity of these proposed rules and please do not use them.

This is a pretty terrible idea with pretty terrible consequences. If I own the device, I should have the right to install whatever I wish on it. Also, limiting what can be installed has the potential to limit the evolution of technology outside of mainstream industry. I urge you to consider the validity of these proposed rules and please do not use them.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Concerned

Last Name: Citizen

Mailing Address: 123 W Easy St

City: Beverly Hills

Country: United States

State or Province: CA

ZIP/Postal Code: 90210

Email Address:

Organization Name:

Comment: Words cannot even begin to describe how outraged I am to think that my own government would even consider outlawing custom firmware to be used on MY own personal computers. I feel like what very little personal liberties and rights I have as a citizen my government wants to take away. Truly vile.

Words cannot even begin to describe how outraged I am to think that my own government would even consider outlawing custom firmware to be used on MY own personal computers. I feel like what very little personal liberties and rights I have as a citizen my government wants to take away. Truly vile.

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: Zak

Last Name: Mak

Mailing Address: 1161 e walnut ave

City: Carson

Country: United States

State or Province: CA

ZIP/Postal Code: 90746

Email Address:

Organization Name:

Comment: Please don't enact this, I use specialized firmware to make my router usable. I can use my cheap routernlike a really expensive one without having to clean out my bank account.

Please don't enact this, I use specialized firmware to make my router usable. I can use my cheap routernlike a really expensive one without having to clean out my bank account.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ben

Last Name: Reiter

Mailing Address: 3765A 17th Street

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94114

Email Address: dimdog@gmail.com

Organization Name:

Comment: As a software engineer and regular consumer of all kinds of computer hardware, I am very concerned by these proposed rules. It is not only common place, but in fact necessary to the regular functioning of many devices to regularly wipe / re-install an new operating system. Additionally, as practically no manufacturer produces a computer that already runs operating systems like Solaris or OpenBSD, it would seemingly become impossible to ever legally install these otherwise completely safe and legal Operating Systems.

As a software engineer and regular consumer of all kinds of computer hardware, I am very concerned by these proposed rules. It is not only common place, but in fact necessary to the regular functioning of many devices to regularly wipe / re-install an new operating system. Additionally, as practically no manufacturer produces a computer that already runs operating systems like Solaris or OpenBSD, it would seemingly become impossible to ever legally install these otherwise completely safe and legal Operating Systems.

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: Troy

Last Name: Halter

Mailing Address: 1811 Ne 55th Street

City: Kansas City

Country: United States

State or Province: MO

ZIP/Postal Code: 64118

Email Address:

Organization Name:

Comment: Banning the ability to install software onto our own devices(which we paid for) is absurd. You won't stop people from actually doing it nor do you have any way of enforcing this. As an aspiring network technician you are trying to criminalize an effective method of learning for me and millions of other technicians.

Banning the ability to install software onto our own devices(which we paid for) is absurd. You won't stop people from actually doing it nor do you have any way of enforcing this. As an aspiring network technician you are trying to criminalize an effective method of learning for me and millions of other technicians.

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: Ian

Last Name: Toltz

Mailing Address: 376 Ocean Ave #902

City: Revere

Country: United States

State or Province: MA

ZIP/Postal Code: 02151

Email Address: itoltz@gmail.com

Organization Name:

Comment: Please do not take away my ability to install software of my choosing on devices I own.

Please do not take away my ability to install software of my choosing on devices I own.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Alexander

Last Name: Barghi

Mailing Address: 22648 Gray Falcon Square

City: Ashburn

Country: United States

State or Province: VA

ZIP/Postal Code: 20148

Email Address: abarghi@abarghi.com

Organization Name:

Comment: I respectfully disagree with this proposal as it will prevent many researchers who use custom Wi-Fi firmware and open-source operating systems to conduct research. It will also threaten many startups that rely on Linux and similar software for their computing infrastructure. Without the ability to install Linux on routers and computers, it will be expensive to redevelop many essential tools for preloaded software such as Windows and Mac OS X. Much of the innovation accomplished by independent researchers and entrepreneurs depends on the ability to modify or replace operating systems and this proposed rule will put an end to such innovation.

In addition, it should be noted that many device manufactures do not update their firmware often, leaving it open to exploits that in many cases are trivial for a knowledgeable user to fix. This is particularly important in the case of Android phones, since manufacturer support for Android phones is very poor. A large number of Android users have modified Android to patch security holes on their own, and some have even sold their patched versions of Android to companies who demand enhanced device security. This proposed rule would make patching security holes impossible and potentially expose people relying on custom versions of Android and other operating systems.

I respectfully disagree with this proposal as it will prevent many researchers who use custom Wi-Fi firmware and open-source operating systems to conduct research. It will also threaten many startups that rely on Linux and similar software for their computing infrastructure. Without the ability to install Linux on routers and computers, it will be expensive to redevelop many essential tools for preloaded software such as Windows and Mac OS X. Much of the innovation accomplished by independent researchers and entrepreneurs depends on the ability to modify or replace operating systems and this proposed rule will put an end to such innovation.

In addition, it should be noted that many device manufactures do not update their firmware often, leaving it open to exploits that in many cases are trivial for a knowledgeable user to fix. This is particularly important in the case of Android phones, since manufacturer support for Android phones is very poor. A large number of Android users have modified Android to patch security holes on their own, and some have even sold their patched versions of Android to companies who demand enhanced device security. This proposed rule would make patching security holes impossible and potentially expose people relying on custom versions of Android and other operating systems.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Adam

Last Name: Gould

Mailing Address: 31150 North Park Drive

City: Farmington Hills

Country: United States

State or Province: MI

ZIP/Postal Code: 48331

Email Address:

Organization Name:

Comment: As a university student, these new regulations are terrible. Limiting wireless devices in the "unregulated" or license free bands will have nothing but bad outcomes. At school, engineering research on wireless devices will be forced to a halt, since there it is no longer legal to modify those devices. As research slows down, companies will pull their money out of U.S. put money into research facilities in countries WITHOUT these restrictions. With these measures, you will kill not only the freedom of choice, the ability to maintain units after their support cycle ends, the ability to change operating systems on computers, but also the university research departments that rely on making modifications to these devices.

As a university student, these new regulations are terrible. Limiting wireless devices in the "unregulated" or license free bands will have nothing but bad outcomes. At school, engineering research on wireless devices will be forced to a halt, since there it is no longer legal to modify those devices. As research slows down, companies will pull their money out of U.S. put money into research facilities in countries WITHOUT these restrictions. With these measures, you will kill not only the freedom of choice, the ability to maintain units after their support cycle ends, the ability to change operating systems on computers, but also the university research departments that rely on making modifications to these 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: Christopher

Last Name: Jacobs

Mailing Address: 2803 Champlin CT

City: Richardson

Country: United States

State or Province: TX

ZIP/Postal Code: 75082

Email Address: chrisj951@gmail.com

Organization Name: null

Comment: I believe it would be best for owners of their equipment to be able to freely modify the software on it. Preventing those from legally modifying it would not make the USA safer, and would only be added restrictions without reason. A significant number of bugs, and even security vulnerabilities, have been found and fixed by people modifying their router software to improve it, and doing so should not be illegal.

I believe it would be best for owners of their equipment to be able to freely modify the software on it. Preventing those from legally modifying it would not make the USA safer, and would only be added restrictions without reason. A significant number of bugs, and even security vulnerabilities, have been found and fixed by people modifying their router software to improve it, and doing so should not be illegal.

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: Amy

Last Name: Lowitz

Mailing Address: 135 E Johnson St #8

City: Madison

Country: United States

State or Province: WI

ZIP/Postal Code: 53703

Email Address: amy.lowitz@gmail.com

Organization Name:

Comment: To Whom it May Concern:

I am writing to ask that the FCC not implement rules that take away the right and the ability of users to install the software of their choosing on their computing devices. The problems created by the proposed new rules will be vastly greater in magnitude and seriousness than the problems they mitigate. There are many reasons why the new rules are problematic. I will briefly list several of them below:

- 1) Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Americans should have the right to fix security holes in devices they own in the event that the manufacturer can't or won't, or in the event that the fix provided by the manufacturer is inadequate.
- 2) There is a long history of users providing their own patches to serious bugs in wifi drivers (bugs for which no fix was ever provided by the manufacturer). These user-generated patches would be illegal under the new rules.
- 3) Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- 4) Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
- 5) Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
- 6) The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
- 7) These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays (including those operated not by authorized law enforcement, but by illegal third parties). It will also harm any attempts to build open source cell towers and systems.
- 8) While the new rules are meant to mitigate potential interference by wireless devices in restricted frequency bands, which can cause safety issues, the rules are poorly drafted such that they are so broad they limit a wide range of activities that have no impact on safety, and needlessly limit the freedom of users to control the electronic devices they own.

In conclusion, the newly proposed rules are much too broad, stepping far beyond what is necessary to prevent unsafe use of restricted frequencies. Not only this, the new rules CAUSE other serious safety problems by limiting emergency first responders' access to mesh networking and by limiting end-users ability to patch security flaws in their own equipment.

The new rules are too broad, anti-commerce, anti-freedom, anti-privacy, and create more safety problems than they solve. I encourage the FCC to draft narrower rules that only limit the radio frequencies of these devices, without restricting users ability to modify other parts of the firmware or software.

Best regards,  
Amy

To Whom it May Concern:

I am writing to ask that the FCC not implement rules that take away the right and the ability of users to install the software of their choosing on their computing devices. The problems created by the proposed new rules will be vastly greater in magnitude and seriousness than the problems they mitigate. There are many reasons why the new rules are problematic. I will briefly list several of them below:

- 1) Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Americans should have the right to fix security holes in devices they own in the event that the manufacturer can't or won't, or in the event that the fix provided by the manufacturer is inadequate.
- 2) There is a long history of users providing their own patches to serious bugs in wifi drivers (bugs for which no fix was ever provided by the manufacturer). These user-generated patches would be illegal under the new rules.
- 3) Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- 4) Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
- 5) Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
- 6) The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
- 7) These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays (including those operated not by authorized law enforcement, but by illegal third parties). It will also harm any attempts to build open source cell towers and systems.
- 8) While the new rules are meant to mitigate potential interference by wireless devices in restricted frequency bands, which can cause safety issues, the rules are poorly drafted such that they are so broad they limit a wide range of activities that have no impact on safety, and needlessly limit the freedom of users to control the electronic devices they own.

In conclusion, the newly proposed rules are much too broad, stepping far beyond what is necessary to prevent unsafe use of restricted frequencies. Not only this, the new rules CAUSE other serious safety problems by limiting emergency first responders' access to mesh networking and by limiting end-users ability to patch security flaws in their own equipment.

The new rules are too broad, anti-commerce, anti-freedom, anti-privacy, and create more safety problems than they solve. I encourage the FCC to draft narrower rules that only limit the radio frequencies of these devices, without restricting users ability to modify other parts of the firmware or software.

Best regards,  
Amy

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jay

Last Name: Pruett

Mailing Address: 1834 Stacey Crest

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77008

Email Address: null

Organization Name: null

Comment: Please don't do this. America deserves to be great.

Please don't do this. America deserves to be great.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Anonymous

Mailing Address: Anonymous

City: Anonymous

Country: United States

State or Province: AL

ZIP/Postal Code: Anonymous

Email Address: null

Organization Name: null

Comment: Please do not implement said rules as:

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 said rules as:

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: Shane

Last Name: Craig

Mailing Address: 14005 Monroe St

City: Omaha

Country: United States

State or Province: NE

ZIP/Postal Code: 68137

Email Address: dj3stripes@gmail.com

Organization Name: Just a tax payer trying to keep my head above water. Please spend my tax dollars on more important things than this

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices for these reason:

-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 computing devices for these reason:

-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: Anthony

Last Name: Martinez

Mailing Address: 5261 Park ridge court

City: Crozet

Country: United States

State or Province: VA

ZIP/Postal Code: 22932

Email Address:

Organization Name:

Comment: Good day, I have come to submit a formal complaint about this policy. I believe that it will stifle wireless network research, make everyone unable to repair security holes in their devices, resulting in a less secure workplace and, more importantly, government, and the fact that this will destroy a entire workplace for no gain for the consumer- One could argue that this feature is inherently anti-consumer. I support capitalism, but I believe that this not only gets in the way of capitalism's ability to grow, but, in many ways, goes against the idea that property is, in fact, ours. It states that we cannot touch that which we have built, and yet by stating that we cannot modify our devices, you are stating something similar to the idea that one cannot repair one's own vehicle- Which, if you look into americas history, simply isn't the case. We replace the engines of our vehicles all the time, so why can we not replace the engines on our computers?

As I request- Please do not let this pass. It's not a good thing.

Good day, I have come to submit a formal complaint about this policy. I believe that it will stifle wireless network research, make everyone unable to repair security holes in their devices, resulting in a less secure workplace and, more importantly, government, and the fact that this will destroy a entire workplace for no gain for the consumer- One could argue that this feature is inherently anti-consumer. I support capitalism, but I believe that this not only gets in the way of capitalism's ability to grow, but, in many ways, goes against the idea that property is, in fact, ours. It states that we cannot touch that which we have built, and yet by stating that we cannot modify our devices, you are stating something similar to the idea that one cannot repair one's own vehicle- Which, if you look into americas history, simply isn't the case. We replace the engines of our vehicles all the time, so why can we not replace the engines on our computers?

As I request- Please do not let this pass. It's not a good thing.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Maloy

Mailing Address: 2109 W. Sewaha Street

City: Tampa

Country: United States

State or Province: FL

ZIP/Postal Code: 33612

Email Address: rmaloy97@gmail.com

Organization Name:

Comment: Good day,

I wish to state that the language utilized in your latest push to regulate wireless communications is vague and may be used to abuse loopholes to further tighten down the freedom of personal computer users. As somebody who frequently utilizes the GNU/Linux operating system, and frequently builds my own machines from parts purchased online; I worry that the latest regulations proposed may make it an unstated requirement to lock the end-user out of modifying their own personal computer.

The language should be revised and improved to ensure that it can't be used to shut down things which are not the focus of the regulations.

Thank you.

Good day,

I wish to state that the language utilized in your latest push to regulate wireless communications is vague and may be used to abuse loopholes to further tighten down the freedom of personal computer users. As somebody who frequently utilizes the GNU/Linux operating system, and frequently builds my own machines from parts purchased online; I worry that the latest regulations proposed may make it an unstated requirement to lock the end-user out of modifying their own personal computer.

The language should be revised and improved to ensure that it can't be used to shut down things which are not the focus of the regulations.

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: Parker

Last Name: Emerson

Mailing Address: 1766 SW Marlow

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97225

Email Address: parker.emerson@gmail.com

Organization Name:

Comment: I am restarting my career as a computer scientist, getting my MSCS. I was a lawyer, but wanted to move into IP litigation. I \*love\* finding out how things work. My education has been fueled by my ability to use a lot of OS programs. Being able to look into my router helped me pass my Internetworking Class, and fostered an interest in network security. Locking down routers will make my job harder after I graduate. Restricting access to open source is myopic and shortsighted. Please don't do it.

I am restarting my career as a computer scientist, getting my MSCS. I was a lawyer, but wanted to move into IP litigation. I \*love\* finding out how things work. My education has been fueled by my ability to use a lot of OS programs. Being able to look into my router helped me pass my Internetworking Class, and fostered an interest in network security. Locking down routers will make my job harder after I graduate. Restricting access to open source is myopic and shortsighted. Please don't 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: John

Last Name: Carroll

Mailing Address: 2483 Banchory Rd

City: Winter Park

Country: United States

State or Province: FL

ZIP/Postal Code: 32792

Email Address: john.h.carroll@gmail.com

Organization Name: --

Comment: This is ridiculous.

This is ridiculous.

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: mahen

Last Name: nowzadick

Mailing Address: cornell lane, pailles

City: port louis

Country: Mauritius

State or Province: mauritius

ZIP/Postal Code: 742CU00111

Email Address: staticglow@live.com

Organization Name:

Comment: Hey do not do this because its my device, my choice.

I am allowed to run anything I want on my Device as long as i am not interfering with the good being of others.

Hey do not do this because its my device, my choice.

I am allowed to run anything I want on my Device as long as i am not interfering with the good being of others.

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: Grant

Last Name: Martin

Mailing Address: 2845 Mill Wood Lane

City: Blacksburg

Country: United States

State or Province: VA

ZIP/Postal Code: 24060

Email Address:

Organization Name:

Comment: If I buy a computer, I should be able to do whatever I want with it. Preventing me from installing OSes like Linux on my computer means every computer runs on either OSX or Windows. There are 2 reasons you might want us to be stuck on operating systems made by big companies: You think it might prevent hackers from hacking. Here's a rule of thumb, if someone wants to break a system, and has physical access to the system, they absolutely can. Your everyday Joe isn't smart enough to do this, but then again your average Joe can't and won't hack into stuff. The other possible reason for your wanting to lock us into OSX or Windows is to spy on us. If a public official is reading this right now, you and I both know that the NSA shouldn't be spying on us, but they don't like to follow the rules. So putting this rule in place will spy on everyone with a computer, and make it illegal to circumvent the spying. We've also established that if someone is smart enough, and willing to break the law, they totally can circumvent this, meaning this negatively affects every average citizen, but does very little to stop hackers and terrorists. Thank you for taking the time to read my comment.

If I buy a computer, I should be able to do whatever I want with it. Preventing me from installing OSes like Linux on my computer means every computer runs on either OSX or Windows. There are 2 reasons you might want us to be stuck on operating systems made by big companies: You think it might prevent hackers from hacking. Here's a rule of thumb, if someone wants to break a system, and has physical access to the system, they absolutely can. Your everyday Joe isn't smart enough to do this, but then again your average Joe can't and won't hack into stuff. The other possible reason for your wanting to lock us into OSX or Windows is to spy on us. If a public official is reading this right now, you and I both know that the NSA shouldn't be spying on us, but they don't like to follow the rules. So putting this rule in place will spy on everyone with a computer, and make it illegal to circumvent the spying. We've also established that if someone is smart enough, and willing to break the law, they totally can circumvent this, meaning this negatively affects every average citizen, but does very little to stop hackers and terrorists. Thank you for taking the time to read my 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: Michael

Last Name: McClanahan

Mailing Address: 24438 S. Rock Ridge

City: Channahon

Country: United States

State or Province: IL

ZIP/Postal Code: 60410

Email Address: 72madhouse@gmail.com

Organization Name:

Comment: This rule will do nothing but limit creativity and prevent security holes that would have been found by the end user to not be released to the software company freely.

A great example of in the past decade would be the iPhone. When jailbreaking began, Apple tried their best to prevent it and make it illegal. What the average iPhone owner didn't understand or know though, was that many of the updates Apple implemented were created by Devs and made popular by fellow "Jailbreakers". Your new rule will just kill invention.

Rather than worry about a very small fraction of people trying to create something better, try going after the larger organizations.

This rule will do nothing but limit creativity and prevent security holes that would have been found by the end user to not be released to the software company freely.

A great example of in the past decade would be the iPhone. When jailbreaking began, Apple tried their best to prevent it and make it illegal. What the average iPhone owner didn't understand or know though, was that many of the updates Apple implemented were created by Devs and made popular by fellow "Jailbreakers". Your new rule will just kill invention.

Rather than worry about a very small fraction of people trying to create something better, try going after the larger organizations.

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: Thomas

Last Name: VanSelus

Mailing Address: 5022 Sheboygan Ave. Apt. 10

City: Madison

Country: United States

State or Province: WI

ZIP/Postal Code: 53705

Email Address:

Organization Name:

Comment: When I was a teenager I enjoyed taking apart and modifying the software and hardware on cheap routers and finding out how they worked. As an adult I have a good job working with and improving much of the same software and technology. At my interview I could answer "yes" when my interviewer asked if I had experience with a particular piece of software because although it had never even been discussed in 5 years of college I had used it in the context of modifying router firmware. Without this experience it is unlikely I would have the job I do. I urge the FCC to not impose any regulations which will limit people's ability to modify software or hardware on their own devices. Doing so will seriously limit the next generation's ability to learn the skills needed to compete in highly technical fields.

When I was a teenager I enjoyed taking apart and modifying the software and hardware on cheap routers and finding out how they worked. As an adult I have a good job working with and improving much of the same software and technology. At my interview I could answer "yes" when my interviewer asked if I had experience with a particular piece of software because although it had never even been discussed in 5 years of college I had used it in the context of modifying router firmware. Without this experience it is unlikely I would have the job I do. I urge the FCC to not impose any regulations which will limit people's ability to modify software or hardware on their own devices. Doing so will seriously limit the next generation's ability to learn the skills needed to compete in highly technical fields.