

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: Thompson

Mailing Address: 5108 Stockton Dr.

City: Raleigh

Country: United States

State or Province: NC

ZIP/Postal Code: 27606

Email Address: thompsonutil@gmail.com

Organization Name:

Comment: There is really no reason for these rules to exist. I am a Computer Engineer and an Amateur Radio operator (KE4GIY) and I have been using Open Source firmware on Linksys wireless routers for years.

If you don't think the Open Source replacements are a good thing then explain to me why that is currently the best route for dealing just this one security exploit:

<http://www.pcworld.com/article/2925552/netgear-and-zyxel-confirm-netusb-flaw-are-working-on-fixes.html>

There is really no reason for these rules to exist. I am a Computer Engineer and an Amateur Radio operator (KE4GIY) and I have been using Open Source firmware on Linksys wireless routers for years.

If you don't think the Open Source replacements are a good thing then explain to me why that is currently the best route for dealing just this one security exploit:

<http://www.pcworld.com/article/2925552/netgear-and-zyxel-confirm-netusb-flaw-are-working-on-fixes.html>

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: Yash

Last Name: Chauhan

Mailing Address: Apartment 1210

City: Richmond Hill

Country: Canada

State or Province: Ontario

ZIP/Postal Code: L4B0A1

Email Address: yashchauhan94@ymail.com

Organization Name: null

Comment: To whomsoever it may concern,

It has come to my attention that the FCC is responding to the fact that people illegally modified radios to operate in a manner that interferes weather Doppler radar at airports by considering a proposal to require manufacturers to lock down computing devices to prevent modification if they have a "modular wireless radio" or a device with an "electronic label".

I understand the concern, but request that this rule is not implemented. This will restrict installation of alternative operating systems on computers, like GNU/Linux, OpenBSD, FreeBSD, etc. As a student studying software, I would like to mention that Linux is very important to my academics and most of the work I do. Without Linux so many software projects both students and professionals have worked on would not be possible.

For a small section of violators most of us who do not plan to take any illegal action will be punished. Please do not let this happen.

With Regards,
Yash Chauhan

To whomsoever it may concern,

It has come to my attention that the FCC is responding to the fact that people illegally modified radios to operate in a manner that interferes weather Doppler radar at airports by considering a proposal to require manufacturers to lock down computing devices to prevent modification if they have a "modular wireless radio" or a device with an "electronic label".

I understand the concern, but request that this rule is not implemented. This will restrict installation of alternative operating systems on computers, like GNU/Linux, OpenBSD, FreeBSD, etc. As a student studying software, I would like to mention that Linux is very important to my academics and most of the work I do. Without Linux so many software projects both students and professionals have worked on would not be possible.

For a small section of violators most of us who do not plan to take any illegal action will be punished. Please do not let this happen.

With Regards,

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Laster

Mailing Address: 1197 Fellowship Rd

City: Mt. Juliet

Country: United States

State or Province: TN

ZIP/Postal Code: 37122

Email Address: matthew.d.laster@gmail.com

Organization Name:

Comment: To whom it may concern,

Wifi OS installation, as well as the installation of other custom OSes much like the various distributions of Linux are needed.

Most routers do not have it within their firmware to properly act as a bridge to extend it out to a further point. I live in a rural location and have to use a bridge on a router I own to give access to the apartment that I also have on my land.

Without the ability to install a custom firmware on the second router; there would be no internet capabilities out there without wiring the entire location.

Further, blocking the usage of Linux, FreeBSD, or other alternative OSes would just further put Microsoft and Apple into a higher power as they would be the only sources of having an operating system, which would quite possibly drive the prices up slightly.

Even further, the abilities of some of the custom firmwares on Android phones is by far better than what we receive from other sources, which is typically mandated by the carrier as well. I have not received a firmware update on my phone in quite possibly two years as Verizon has more than likely deemed it fit to not allow an update to it anymore, despite the device still working.

If anything this entire proposal is a step backwards from everything we want in an open and free internet.

To whom it may concern,

Wifi OS installation, as well as the installation of other custom OSes much like the various distributions of Linux are needed.

Most routers do not have it within their firmware to properly act as a bridge to extend it out to a further point. I live in a rural location and have to use a bridge on a router I own to give access to the apartment that I also have on my land.

Without the ability to install a custom firmware on the second router; there would be no internet capabilities out there without wiring the entire location.

Further, blocking the usage of Linux, FreeBSD, or other alternative OSes would just further put Microsoft and Apple into a higher power as they would be the only sources of having an operating system, which would quite possibly drive the prices up slightly.

Even further, the abilities of some of the custom firmwares on Android phones is by far better than what we receive from other sources, which is typically mandated by the carrier as well. I have not received a firmware update on my phone in quite possibly two years as Verizon has more than likely deemed it fit to not allow an update to it anymore, despite the device still working.

If anything this entire proposal is a step backwards from everything we want in an open and free internet.

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: Langley

Mailing Address: 1368 oak st

City: redlands

Country: United States

State or Province: CA

ZIP/Postal Code: 92373

Email Address: dnr15topher@live.com

Organization Name:

Comment: Please DO NOT do this!

I've always required on third-party firmware/software to improve my devices, especially long after the manufacturer chooses to support the device.

Please DO NOT do this!

I've always required on third-party firmware/software to improve my devices, especially long after the manufacturer chooses to support the device.

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: Dallin

Last Name: Hunter

Mailing Address: 640 E Long Shadow Dr

City: Draper

Country: United States

State or Province: UT

ZIP/Postal Code: 84020

Email Address: dallin.hunter@gmail.com

Organization Name: null

Comment: Greetings,

I have been working with computers for over 15 years, both professionally and as a hobby. I am familiar with their operations, and I'm very good at fixing them. The various synopses I have read of this proposal indicate to me that my hobby and my livelihood would be severely impacted by your proposed rule in a very negative way.

Forthwith I will attempt to outline a few non-nefarious use-case scenarios in which installing new firmware or a new OS on a WiFi enabled device would not only improve the wireless performance and stability, but would most likely make the device wholly use-able after prior dysfunction. A number of them will be from my own personal experience.

I am currently in possession of a router that has lost significant functionality since I purchased it. The original price was around \$250, so it would be a pity for it to lose complete function, but the vendor hasn't yet rectified the issues I am facing even after three or four firmware revisions. I am currently considering installing custom firmware on this device to improve its functionality and prevent me from having to purchase a brand new router that, because of my particular connectivity needs, would cost as much or more than \$250. With a newborn, \$250 is a lot of money to spend on a piece of technology I could fix myself for free with a swift firmware installation.

My wife's computer was performing poorly with her last operating system (an old and ailing copy of Windows 7). A new laptop can cost a lot of money nowadays, especially should she have desired the same level of operation and function. I wiped her hard drive clean, after backing up her files of course, and installed a brand new solid state drive and a fresh copy of Windows 7. Now, her laptop has in it a WiFi module. It is my understanding that her laptop would fall under your rule's classification as a device that can generate radio frequencies, and so my actions could be seen as illegal and fine-able. However, the only thing my actions have done is make her laptop functional where before it was not, and has assuaged the need of buying a new laptop.

In my job specifically, one of my main duties is prepping laptops and desktops for use by our user-base. The way I do this is by wiping the current operating system of the computer and then installing our customized version of Windows 7 Enterprise on them. Again, it is my understanding that this would be illegal with your rule in place. I'm sure we would figure out a way around this as a department, but it would negatively impact the way we do business.

As an extension of the above, if installing a new operating system on a computer fresh from an OEM is made illegal, that means that consumers are at the mercy of said OEMs when it comes to pre-installed software ("bloatware"). This being the case, OEMs could potentially install invasive and harmful applications to keep track of information entered on the customer's computers for any purpose, and there would be nothing the consumer could do about it.

Currently, I am in the possession of a smartphone, which has inherent WiFi capabilities, which was not functioning a month ago. It would start, but wouldn't boot into its operating system. Something was wrong with both the OS and the firmware on the device, so I flashed a new firmware to the on-chip ROM and I installed a new operating system, a form of Android Lollipop. Now the phone works perfectly, and is completely usable once again, a device worth probably about \$200 in today's market.

Another potential victim of this ruling is the open-source Linux community at large. Without the ability to install new operating systems or firmware on WiFi capable devices, the entire community would likely die out, disbanding a vast and diverse group of talented and dedicated programmers and innovators. Without innovators, we will stagnate in the technology sector.

I am, politically speaking, in support of agency. I believe that the individual should have choice to do whatever they desire, as long as the life and prosperity of others is not in danger as a result of their decisions. This ruling sounds to me like it robs the individual of choice and provides corporations with yet another tool to use for exploitation and profit. Corporations don't need to be given more power; corporations, as it stands, have too much power already.

Please do not implement this rule. Please allow consumers to continue to have the freedom to use the software they see fit on the devices they have legally obtained. Please don't give corporations more control over our electronics. Please don't stifle innovation, and let us continue to be a land of innovators. I have admired the decisions of the current FCC over the past couple of years, and I think you are doing a wonderful job so far, in support of the free internet. Please continue to move forward, and not backward.

Respectfully yours,
Dallin Hunter

Greetings,

I have been working with computers for over 15 years, both professionally and as a hobby. I am familiar with their operations, and I'm very good at fixing them. The various synopses I have read of this proposal indicate to me that my hobby and my livelihood would be severely impacted by your proposed rule in a very negative way.

Forthwith I will attempt to outline a few non-nefarious use-case scenarios in which installing new firmware or a new OS on a WiFi enabled device would not only improve the wireless performance and stability, but would most likely make the device wholly use-able after prior dysfunction. A number of them will be from my own personal experience.

I am currently in possession of a router that has lost significant functionality since I purchased it. The original price was around \$250, so it would be a pity for it to lose complete function, but the vendor hasn't yet rectified the issues I am facing even after three or four firmware revisions. I am currently considering installing custom firmware on this device to improve its functionality and prevent me from having to purchase a brand new router that, because of my particular connectivity needs, would cost as much or more than \$250. With a newborn, \$250 is a lot of money to spend on a piece of technology I could fix myself for free with a swift firmware installation.

My wife's computer was performing poorly with her last operating system (an old and ailing copy of Windows 7). A new laptop can cost a lot of money nowadays, especially should she have desired the same level of operation and function. I wiped her hard drive clean, after backing up her files of course, and installed a brand new solid state drive and a fresh copy of Windows 7. Now, her laptop has in it a WiFi module. It is my understanding that her laptop would fall under your rule's classification as a device that can generate radio frequencies, and so my actions could be seen as illegal and fine-able. However, the only thing my actions have done is make her laptop functional where before it was not, and has assuaged the need of buying a new laptop.

In my job specifically, one of my main duties is prepping laptops and desktops for use by our user-base. The way I do this is by wiping the current operating system of the computer and then installing our customized version of Windows 7 Enterprise on them. Again, it is my understanding that this would be illegal with your rule in place. I'm sure we would

figure out a way around this as a department, but it would negatively impact the way we do business.

As an extension of the above, if installing a new operating system on a computer fresh from an OEM is made illegal, that means that consumers are at the mercy of said OEMs when it comes to pre-installed software ("bloatware"). This being the case, OEMs could potentially install invasive and harmful applications to keep track of information entered on the customer's computers for any purpose, and there would be nothing the consumer could do about it.

Currently, I am in the possession of a smartphone, which has inherent WiFi capabilities, which was not functioning a month ago. It would start, but wouldn't boot into its operating system. Something was wrong with both the OS and the firmware on the device, so I flashed a new firmware to the on-chip ROM and I installed a new operating system, a form of Android Lollipop. Now the phone works perfectly, and is completely usable once again, a device worth probably about \$200 in today's market.

Another potential victim of this ruling is the open-source Linux community at large. Without the ability to install new operating systems or firmware on WiFi capable devices, the entire community would likely die out, disbanding a vast and diverse group of talented and dedicated programmers and innovators. Without innovators, we will stagnate in the technology sector.

I am, politically speaking, in support of agency. I believe that the individual should have choice to do whatever they desire, as long as the life and prosperity of others is not in danger as a result of their decisions. This ruling sounds to me like it robs the individual of choice and provides corporations with yet another tool to use for exploitation and profit. Corporations don't need to be given more power; corporations, as it stands, have too much power already.

Please do not implement this rule. Please allow consumers to continue to have the freedom to use the software they see fit on the devices they have legally obtained. Please don't give corporations more control over our electronics. Please don't stifle innovation, and let us continue to be a land of innovators. I have admired the decisions of the current FCC over the past couple of years, and I think you are doing a wonderful job so far, in support of the free internet. Please continue to move forward, and not backward.

Respectfully yours,
Dallin Hunter

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: Rocco

Last Name: Pel

Mailing Address: Via Pinerolo

City: Milano

Country: Italy

State or Province: Milano

ZIP/Postal Code: 20151

Email Address:

Organization Name:

Comment: We want to have control over our devices, we should be able to have full access to what we pay for, we should be able to modify and customize our products in the way we please, nobody should be able to decide what WE can or cannot do with what we spent money on.

We want to have control over our devices, we should be able to have full access to what we pay for, we should be able to modify and customize our products in the way we please, nobody should be able to decide what WE can or cannot do with what we spent money on.

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: Joseph

Last Name: Heddins

Mailing Address: 518 Fleetwood Drive

City: Norman

Country: United States

State or Province: OK

ZIP/Postal Code: 73072

Email Address: joseph.heddins@ou.edu

Organization Name:

Comment: Do not restrict the freedom of the American people to use their electronic devices as they see fit. Making it illegal to install alternate Operating Systems onto machines puts the consumer at the mercy of the manufacturer, and in many cases, especially that of Android-based devices, the manufacturer does not provide key security patches. Google will not patch a critical security flaw in the web browser component of Android 4.3 and before, and these OS versions make up the majority of current Android users. Additionally, many manufacturers are not patching another security flaw in all Android operating system versions where a remote user can gain remote code execution privileges using a backdoor in MMS. This virus is known as "Stagefright" and is only patchable by the manufacturer of a device. Many devices will not be patched due to the decision of the manufacturer. Taking away the legal freedom of American citizens to install custom OS versions on their devices takes away their ability to defend themselves against malicious attacks on them and their devices.

On top of this, wireless networking research relies on the abilities of researchers to modify their devices and their operating systems. Restricting this ability will cause technological advancement to stagnate and hurt society and progress as a whole. Even users have patched serious security bugs and holes in their WiFi drivers and devices, things that would be made illegal under the proposed legislation. Users are already encouraged to not modify their own devices by manufacturers who will void a warranty for modifying the product(as they have the logical right to do so) but making it downright illegal is morally and justifiably wrong.

Billions of dollars in commerce depend on people being able to install their own software on their WiFi devices. Secure WiFi vendors, retail hotspot vendors, and other places like Internet Cafes depend on the ability of their managers and IT departments to install and run their technology as they see fit. Don't take away this freedom from Americans. Do NOT pass this proposal.

Do not restrict the freedom of the American people to use their electronic devices as they see fit. Making it illegal to install alternate Operating Systems onto machines puts the consumer at the mercy of the manufacturer, and in many cases, especially that of Android-based devices, the manufacturer does not provide key security patches. Google will not patch a critical security flaw in the web browser component of Android 4.3 and before, and these OS versions make up the majority of current Android users. Additionally, many manufacturers are not patching another security flaw in all Android operating system versions where a remote user can gain remote code execution privileges using a backdoor in MMS. This virus is known as "Stagefright" and is only patchable by the manufacturer of a device. Many devices will not be patched due to the decision of the manufacturer. Taking away the legal freedom of American citizens to install custom OS versions on their devices takes away their ability to defend themselves against malicious attacks on them and their devices.

On top of this, wireless networking research relies on the abilities of researchers to modify their devices and their operating systems. Restricting this ability will cause technological advancement to stagnate and hurt society and progress as a whole. Even users have patched serious security bugs and holes in their WiFi drivers and devices, things that would be made illegal under the proposed legislation. Users are already encouraged to not modify their own devices by manufacturers who will void a warranty for modifying the product(as they have the logical right to do so) but making it downright illegal is morally and justifiably wrong.

Billions of dollars in commerce depend on people being able to install their own software on their WiFi devices. Secure WiFi vendors, retail hotspot vendors, and other places like Internet Cafes depend on the ability of their managers and IT departments to install and run their technology as they see fit. Don't take away this freedom from Americans. Do NOT pass this proposal.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Albritton

Mailing Address: 1101 bethany ct

City: Marietta

Country: United States

State or Province: GA

ZIP/Postal Code: 30066

Email Address:

Organization Name:

Comment: Implementing this will adversely impact our technological lead in the world.

If it wasn't for hacking items which for the most part leads to innovation and the betterment of all.

I Am Against This Proposal!

Implementing this will adversely impact our technological lead in the world.

If it wasn't for hacking items which for the most part leads to innovation and the betterment of all.

I Am Against This Proposal!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Sean

Last Name: Michael

Mailing Address: 2903 Gladespring Ln

City: Dickinson

Country: United States

State or Province: TX

ZIP/Postal Code: 77539

Email Address:

Organization Name:

Comment: Please do not implement this proposal. Allow consumers to choose how they want to use their own devices that they legally own.

The philosophy behind open source software and the reasoning for modification to devices is meant to improve that physical device. Open source software is installed because the consumer is not pleased with the lack of support that their device has received. The manufacturer doesn't fix security holes in a timely manner. This leaves sensitive personal data to be vulnerable to attack and exploitation. This proposal would only exacerbate that problem because the current behavior and business practices of manufacturers will not change once the proposal is implemented.

When security holes go unfixed by the manufacturer, this drastically increases the chances of identity theft. Multiple unfixed security holes on one device increase that chance even more. That is when it falls to open source programmers to fill in the gaps that the manufacturer refuses to take responsibility for. This proposal would prohibit the individual consumer's ability to modify his or her device. This, in turn, prohibits the consumer from protecting themselves against newly developed bugs or security threats.

Please do not implement this proposal. Allow consumers to choose how they want to use their own devices that they legally own.

The philosophy behind open source software and the reasoning for modification to devices is meant to improve that physical device. Open source software is installed because the consumer is not pleased with the lack of support that their device has received. The manufacturer doesn't fix security holes in a timely manner. This leaves sensitive personal data to be vulnerable to attack and exploitation. This proposal would only exacerbate that problem because the current behavior and business practices of manufacturers will not change once the proposal is implemented.

When security holes go unfixed by the manufacturer, this drastically increases the chances of identity theft. Multiple unfixed security holes on one device increase that chance even more. That is when it falls to open source programmers to fill in the gaps that the manufacturer refuses to take responsibility for. This proposal would prohibit the individual consumer's ability to modify his or her device. This, in turn, prohibits the consumer from protecting themselves against newly developed bugs or security threats.

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: Roger

Last Name: Vortman

Mailing Address: 134 John St.

City: Santa Cruz

Country: United States

State or Province: CA

ZIP/Postal Code: 95060

Email Address: rvortman@gmail.com

Organization Name:

Comment: It isn't clear to me exactly what problem is being solved by this proposed rule, however by excluding third-party firmware on OEM wireless routers, a whole source of innovation and invention will be removed. The objective of third-party firmware isn't to allow more than the legal amount of power or to allow the illegal use of frequencies, it's to add functionality and extensibility to routers, and to provide the ability to replace the very limited OEM web admin interfaces with richer, more functional web admin interfaces.

The FCC needs to figure out exactly what it is regulating about routers, and only enact rules that affect that. If it is regulating output power, channels, and protocols, for example, then regulate those and leave other functionality and administration tools open to being re-designed and modified.

What I'm asking is for the FCC to not regulate what doesn't need to be regulated, and leave the door open for innovation and creativity in areas of wireless router functionality that don't need to be regulated.

Thank you very much for considering my opinions. They are based in many years of experience in the software and networking development world, where innovation and invention provide big benefits to users, and open up whole new area of functionality.

It isn't clear to me exactly what problem is being solved by this proposed rule, however by excluding third-party firmware on OEM wireless routers, a whole source of innovation and invention will be removed. The objective of third-party firmware isn't to allow more than the legal amount of power or to allow the illegal use of frequencies, it's to add functionality and extensibility to routers, and to provide the ability to replace the very limited OEM web admin interfaces with richer, more functional web admin interfaces.

The FCC needs to figure out exactly what it is regulating about routers, and only enact rules that affect that. If it is regulating output power, channels, and protocols, for example, then regulate those and leave other functionality and administration tools open to being re-designed and modified.

What I'm asking is for the FCC to not regulate what doesn't need to be regulated, and leave the door open for innovation and creativity in areas of wireless router functionality that don't need to be regulated.

Thank you very much for considering my opinions. They are based in many years of experience in the software and networking development world, where innovation and invention provide big benefits to users, and open up whole new area of functionality.

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: Curtis

Last Name: Aaron

Mailing Address: 23124 Alder Ln

City: California

Country: United States

State or Province: MD

ZIP/Postal Code: 20619

Email Address: bobbytehman@gmail.com

Organization Name:

Comment: Start your comment by respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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

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

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

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

Start your comment by respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joe

Last Name: Carranza

Mailing Address: 5055 Jeffreys A102

City: Las Vegas

Country: United States

State or Province: NV

ZIP/Postal Code: 89119

Email Address:

Organization Name:

Comment: Please consider leaving this tool, one that is extremely useful in helping people learn more about the machines we all use on a regular basis, in its current state.

Please consider leaving this tool, one that is extremely useful in helping people learn more about the machines we all use on a regular basis, in its current state.

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: Andre

Last Name: Bruns

Mailing Address: Schildweg 26

City: Luegde

Country: Germany

State or Province: NRW

ZIP/Postal Code: 32676

Email Address: thl@countermail.com

Organization Name:

Comment: Hello,

I am writing from Germany. I heard only recently from Your plans, that also affect the European Union.

I want to tell You, that You won't be able to get this through, because it is such a large limitation of freedom. How can You tell us, the users, which software we are allowed to use on our devices? I am sorry, but this is just a way to much.

The history shows, that firmware on WiFi devices is very likely to have security holes. At least after 2 years have passed and the manufacturer won't give support for it anymore. So this is where free software comes into account. With free software it is possible to close security leaks and by that even to reduce the waste, that would be produced when being forced to buy a new device every two years.

I understand, that interference with certain channels must be excluded, but by forcing the manufacturers to prevent people from using free software, You do not solve the problem. Why don't You try to find a solution with all countries to agree on certain frequencies for WiFi?

And by the way, a misuse of free software is illegal already now! So if somebody really wanted to keep doing so, he will be able to do it, if he is educated well enough. You want to keep people from using Linux, Cyanogenmod or OpenWRT all over the world on devices with radio connection? You use a very little number of people to make them guilty and so the very large group of people who use free software without harming anybody should be suffering from those few?

I am sorry, but this is not fair! And You have overestimated Your power.

You will not succeed in getting this through.

Hello,

I am writing from Germany. I heard only recently from Your plans, that also affect the European Union.

I want to tell You, that You won't be able to get this through, because it is such a large limitation of freedom. How can You tell us, the users, which software we are allowed to use on our devices? I am sorry, but this is just a way to much.

The history shows, that firmware on WiFi devices is very likely to have security holes. At least after 2 years have passed and the manufacturer won't give support for it anymore. So this is where free software comes into account. With free

software it is possible to close security leaks and by that even to reduce the waste, that would be produced when being forced to buy a new device every two years.

I understand, that interference with certain channels must be excluded, but by forcing the manufacturers to prevent people from using free software, You do not solve the problem. Why don't You try to find a solution with all countries to agree on certain frequencies for WiFi?

And by the way, a misuse of free software is illegal already now! So if somebody really wanted to keep doing so, he will be able to do it, if he is educated well enough. You want to keep people from using Linux, Cyanogenmod or OpenWRT all over the world on devices with radio connection? You use a very little number of people to make them guilty and so the very large group of people who use free software without harming anybody should be suffering from those few?

I am sorry, but this is not fair! And You have overestimated Your power.

You will not succeed in getting this through.

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: Sean

Last Name: Jackson

Mailing Address: 1049 Felspar St #25

City: San Diego

Country: United States

State or Province: CA

ZIP/Postal Code: 92109

Email Address:

Organization Name:

Comment: I think that any narrowing of the possible software run on any device is a bad idea and will harm innovation. By disallowing consumers to experiment with different software solutions, this proposed rule change likely will prevent new market entrants from improving upon current design themselves. It also creates an artificial market constraint which adds no value to the consumer and causes much harm.

There is no practical reason for this proposed rule change and much potential harm if implemented as written.

I think that any narrowing of the possible software run on any device is a bad idea and will harm innovation. By disallowing consumers to experiment with different software solutions, this proposed rule change likely will prevent new market entrants from improving upon current design themselves. It also creates an artificial market constraint which adds no value to the consumer and causes much harm.

There is no practical reason for this proposed rule change and much potential harm if implemented 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: Hans

Last Name: Stephensen

Mailing Address: Langebjergvej 244

City: Humlebk

Country: Denmark

State or Province: Denmark

ZIP/Postal Code: 3050

Email Address: Arngorf@gmail.com

Organization Name:

Comment: Master computer science students from Denmark here.

I'm literary shocked. But let me step down a bit to tell you why I think this must not come to pass.

If you look where new ideas and inventions originate from in areas such as engineering and computer science. It is from the small group of guys, sitting together with what seems like a fun little idea. These people cannot work under too much regulation, or they simply cannot decipher what is legal and what is not. In fact, the difference between hacking and learning from existing products on the market is indistinguishable. Using software/hardware in ways it was not meant to, is often the best way to explore possible ideas and see what is possible.

If something like this would come true in Europe, I fear I might lose interest in my current field of study.

Please do not do this. You say freedom is your thing. Well, not on this point apparently.

Kind regards,

Hans Jacob Stephensen

Master student at University of Copenhagen

Master computer science students from Denmark here.

I'm literary shocked. But let me step down a bit to tell you why I think this must not come to pass.

If you look where new ideas and inventions originate from in areas such as engineering and computer science. It is from the small group of guys, sitting together with what seems like a fun little idea. These people cannot work under too much regulation, or they simply cannot decipher what is legal and what is not. In fact, the difference between hacking and learning from existing products on the market is indistinguishable. Using software/hardware in ways it was not meant to, is often the best way to explore possible ideas and see what is possible.

If something like this would come true in Europe, I fear I might lose interest in my current field of study.

Please do not do this. You say freedom is your thing. Well, not on this point apparently.

Kind regards,

Hans Jacob Stephensen

Master student at University of Copenhagen

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: Alfred

Last Name: Farleigh

Mailing Address: 2990 W. Long Lake Rd.

City: Orleans

Country: United States

State or Province: MI

ZIP/Postal Code: 48865

Email Address:

Organization Name:

Comment: Please do not enact rules that prevent customized versions of software and firmware onto small, even commercial, RF devices.

Such restrictions will hamper innovation and bootstrapping new products in broad areas of technological opportunities, as the commercial hardware and open source software technologists have decidedly shown, in such products as router firmware and modular RF hardware.

If there is a demonstrable problem, and not responding to commercial pressure, enforcement is appropriate, not a priori wholesale ban.

Thank You for the opportunity to provide this feedback

Please do not enact rules that prevent customized versions of software and firmware onto small, even commercial, RF devices.

Such restrictions will hamper innovation and bootstrapping new products in broad areas of technological opportunities, as the commercial hardware and open source software technologists have decidedly shown, in such products as router firmware and modular RF hardware.

If there is a demonstrable problem, and not responding to commercial pressure, enforcement is appropriate, not a priori wholesale ban.

Thank You for the opportunity to provide this feedback

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: Moore

Mailing Address: 5009 Magic Lantern Dr

City: Knoxville

Country: United States

State or Province: TN

ZIP/Postal Code: 37918

Email Address: sorakiu@gmail.com

Organization Name:

Comment: Came here from hackaday. I do not want any rules that tie the hands of open firmware projects that like DD-WRT, openWRT or tomato. I personally believe projects like this have massively improved the average stability, security and speed of internet routers. Almost all consumer grade routers are insecure out of the box. Having the ability to install stable, reliable and secure firmware from one of these projects is the only way I will allow one of these devices in my house.

I strongly recommend that we prioritize these kinds of efforts over any other kinds of rules, regulations, etc.

Came here from hackaday. I do not want any rules that tie the hands of open firmware projects that like DD-WRT, openWRT or tomato. I personally believe projects like this have massively improved the average stability, security and speed of internet routers. Almost all consumer grade routers are insecure out of the box. Having the ability to install stable, reliable and secure firmware from one of these projects is the only way I will allow one of these devices in my house.

I strongly recommend that we prioritize these kinds of efforts over any other kinds of rules, regulations, etc.

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: Noah

Last Name: Greenstein

Mailing Address: 72 Lefurgy Ave.

City: Dobbs Ferry

Country: United States

State or Province: NY

ZIP/Postal Code: 10522

Email Address:

Organization Name:

Comment: The danger from not having the securest and most up technologically up to date computer systems far outweighs the benefit from controlling the wireless spectrum. Nearly all the state of the art networking systems would be critically hindered if open access was taken away. Protection from internet threats is much more important nowadays than the potential for local abuse of the wireless spectrum.

The danger from not having the securest and most up technologically up to date computer systems far outweighs the benefit from controlling the wireless spectrum. Nearly all the state of the art networking systems would be critically hindered if open access was taken away. Protection from internet threats is much more important nowadays than the potential for local abuse of the wireless spectrum.

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: Roger

Last Name: Ruminski

Mailing Address: 1885 chapel hills drive

City: Colorado Springs

Country: United States

State or Province: CO

ZIP/Postal Code: 80920

Email Address: teh.dbgtrgr@gmail.com

Organization Name:

Comment: I believe that when I purchase a device designed for personal computing I should be able to put whatever software on it that I like. This is especially true in this world we live in where exploits and security holes are discovered everyday and manufacturers are complacent and don't fix any of them in their software in a timely manner, putting me at risk. Whereas usermade software can be patched on the fly without needing the slow middleman manufacturer.

I own the device, I should be able to do with it what I please.

I believe that when I purchase a device designed for personal computing I should be able to put whatever software on it that I like. This is especially true in this world we live in where exploits and security holes are discovered everyday and manufacturers are complacent and don't fix any of them in their software in a timely manner, putting me at risk. Whereas usermade software can be patched on the fly without needing the slow middleman manufacturer.

I own the device, I should be able to do with it what I please.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Moretti

Mailing Address: 120 Meshanticut Valley Pkwy

City: Cranston

Country: United States

State or Province: RI

ZIP/Postal Code: 02920

Email Address: thekillerdonut1@aol.com

Organization Name:

Comment: Restricting the use of custom and/or open source operating systems and router firmware to address the problem of people using bands they shouldn't use is like nuking the entire country of Switzerland to prevent off-shore bank accounts; It would cause much more harm than good, and still wouldn't really even address the issue.

I use a free and open source Linux based operating system to do my work every single day. All of my devices get internet through a router using free and open source firmware that I have custom configured. It should be noted that if I set my router's region to the United States, it already restricts my ability to use RF channels that are not allowed for civilian use in the USA.

Anybody who wants to maliciously abuse those restricted channels will be able to regardless of whether or not that firmware is restricted. Even hardware locking routers to prevent custom firmware installation will not work, because a malicious user could just build their own device to transmit on the banned RF frequencies.

All banning these custom firmwares will do is prevent legitimate users like myself from getting the most out of their hardware. In the case of restricting Linux installations on PCs, that would bring my work to a screeching halt, and fly in the face of the very concept of "Freedom".

Restricting the use of custom and/or open source operating systems and router firmware to address the problem of people using bands they shouldn't use is like nuking the entire country of Switzerland to prevent off-shore bank accounts; It would cause much more harm than good, and still wouldn't really even address the issue.

I use a free and open source Linux based operating system to do my work every single day. All of my devices get internet through a router using free and open source firmware that I have custom configured. It should be noted that if I set my router's region to the United States, it already restricts my ability to use RF channels that are not allowed for civilian use in the USA.

Anybody who wants to maliciously abuse those restricted channels will be able to regardless of whether or not that firmware is restricted. Even hardware locking routers to prevent custom firmware installation will not work, because a malicious user could just build their own device to transmit on the banned RF frequencies.

All banning these custom firmwares will do is prevent legitimate users like myself from getting the most out of their hardware. In the case of restricting Linux installations on PCs, that would bring my work to a screeching halt, and fly in the face of the very concept of "Freedom".

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Shazedur Rahim

Last Name: Joardar

Mailing Address: HOUSE NAME#THIKANA, JOYNABARHI, HEMAYETPUR, SAVAR

City: DHAKA

Country: Bangladesh

State or Province: DHAKA

ZIP/Postal Code: 1340

Email Address: toshazed@gmail.com

Organization Name: FOSS Bangladesh

Comment: As an user, I object this for the following 4 reasons, mainly.

1. Digital Freedom: I want to have control over my devices as long as I want. It is my right. I use GNU+Linux, CyanogenMod/Replicant and OpenWRT on my devices. I want to use Free/Libre and Open Source Software on my devices. But if this proposal passes, we won't be able to do that. As a result, we won't have control over our devices rather NSA/FBI/CIA may have the control and may peep on our communication data. So, please, don't take that personal freedom from us.

2. Security: If this proposal passes, I am sure there will be more security problems. As we all have to rely on the devices vendors to fix bugs and vulnerabilities, we all need to wait for a certain time for those patches and to just rely on them. And most of the time, the vendors don't care about this, they neglect our security problems. But I want to rely on the Free/Libre and Open Source community. Because they try their best to release patches as soon as 0-day it becomes public. So, my digital security is a big concern to me. That's why I request you to stop this.

3. Privacy: If this proposal passes, we all have to use what the manufacturers only provide us with. But we will never know what we are running. The manufacturers may provide us with programs with malicious functionalities. We shouldn't trust them blindly, right? Even if we find out that they're providing us with malwares, we won't be able to remove/change/fix that. So, it'd be nice if we can modify and really of our own for the devices we are working/using.

4. On Emergency: In any country, we often get hit by natural disasters, right? Suppose, a country gets hit badly by an massive earth quake. Then how people can still get connected with each other? Yes, by creating a wireless mesh network. But if the current proposal by you passes, it'll be illegal to do that. So, please, don't pass the proposal.

In short, I object this proposal because digital freedom, data and communication security and my privacy is **very much important** to me. Please, stop your current vulnerable proposal as it is affecting me and the mass people on this globe who are with the wireless technology and get ready to save the WiFi, our WiFi.

As an user, I object this for the following 4 reasons, mainly.

1. Digital Freedom: I want to have control over my devices as long as I want. It is my right. I use GNU+Linux, CyanogenMod/Replicant and OpenWRT on my devices. I want to use Free/Libre and Open Source Software on my devices. But if this proposal passes, we won't be able to do that. As a result, we won't have control over our devices rather NSA/FBI/CIA may have the control and may peep on our communication data. So, please, don't take that personal freedom from us.

2. Security: If this proposal passes, I am sure there will be more security problems. As we all have to rely on the devices vendors to fix bugs and vulnerabilities, we all need to wait for a certain time for those patches and to just rely on them. And most of the time, the vendors don't care about this, they neglect our security problems. But I want to rely on the Free/Libre and Open Source community. Because they try their best to release patches as soon as 0-day it becomes public. So, my digital security is a big concern to me. That's why I request you to stop this.

3. Privacy: If this proposal passes, we all have to use what the manufacturers only provide us with. But we will never know what we are running. The manufacturers may provide us with programs with malicious functionalities. We shouldn't trust them blindly, right? Even if we find out that they're providing us with malwares, we won't be able to remove/change/fix that. So, it'd be nice if we can modify and really of our own for the devices we are working/using.

4. On Emergency: In any country, we often get hit by natural disasters, right? Suppose, a country gets hit badly by an massive earth quake. Then how people can still get connected with each other? Yes, by creating a wireless mesh network. But if the current proposal by you passes, it'll be illegal to do that. So, please, don't pass the proposal.

In short, I object this proposal because digital freedom, data and communication security and my privacy is **very much important** to me. Please, stop your current vulnerable proposal as it is affecting me and the mass people on this globe who are with the wireless technology and get ready to save the WiFi, our WiFi.

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: Colson

Mailing Address: Derryrush

City: Rosmuc

Country: Ireland

State or Province: Galway

ZIP/Postal Code: 0000

Email Address:

Organization Name:

Comment: I would respectfully like to ask you, the FCC to not implement any such rule that would prohibit the installation of custom firmware on wifi capable devices.

Doing so would be a great damage to the furthering of mankind's knowledge and understand. It would prevent better software, computers, and wifi technology from being developed and likely cause the tech industry to stagnate as intelligent individuals would have no effect on our future, instead allowing monopolies to occur.

This, however, is not the only issue resulting from this proposal. Security loopholes in technology, which could be damaging to business, or even government property would not be as easy to fix when technology is locked down and cannot be changed. Imagine the consequences of companies being attacked and compromised because they couldn't do anything about a security loophole they knew about.

Please consider this very carefully. I very strongly believe this proposal should not be passed. I'd like to think you agree with my points.

I would respectfully like to ask you, the FCC to not implement any such rule that would prohibit the installation of custom firmware on wifi capable devices.

Doing so would be a great damage to the furthering of mankind's knowledge and understand. It would prevent better software, computers, and wifi technology from being developed and likely cause the tech industry to stagnate as intelligent individuals would have no effect on our future, instead allowing monopolies to occur.

This, however, is not the only issue resulting from this proposal. Security loopholes in technology, which could be damaging to business, or even government property would not be as easy to fix when technology is locked down and cannot be changed. Imagine the consequences of companies being attacked and compromised because they couldn't do anything about a security loophole they knew about.

Please consider this very carefully. I very strongly believe this proposal should not be passed. I'd like to think you agree with my points.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Wayne

Last Name: Mead

Mailing Address: 3831 Canton Dr.

City: Pearland

Country: United States

State or Province: TX

ZIP/Postal Code: 77584

Email Address: isk@imsorrykun.com

Organization Name: null

Comment: This is very concerning and I think there are a few points that will damage the security of communications in the future and hinder development of improved technologies.

As we have seen in the pass open platform modifications have developed more technologies that have been adopted as system standards by other companies. I see restricting installation of 3rd party operating systems and utilities on devices like these rules propose or at least don't explicitly protect, as a risk to the end users. Software like FreeBSD, DDWRT, GNU/Linux, OpenBSD, and other community based tools can hinder development by damaging user base, and user test base.

Custom firmware on phones can fix issues with a users current phone systems that can improve security of the end user, as well as allow options for end of life uses.

Finally this allows manufacturers to in effect own devices bought by the end user. This is dangerous and disingenuous to the end user who believe they own the device.

This is very concerning and I think there are a few points that will damage the security of communications in the future and hinder development of improved technologies.

As we have seen in the pass open platform modifications have developed more technologies that have been adopted as system standards by other companies. I see restricting installation of 3rd party operating systems and utilities on devices like these rules propose or at least don't explicitly protect, as a risk to the end users. Software like FreeBSD, DDWRT, GNU/Linux, OpenBSD, and other community based tools can hinder development by damaging user base, and user test base.

Custom firmware on phones can fix issues with a users current phone systems that can improve security of the end user, as well as allow options for end of life uses.

Finally this allows manufacturers to in effect own devices bought by the end user. This is dangerous and disingenuous to the end user who believe they own the device.

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: Amanda

Last Name: Krue

Mailing Address: 1117 Laurel Ave Apt 6

City: Knoxville

Country: United States

State or Province: TN

ZIP/Postal Code: 37916

Email Address: skweeds@gmail.com

Organization Name:

Comment: This is a terrible idea.

If the government enacts something like this, we will be as bad as the totalitarian overlords in dystopian speculative fiction novels.

People need to be creative. That's what makes America successful.

Laws like this that restrict an individual's use of technology on his or her own machine should be considered as alarming as laws that shut down all public libraries.

Income inequality is bad enough. Don't make it worse.

This is a terrible idea.

If the government enacts something like this, we will be as bad as the totalitarian overlords in dystopian speculative fiction novels.

People need to be creative. That's what makes America successful.

Laws like this that restrict an individual's use of technology on his or her own machine should be considered as alarming as laws that shut down all public libraries.

Income inequality is bad enough. Don't make it worse.

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: Joseph

Last Name: Liverance

Mailing Address: P.O. Box 604

City: Ellettsville

Country: United States

State or Province: IN

ZIP/Postal Code: 47429

Email Address: jarlie63@gmail.com

Organization Name:

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

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

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

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

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.

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

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

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

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

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: Harrison

Last Name: Wojcik

Mailing Address: 1262 Birch Pond Trail

City: White Bear Lake

Country: United States

State or Province: MN

ZIP/Postal Code: 55110

Email Address: null

Organization Name: null

Comment: Greetings FCC comment reader. I am writing to respectfully request that you not implement rules that take away my ability to install the software of my choosing on my computing devices.

There are 4 points which were brought to my attention regarding this matter, with all of which I agree wholeheartedly. They are:

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

I also believe that the backbone of American commerce lies in free invention and experimentation. New inventors will be hamstrung in their attempts to revolutionize the computing industry without the ability to create new operating systems or install custom software on devices that they own. Please let America work to resume its place at the forefront of innovation and technology.

Thank you for your consideration.

Greetings FCC comment reader. I am writing to respectfully request that you not implement rules that take away my ability to install the software of my choosing on my computing devices.

There are 4 points which were brought to my attention regarding this matter, with all of which I agree wholeheartedly. They are:

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

I also believe that the backbone of American commerce lies in free invention and experimentation. New inventors will be hamstrung in their attempts to revolutionize the computing industry without the ability to create new operating systems or install custom software on devices that they own. Please let America work to resume its place at the forefront of innovation and technology.

Thank you for your consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Nobile

Mailing Address: 155 Elmwood Avenue

City: Hanover

Country: United States

State or Province: PA

ZIP/Postal Code: 17331

Email Address: nobility33@gmail.com

Organization Name:

Comment: This needs to remain an option. I never get updates on any commercial grade router. This is a huge security risk. The most important thing you can do to prevent being "hacked" is install updates. The open source alternative however gives me regular updates. It's that simple. There are numerous other reasons why, however I just wanted to give this simple real world example.

This needs to remain an option. I never get updates on any commercial grade router. This is a huge security risk. The most important thing you can do to prevent being "hacked" is install updates. The open source alternative however gives me regular updates. It's that simple. There are numerous other reasons why, however I just wanted to give this simple real world example.

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: D

Last Name: Lue Choy

Mailing Address: Crescent

City: Stouffville

Country: Canada

State or Province: Ontario

ZIP/Postal Code: l4a0a3

Email Address: dluechoy@gmail.com

Organization Name: null

Comment: The preposed rules that are designed not to permit any subsequent software changes without an application to obtain a new FCC ID and certification are insufficiently flexible to accommodate current common practices, including vendor and open-source development.

Ignoring open-source and research development, which I presume will have their own protections, as European lawmakers have considered in their regulations--

Often companies will rush a product to market using off-the-shelf components, including SDRs, and the integration of these components are often done piecemeal and are far from perfect in their implementation in ways that are not apparent in limited number of specific test cases/modes that can be challenged during any rigorous certification process.

The generic Wi-Fi router for example can be 'manufactured' by hundreds of companies using a very limited set of off-the-shelf components designed for the purpose, but each will have their own implementation of the software that handles interfacing the wired to the wireless.

But other appliances will have other functions, that will also be affected by software, and software glitches.

This leads to the crux of the problem I see in the current wording of the proposed changes:

an exceedingly broad definition for "software". For a microwave manufacturer to fix a timer not shutting off, or beeping randomly every n hours uncommanded, this would require a software modification better known as a patch. For an automobile that has a potentially fatal software-controlled battery charger problem requiring a patch, would run afoul of this rule for any wireless or radio module it may contain.

And compartmentalizing the SCR into its own module does not alleviate the conflict in the wording as "software" permeates everything connected digitally, where does the radio end in an integrated system?

Wording that specifically focuses on the software functions/routines that directly affect radio operation, and hardening/segregating shared resources from the rest of the system and hardware would be preferable to "software".

Ignoring the broad definition of software; specifying resistance to unauthorized software / prohibiting software modification, except for specific named entities at filing, is extremely impractical.

Without reverting to the use of ROMs as was the accepted norm in the 80's software on devices will inherently be malleable when it reaches the consumer. But given the inherently incomplete condition of software both because of hap-hazard design but also evolving protocol/larger software conventions, ROMs are both unacceptable in terms of cost to iterate, but also in functionality/significantly increased obsolescence rate.

Cryptographic signing of software to processors using keys is an option, however integrating this would require hardware component manufacturers to integrate these from the very beginning. This will take many years for existing stock to deplete while new hardware is developed to replace it; Assuming that companies won't continue to manufacture generic (unlocked/weakly locked) processors for manufacturers who will continue to make non-conformant goods for sale onto the grey market where it will still proliferate throughout the continent.

I would like to also argue that combined with the requirement tying manufacturer to hardware to a very limited subset of possible companies, this would destroy the commodity market that has allowed development to flourish -- but we have DVD's and region locking as an example of cryptographic software (video) being locked to a limited number of licensed companies using keys. In practice companies produced appropriately region locked players, and consumers would buy the appropriate region locked media-- and various groups reverse engineered (or extracted) the keys, manufacturers responded by invalidating the compromised keys causing innocent consumers to lose the use of the legally obtained players and media, while third parties then stepped to the next key...
So that won't work.

Compounding this, is that often companies will go out of business or abandon product lines, and consumers may require software updates to avoid obsolescence or for their own protection. Software intended for a non-specific type of processor/hardware would be interoperable, and conformant, however the rules as stated would not permit it sue.

A rational compromise might be to clearly separate definition of into program & configuration, and hardware-functions (incl shared resources) from all other software.

This will allow the relevant hardware-functions to be integrity checked internally or by hidden rules and for that hardware-software to reject invalid/nonconformant configuration, while configuration data is free to be modified by vendors rebranding their nonsense, and other software (that happens to be on the same device) to be modified without burdening everyone with recertification.

Opensource will continue NNY

The proposed rules that are designed not to permit any subsequent software changes without an application to obtain a new FCC ID and certification are insufficiently flexible to accommodate current common practices, including vendor and open-source development.

Ignoring open-source and research development, which I presume will have their own protections, as European lawmakers have considered in their regulations--

Often companies will rush a product to market using off-the-shelf components, including SDRs, and the integration of these components are often done piecemeal and are far from perfect in their implementation in ways that are not apparent in limited number of specific test cases/modes that can be challenged during any rigorous certification process.

The generic Wi-Fi router for example can be 'manufactured' by hundreds of companies using a very limited set of off-the-shelf components designed for the purpose, but each will have their own implementation of the software that handles

interfacing the wired to the wireless.

But other appliances will have other functions, that will also be affected by software, and software glitches.

This leads to the crux of the problem I see in the current wording of the proposed changes:

an exceedingly broad definition for "software". For a microwave manufacturer to fix a timer not shutting off, or beeping randomly every n hours uncommanded, this would require a software modification better known as a patch. For an automobile that has a potentially fatal software-controlled battery charger problem requiring a patch, would run afowl of this rule for any wireless or radio module it my contain.

And compartmentalizing the SCR into its own module does not alleviate the conflict in the wording as "software" permeates everything connected digitally, where does the radio end in an integrated system?

Wording that specifically focuses on the software functions/routines that directly affect radio operation, and hardening/segregating shared resouces from the rest of the system and hardware would be preferable to "software".

Ignoring the broad definition of software; specifying resistance to unauthorized software / prohibiting software modification, except for specific named entities at filing, is extremely impractical.

Without reverting to the use of ROMs as was the accepted norm in the 80's software on devices will inheriently be malleable when it reaches the consumer. But given the inherently incomplete condition of software both because of hap-hazard design but also evolving protocol/larger software conventions, ROMs are both unacceptable in terms of cost to iterate, but also in functionality/significantly increased obsolesence rate.

Cryptographic signing of software to processors using keys is an option, however integrating this would require hardware component manufacturers to integrate these from the very beginning. This will take many years for existing stock to deplete while new hardware is developed to replace it; Assuming that companies won't continue to manufacture generic (unlocked/weakly locked) processors for manufacturers who will continue to make non-conformant goods for sale onto the grey market where it will still proliferate throughout the continent.

I would like to also argue that combined with the requirement tying manufacturer to hardware to a very limited subset of possible companies, this would destroy the commodity market that has allowed development to flourish -- but we have DVD's and region locking as an example of ctypographic software (video) being locked to a limited number of licensed companes using keys. In practise companies produced appropriately region locked players, and consumers would buy the appropriate region locked media-- and various groups reverse engineered (or extracted) the keys, manufactures responded by invalidating the compromised keys causing innocent consumers to lose the use of the legally obtained players and media, while third parties then stepped to the next key...
So that won't work.

Compounding this, is that often companies will gou out of business or apandon product lines, and consumers may require software updates to avoid obsolesence or for their own protection. Software intended for a non-specific type of processor/hardware would be interoperatable, and conformant, however the rules as stated would not permit it sue.

A rational compromise might be to clearly seperate definition of into program & configuration, and harware-functions (incl shared resources) from all other software.

This will allow the relevant hardware-functions to be integrity checked internally or by hidden rules and for that hardware-software to reject invalid/nonconformant configuration, while configuration data is free to be modified by vendors rebranding their nonsense, and other software (that happens to be on teh same device) to be modified without burdening everyone with recertification.

Opensource will continue NNY

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: TJ

Last Name: Schneider

Mailing Address: 295 Elbo Lane

City: Cherry Hill

Country: United States

State or Province: NJ

ZIP/Postal Code: 08054

Email Address:

Organization Name:

Comment: I do not think it is a wise decision to implement rules that take away the ability for users to install software that they chose on computing devices.

In order to advance our technology, researchers need to install their own modifications to the devices they use, in order to test limits, and see what is possible. We will be stuck in the past if this is implemented.

If there is an issue with your device, and the company neglects to fix it, some people must do it on their own, as otherwise they could be vulnerable to a multitude of things depending on each situation.

In the past there have been some key examples of this, that would be potentially banned by this document.

Tons of things rely on things that would be removed, such as secure wifi, hotspots at retail, ect. All these would not exist if this document was passed.

I do not think it is a wise decision to implement rules that take away the ability for users to install software that they chose on computing devices.

In order to advance our technology, researchers need to install their own modifications to the devices they use, in order to test limits, and see what is possible. We will be stuck in the past if this is implemented.

If there is an issue with your device, and the company neglects to fix it, some people must do it on their own, as otherwise they could be vulnerable to a multitude of things depending on each situation.

In the past there have been some key examples of this, that would be potentially banned by this document.

Tons of things rely on things that would be removed, such as secure wifi, hotspots at retail, ect. All these would not exist if this document was passed.

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: H.R.

Last Name: Shadhin

Mailing Address: 63/3 , Lake Circus ,Kalabagan, Dhanmondi

City: Dhaka

Country: Bangladesh

State or Province: Dhaka

ZIP/Postal Code: 1207

Email Address: hrshadhin.i386@gmail.com

Organization Name: ShanixLab

Comment: I object this because security and privacy is **important** to me

I object this because security and privacy is **important** to me

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Gabriel

Last Name: Parmley

Mailing Address: 1686 N Stella Ave, Apt 13

City: Wenatchee

Country: United States

State or Province: WA

ZIP/Postal Code: 98801

Email Address: gabeparmley@gmail.com

Organization Name: null

Comment: I request that customization and modification of software/firmware not be restricted for wireless devices. The ability for the public community to implement new features and bug/vulnerability patches, without the need to wait for hardware vendors to release patches, is critical.

Many times in the past severe bugs and security vulnerabilities have been able to be patched by the public community before hardware vendors were able to officially patch them. Allowing the public community to build their own software/firmware and/or modify existing software/firmware makes it possible to find and/or prevent vulnerabilities before hardware vendors ever would.

I propose that the FCC find an alternative to enforcing radio regulations. Whether it be working with the public community to implement enforcement into public software/firmware and/or working with hardware vendors to create software/firmware that would only be responsible for enforcing the legal requirements for the hardware, but allowing the public community to have the option to be responsible for the rest of the software/firmware.

Overall, I believe globally restricting custom and modified software/firmware is too strict and excessive and enforcing legal requirements should be done in a more precise action.

I request that customization and modification of software/firmware not be restricted for wireless devices. The ability for the public community to implement new features and bug/vulnerability patches, without the need to wait for hardware vendors to release patches, is critical.

Many times in the past severe bugs and security vulnerabilities have been able to be patched by the public community before hardware vendors were able to officially patch them. Allowing the public community to build their own software/firmware and/or modify existing software/firmware makes it possible to find and/or prevent vulnerabilities before hardware vendors ever would.

I propose that the FCC find an alternative to enforcing radio regulations. Whether it be working with the public community to implement enforcement into public software/firmware and/or working with hardware vendors to create software/firmware that would only be responsible for enforcing the legal requirements for the hardware, but allowing the public community to have the option to be responsible for the rest of the software/firmware.

Overall, I believe globally restricting custom and modified software/firmware is too strict and excessive and enforcing legal requirements should be done in a more precise action.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Cloos

Mailing Address: 3742 E Main Rd Lot 3

City: Fredonia

Country: United States

State or Province: NY

ZIP/Postal Code: 14063

Email Address: cloos@jhcloos.com

Organization Name: null

Comment: The ability for those who purchase hardware capable of using IEEE 802.11 and similar radio technologies to have full and unfettered control of the software they run on their hardware is vital both to ensure continued innovation and to ensure security.

Commercial software, especially for consumer hardware, is written on a deadline, buggy and never gets updates. The vendors just move on to new hardware products.

FLOSS software, on the other hand, is written and maintained by those who actually use the hardware and care about how well it works. The fact that the source code is public helps ensure that bugs get fixed and the floss culture tends to ensure that those fixes get deployed.

The proposed regulation will only cause harm to the public. The public will not benefit from it.

1] https://en.wikipedia.org/wiki/Alternative_terms_for_free_software

The ability for those who purchase hardware capable of using IEEE 802.11 and similar radio technologies to have full and unfettered control of the software they run on their hardware is vital both to ensure continued innovation and to ensure security.

Commercial software, especially for consumer hardware, is written on a deadline, buggy and never gets updates. The vendors just move on to new hardware products.

FLOSS software, on the other hand, is written and maintained by those who actually use the hardware and care about how well it works. The fact that the source code is public helps ensure that bugs get fixed and the floss culture tends to ensure that those fixes get deployed.

The proposed regulation will only cause harm to the public. The public will not benefit from it.

1] https://en.wikipedia.org/wiki/Alternative_terms_for_free_software

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nathan

Last Name: Rathbun

Mailing Address: 1299 Heatherwood Lane

City: Ann Arbor

Country: United States

State or Province: MI

ZIP/Postal Code: 48108

Email Address:

Organization Name:

Comment: This proposal is both backwards-thinking and clearly does not favor citizens. It should in no way be moved forward nor enacted. The constant encroachment of private enterprise onto the rights of citizens to make basic choices in their technology is stifling to technological advancement, personal freedom and the general prosperity of our country. Do not pass this proposal. Do not propose more like it. And quit giving your ears and time to corporations who want to control technology instead of the users who rightfully own their own devices.

This proposal is both backwards-thinking and clearly does not favor citizens. It should in no way be moved forward nor enacted. The constant encroachment of private enterprise onto the rights of citizens to make basic choices in their technology is stifling to technological advancement, personal freedom and the general prosperity of our country. Do not pass this proposal. Do not propose more like it. And quit giving your ears and time to corporations who want to control technology instead of the users who rightfully own their own 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: Adam

Last Name: Downey

Mailing Address: 103 Williams Dr.

City: Bonaire

Country: United States

State or Province: GA

ZIP/Postal Code: 31005

Email Address:

Organization Name:

Comment: I, Adam Downey, do respectfully ask the FCC to not implement rules that take away the ability of users to install the software and or firmware of their choosing on their computing devices.

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

I understand fully that devising a way to prevent radios and devices from operating outside of authorized frequencies is an important and arduous task to accomplish. Please do not inhibit the law abiding citizens from being able to work on their equipment, when, regardless of laws put in place now or in the future, criminals will continue to accomplish illegal use of radios and devices. You stand currently to only inhibit the good and law abiding citizens whilst doing nothing to those you intend to corral.

I, Adam Downey, do respectfully ask the FCC to not implement rules that take away the ability of users to install the software and or firmware of their choosing on their computing devices.

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

I understand fully that devising a way to prevent radios and devices from operating outside of authorized frequencies is an important and arduous task to accomplish. Please do not inhibit the law abiding citizens from being able to work on their equipment, when, regardless of laws put in place now or in the future, criminals will continue to accomplish illegal use of radios and devices. You stand currently to only inhibit the good and law abiding citizens whilst doing nothing to those you intend to corral.

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: Knapp

Mailing Address: 7607 called real

City: Goleta

Country: United States

State or Province: CA

ZIP/Postal Code: 93117

Email Address: jaknapp8@gmail.com

Organization Name:

Comment: Preventing the installation of open source software on anything is absurd.

Routers are the gateway for internet in a household, all traffic from and to that household goes through that router. The only way to prevent spyware from being installed on a router is to install trusted open source software. Preventing people from installing trusted software will only result in more spyware! If you truly wanted to secure the future of trusted computing and internet access, you would require router manufacturers to open source their radio & modem drivers so we could be assured there is nothing malicious hidden within. These proposed limitations would not even hinder someone who wanted to illegally broadcast in the WiFi spectrum, they only make the internet less safe.

Preventing the installation of open source software on anything is absurd.

Routers are the gateway for internet in a household, all traffic from and to that household goes through that router. The only way to prevent spyware from being installed on a router is to install trusted open source software. Preventing people from installing trusted software will only result in more spyware! If you truly wanted to secure the future of trusted computing and internet access, you would require router manufacturers to open source their radio & modem drivers so we could be assured there is nothing malicious hidden within. These proposed limitations would not even hinder someone who wanted to illegally broadcast in the WiFi spectrum, they only make the internet less safe.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ryan

Last Name: Lutz

Mailing Address: 845 E Chestnut Ave

City: Orange

Country: United States

State or Province: CA

ZIP/Postal Code: 92867

Email Address: ryan.lutz37@gmail.com

Organization Name:

Comment: Please do not enact this legislation as it will restrict the creative and scientific output that this country already sorely lacks. I flash my routers' firmware with open source firmware occasionally, and the idea that the FCC is trying to prohibit this seems like something only a Big Brother-type department would do.

Please do not enact this legislation as it will restrict the creative and scientific output that this country already sorely lacks. I flash my routers' firmware with open source firmware occasionally, and the idea that the FCC is trying to prohibit this seems like something only a Big Brother-type department would do.

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: Airley

Mailing Address: Dine@20hz.co.uk

City: Guildford

Country: United Kingdom

State or Province: Surrey

ZIP/Postal Code: Gu1 4dl

Email Address: Dine@20hz.co.uk

Organization Name: Showave ltd

Comment: This is draconian. How are the generations of self taught engineers going to learn without access to the hardware they bought and thus own?

Another proposal written by people who don't understand computing of the history of.

This is draconian. How are the generations of self taught engineers going to learn without access to the hardware they bought and thus own?

Another proposal written by people who don't understand computing of the history of.

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: Ferdia

Last Name: O'Neill

Mailing Address: Yes.

City: Dublin

Country: Ireland

State or Province: n/a

ZIP/Postal Code: n/a

Email Address:

Organization Name:

Comment: This proposal is a terrible idea and would impede the development of many aspects of wireless communication, as well as restricting those wishing not to be forced to you windows or OS x

This proposal is a terrible idea and would impede the development of many aspects of wireless communication, as well as restricting those wishing not to be forced to you windows or OS x

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: Homer

Last Name: Reed

Mailing Address: 2635 Barham Rd. SW

City: Roanoke

Country: United States

State or Province: VA

ZIP/Postal Code: 24015

Email Address: cullen.reed@gmail.com

Organization Name:

Comment: Respectfully this is a bad idea. It severely inhibits innovation and gives access to the very few. This is obviously a rule designed to do that so that a few companies can capture more market share. Making rules like this seriously endanger our democracy, privacy and freedoms.

Respectfully this is a bad idea. It severely inhibits innovation and gives access to the very few. This is obviously a rule designed to do that so that a few companies can capture more market share. Making rules like this seriously endanger our democracy, privacy and freedoms.