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: Joshua
Last Name: Henry
Mailing Address: 105 Sue Ann CT.
City: Sterling
Country: United States
State or Province: VA
ZIP/Postal Code: 20164
Email Address: hipufiamiumi@gmail.com
Organization Name:
Comment: Wireless networking research depends on the ability of researchers to investigate and modify their devices. Without the ability to modify devices, the cost of researching wireless networking devices will skyrocket. This will likely create a barrier, preventing individuals from learning on their own, and will stunt innovation. This also prevents anyone other than the manufacturer from testing, finding, and patching security flaws in devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. There are thousands of instances of this happening, and poses a much greater security risk than the one that this proposed regulation addresses. Users of the devices 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, and until such a time; a regulation that will effectively ban open source firmwares is unwarranted and purposeless.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Without the ability to modify devices, the cost of researching wireless networking devices will skyrocket. This will likely create a barrier, preventing individuals from learning on their own, and will stunt innovation. This also prevents anyone other than the manufacturer from testing, finding, and patching security flaws in devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. There are thousands of instances of this happening, and poses a much greater security risk than the one that this proposed regulation addresses. Users of the devices 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, and until such a time; a regulation that will effectively ban open source firmwares is unwarranted and purposeless.

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: Floyd
Last Name: Bass
Mailing Address: 3120 Ave. U N.W.
City: Winter Haven
Country: United States
State or Province: FL
ZIP/Postal Code: 33881
Email Address:
Organization Name:
Comment: Please don't do this - it's bad for individual freedom and for technological progress, infringes upon the freedom of individual users of electronic devices, and it will be vastly detrimental to the vast majority of American users of these technologies.

Please don't do this - it's bad for individual freedom and for technological progress, infringes upon the freedom of individual users of electronic devices, and it will be vastly detrimental to the vast majority of American users of these technologies.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Michael
Last Name: Douglas
Mailing Address: 1 Hall Terrace
City: Bedford Park
Country: Australia
State or Province: South Australia
ZIP/Postal Code: 5042
Email Address:
Organization Name:
Comment: This proposal is completely ridiculous. A complete violation of Freedom.

This proposal is completely ridiculous. A complete violation 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: Joshua
Last Name: Cain
Mailing Address: 1512 Thomas Drive, Apartment 6
City: Bellevue
Country: United States
State or Province: NE
ZIP/Postal Code: 68005
Email Address:
Organization Name: Managed.com
Comment: To whom it may concern,

Why must we lock down devices? Is exploring another operating system or updating to a different firmware under warranty illegal? No, this must stop. The reason why people modify the devices is because the firmware provided by the manufacturer is sorely lacking in features. In this day and age, base configuration is unacceptable. If this also applies to OSes, you just lost a lot of the PC users in the US. The reason I comment is because Open Firmware provides the customers to assist the manufacturers with flaws they added in or to show off features that the manufacturers never knew they could add in. If you do this, Android itself is illegal, thus shutting down the wireless companies here in the US who develop custom versions to add to their hardware.

To whom it may concern,

Why must we lock down devices? Is exploring another operating system or updating to a different firmware under warranty illegal? No, this must stop. The reason why people modify the devices is because the firmware provided by the manufacturer is sorely lacking in features. In this day and age, base configuration is unacceptable. If this also applies to OSes, you just lost a lot of the PC users in the US. The reason I comment is because Open Firmware provides the customers to assist the manufacturers with flaws they added in or to show off features that the manufacturers never knew they could add in. If you do this, Android itself is illegal, thus shutting down the wireless companies here in the US who develop custom versions to add to their hardware.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: David
Last Name: Whitcombe
Mailing Address: 735 Ute Ave
City: Rifle
Country: United States
State or Province: CO
ZIP/Postal Code: 81650
Email Address:
Organization Name:
Comment: While the intentions of more tightly regulating consumer radio devices using the bands occupied by Wireless Devices (typically under the 802.11 scheme) may seem like a good idea, implementing it well may be very, very difficult. As it currently stands, the proposed rule would prohibit several of the things that I do every day in my home, while staying within FCC regulations.
In other words, the modifications to the software that I've made to devices in my home allow: my phone to actually work (CyanogenMod), my wireless routers to talk to one another quite efficiently (DD-WRT), and devices I build myself using microprocessors which can seamlessly connect to my network. I am only able to do this by using software of my own design (or designed by others) to modify the firmware in these devices.

The DMCA made it illegal to fix your own tractor. I'm pretty sure the authors of that legislation didn't intend that as an effect of the law, but it does, and it does a lot of other horrible things as well.

Tightening regulations is fine, but this has side-effects that could be much worse than leaving the regulations as they are.

If writing custom firmware might permit me to turn a well-behaved device (as far as the spectrum is concerned) into an ill-behaved device, there are lots of other things that I could do (which would be far easier than writing firmware) to exhibit bad behavior.

Concluding: This proposal will adversely effect innovation in electronics, network security, home automation, mobile networks, and people's everyday, happy lives. Some end users of electronics (though not all, to be sure) have as much experience and expertise as the companies which built them, and should be allowed to modify those devices so long as the modifications don't result in a device which violates the current (entirely adequate) appropriate FCC regulations. DD-WRT permits me to increase the output power of my router, but because doing so violates FCC regulations, I don't. I can go to Radio Shack (my town still has one) and by a 2 meter handie talkie, but because I don't have a Technician license, I wouldn't use it as that's in violation of current FCC regulations.

Please don't do this. We don't need another DMCA.

While the intentions of more tightly regulating consumer radio devices using the bands occupied by Wireless Devices (typically under the 802.11 scheme) may seem like a good idea, implementing it well may be very, very difficult. As it currently stands, the proposed rule would prohibit several of the things that I do every day in my home, while staying within FCC regulations.

In other words, the modifications to the software that I've made to devices in my home allow: my phone to actually work (CyanogenMod), my wireless routers to talk to one another quite efficiently (DD-WRT), and devices I build myself using microprocessors which can seamlessly connect to my network. I am only able to do this by using software of my own design (or designed by others) to modify the firmware in these devices.

The DMCA made it illegal to fix your own tractor. I'm pretty sure the authors of that legislation didn't intend that as an effect of the law, but it does, and it does a lot of other horrible things as well.

Tightening regulations is fine, but this has side-effects that could be much worse than leaving the regulations as they are.

If writing custom firmware might permit me to turn a well-behaved device (as far as the spectrum is concerned) into an ill-behaved device, there are lots of other things that I could do (which would be far easier than writing firmware) to exhibit bad behavior.

Concluding: This proposal will adversely effect innovation in electronics, network security, home automation, mobile networks, and people's everyday, happy lives. Some end users of electronics (though not all, to be sure) have as much experience and expertise as the companies which built them, and should be allowed to modify those devices so long as the modifications don't result in a device which violates the current (entirely adequate) appropriate FCC regulations. DD-WRT permits me to increase the output power of my router, but because doing so violates FCC regulations, I don't. I can go to Radio Shack (my town still has one) and by a 2 meter handie talkie, but because I don't have a Technician license, I wouldn't use it as that's in violation of current FCC regulations.

Please don't do this. We don't need another DMCA.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Andrew
Last Name: Howard
Mailing Address: 228 E 7th Street #312, St Paul, MN 55101, United States
City: 7th Street
Country: United States
State or Province: ME
ZIP/Postal Code: 55101
Email Address:
Organization Name:
Comment: 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. Not fixing security holes either feeds cyberthreats or increases electronic waste.
5. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
6. There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

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. Not fixing security holes either feeds cyberthreats or increases electronic waste.
5. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
6. There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

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: Justin
Last Name: Johnson
Mailing Address: 5350 Old Dowlen Rd APT#312
City: Beaumont
Country: United States
State or Province: TX
ZIP/Postal Code: 77706
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

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: Skagerberg
Mailing Address: 1306 Irene Ave
City: Benton City
Country: United States
State or Province: WA
ZIP/Postal Code: 99320
Email Address: thisbirdisnomore@gmail.com
Organization Name: null
Comment: So the FCC wants to restrict what we do with out own hardware. This doesn't need to happen. I'm an a Linux user. I use Linux get get away from the data collection and huge security concerns that come with using the Windows operating system. I install OpenWRT or similar on my wireless routers due to broken or crippled firmware from manufacturers. I install custom firmware on my Android devices to get away carrier bloatware and to upgrade my device to a more secure version of Android when the carriers decide to abandon their phones.

Last I checked this was America, and I can do whatever I want with my own property. By restricting what software and firmware I run on my own equipment, you are restricting my choice and freedoms as an American. What I do with my equipment is none of your business or the business of the manufactures. If this proposed rule passes, you are telling the American people they they don't own their equipment, but leasing it from the manufacturers. This will not stand.

We need to be able to install alternative software and firmware on our devices to advance technology, by fixing bugs and mistakes that the manufactures make or just plain ignore. By passing this rule, This rule does nothing to improve the advancement out of technological capabilities, but sends us several steps back.

I say this to you FCC. Do not give in to the corporate lobbying to get this passed. Let the American people keep their freedom of choice to run the software and firmware of their choosing. You did something good with net neutrality. Don't drop the ball on this one.

So the FCC wants to restrict what we do with out own hardware. This doesn't need to happen. I'm an a Linux user. I use Linux get get away from the data collection and huge security concerns that come with using the Windows operating system. I install OpenWRT or similar on my wireless routers due to broken or crippled firmware from manufacturers. I install custom firmware on my Android devices to get away carrier bloatware and to upgrade my device to a more secure version of Android when the carriers decide to abandon their phones.

Last I checked this was America, and I can do whatever I want with my own property. By restricting what software and firmware I run on my own equipment, you are restricting my choice and freedoms as an American. What I do with my equipment is none of your business or the business of the manufactures. If this proposed rule passes, you are telling the American people they they don't own their equipment, but leasing it from the manufacturers. This will not stand.

We need to be able to install alternative software and firmware on our devices to advance technology, by fixing bugs and mistakes that the manufactures make or just plain ignore. By passing this rule, This rule does nothing to improve the advancement out of technological capabilities, but sends us several steps back.

I say this to you FCC. Do not give in to the corporate lobbying to get this passed. Let the American people keep their freedom of choice to run the software and firmware of their choosing. You did something good with net neutrality. Don't drop the ball on this one.

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: Vasquez
Mailing Address: 2419 84TH ST GRD FL
City: Brooklyn
Country: United States
State or Province: NY
ZIP/Postal Code: 11214
Email Address: jvasquez1011@gmail.com
Organization Name:
Comment: Hello FCC,

I just wanted to say that preventing firmware modifications to hardware devices (e.g Routers) is completely against the way that the technological community advances technology. It prevents people from not only being locked in to a specific vendors implementation of a product, but it also prevents the community from auditing what the vendor's are doing, thus hindering security.

There are router products out there that don't even receive firmware updates anymore, and are left in a vulnerable state. Only open source firmware communities are the ones making any further updates to these machine.

Another thing to mention is that allowing the community to continue updating the firmware of a device, increases the router's lifespan in the sense that a previously would-be deprecated/replaced device, could be used for even more years, which has a direct effect in the recycling effort. This allows us people re-use these components which helps our environment.

Please reconsider your proposal to ban firmware modifications to Routers and any other devices by the Open Source community.

- Jonathan

Hello FCC,

I just wanted to say that preventing firmware modifications to hardware devices (e.g Routers) is completely against the way that the technological community advances technology. It prevents people from not only being locked in to a specific vendors implementation of a product, but it also prevents the community from auditing what the vendor's are doing, thus hindering security.

There are router products out there that don't even receive firmware updates anymore, and are left in a vulnerable state. Only open source firmware communities are the ones making any further updates to these machine.

Another thing to mention is that allowing the community to continue updating the firmware of a device, increases the router's lifespan in the sense that a previously would-be deprecated/replaced device, could be used for even more years, which has a direct effect in the recycling effort. This allows us people re-use these components which helps our environment.

Please reconsider your proposal to ban firmware modifications to Routers and any other devices by the Open Source community.

- Jonathan

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: Nematz
Mailing Address: 63 High Ridge Road
City: Monroe
Country: United States
State or Province: NY
ZIP/Postal Code: 10950
Email Address: rn10950@gmail.com
Organization Name:
Comment: This rule will put an end to the innovation that allowed the computing industry to advance to the point that it currently is at. This will allow monopolies to form, and will take all of the possibility for other software such as OpenWRT, dd-wrt, and GNU/Linux to advance and compete with other corporations. Many of the mainstays of computing today started out by some kids messing around with a computer in their garage, and it progressed into the multi-billion dollar corporations they are today. This proposed regulation will make all of that impossible, with no benefit to consumers. Only established corporations will benefit from this, and all startups will suffer. What if IBM decided to lock down the IBM-PC? We probably wouldn't have all of the DOS ans Windows software we have today, and GNU/Linux may not even exist. Passing a rule like this would have an unmeasurable amount of negative effect on the computing industry and innovation in general. Security holes may take longer to find and patch, therefore allowing black hat hackers to steal more sensitive information. This proposed rule may have a bigger negative effect than ending Net Neutrality. It would be in nobody's best interest to approve it.

This rule will put an end to the innovation that allowed the computing industry to advance to the point that it currently is at. This will allow monopolies to form, and will take all of the possibility for other software such as OpenWRT, dd-wrt, and GNU/Linux to advance and compete with other corporations. Many of the mainstays of computing today started out by some kids messing around with a computer in their garage, and it progressed into the multi-billion dollar corporations they are today. This proposed regulation will make all of that impossible, with no benefit to consumers. Only established corporations will benefit from this, and all startups will suffer. What if IBM decided to lock down the IBM-PC? We probably wouldn't have all of the DOS ans Windows software we have today, and GNU/Linux may not even exist. Passing a rule like this would have an unmeasurable amount of negative effect on the computing industry and innovation in general. Security holes may take longer to find and patch, therefore allowing black hat hackers to steal more sensitive information. This proposed rule may have a bigger negative effect than ending Net Neutrality. It would be in nobody's best interest to approve it.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: eric
Last Name: Priolo
Mailing Address: 1310 Harvey
City: Wichita falls
Country: United Kingdom
State or Province: texas
ZIP/Postal Code: 76302
Email Address:
Organization Name:
Comment: Please do not limit my ability to modify my network equipment. This proposal will limit my ability to earn a living, and furthermore, is a gross attempt at limiting the freedom of enthusiasts and budding engineer.

Please do not limit my ability to modify my network equipment. This proposal will limit my ability to earn a living, and furthermore, is a gross attempt at limiting the freedom of enthusiasts and budding engineer.

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: Willy
Last Name: Kim
Mailing Address: 370 Northside Dr., Apt. 2312
City: Atlanta
Country: United States
State or Province: GA
ZIP/Postal Code: 30318
Email Address: wkim149@gmail.com
Organization Name:
Comment: I am one hundred percent against this rule. I would like to point out that this rule will kill our future hackers, I mean white hats. The advancement of technology mostly comes from people sitting around at their houses and trying out things. This rule will greatly narrow or slow down the advancement of technology in the future.

Imagine this rule in effect when the PCs were first out. Today, we won't have Apple or Google. We won't have genius hackers working on the computer science field. Actually, they might be, just in different countries other than the United States of America. The U.S. might be way behind the competition in technologies.

The government should stop distracting techies with difficult laws. It should not take our freedom on what we can do on our own devices as long as we aren't harming anybody's security or privacy. The government should help poorly resourced and young techies to develop their skills instead of helping big corporations getting bigger. Remember, the big corporations can only be there because those poorly resourced and young techies had freedom to explore the world of technology.

I am one hundred percent against this rule. I would like to point out that this rule will kill our future hackers, I mean white hats. The advancement of technology mostly comes from people sitting around at their houses and trying out things. This rule will greatly narrow or slow down the advancement of technology in the future.

Imagine this rule in effect when the PCs were first out. Today, we won't have Apple or Google. We won't have genius hackers working on the computer science field. Actually, they might be, just in different countries other than the United States of America. The U.S. might be way behind the competition in technologies.

The government should stop distracting techies with difficult laws. It should not take our freedom on what we can do on our own devices as long as we aren't harming anybody's security or privacy. The government should help poorly resourced and young techies to develop their skills instead of helping big corporations getting bigger. Remember, the big corporations can only be there because those poorly resourced and young techies had freedom to explore the world of technology.

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: Wyatt
Mailing Address: 2211 Fisher Ct
City: Redondo Beach
Country: United States
State or Province: CA
ZIP/Postal Code: 90278
Email Address:
Organization Name:
Comment: Like many users that have come here today I am concerned about the FCC may make it illegal to install open source operating systems such DD-WRT on routers and GNU/Linux and FreeBSD on computers.

Which is prompted by this link:

http://archive.is/tGCkU

I have 3 different categories of concern which I will address in the attached file. Your proposal is very difficult for someone outside of the government to understand, even with an engineering background.

See attached file for the rest.

Like many users that have come here today I am concerned about the FCC may make it illegal to install open source operating systems such DD-WRT on routers and GNU/Linux and FreeBSD on computers.

Which is prompted by this link:

http://archive.is/tGCkU

I have 3 different categories of concern which I will address in the attached file. Your proposal is very difficult for someone outside of the government to understand, even with an engineering background.

See attached file for the rest.

-Locking Down Software Controlled Radio
18. 20. Your proposal would mandate DRM (digital restrictions management) in devices and prevent users from installing alternate operating systems on devices that they own.

"the device contains security features to prevent the loading of software that would allow the radio to operate in violation of the Commission's rules."

"the rules do not permit any subsequent software changes absent the filing of an application to obtain a new FCC ID."

Manufacturers would simply lock down an entire product to comply with this. Manufacturers segregate certain products with the same SDR but with different software, with multiples cost or obsoleting software to force people to buy the product again when the hardware still works. Or simply they might not provide software for a certain specialist, but still legal with the FCC. Consumers get around this with open source software. Their lock downs, if the courts accept this, would make this business practice de jure, granting them a legal monopoly.

This would directly affect my work as I install and use Ubuntu Linux on home computers and use it for programming. Other businesses may have specialist uses and would be focused to adopt costly networking solutions.

I can understand the FCC's concern over users modifying a configuration setting to change a WIFI radio to go into the cell phone spectrum. But there is a big difference between providing a graphical user interface that controls frequency to changing a setting deep in the driver to override that. Almost all users don't go beyond that. A consumer with that level of technological knowledge and criminal intent to modify a driver might just modify the hardware radio directly. This would moot any benefit the FCC would hope to achieve while causing great harm to the open source community, resellers and researchers; exposing them to great liability. I believe there are better ways for the FCC to achieve this and it should consult those beyond a telecommunications lobby which would profit quite nicely from such a legal monopoly your proposing.

Why should the FCC care? Many new, exciting, companies and technologies come out of the open source community. Google used Python and Linux to run it's search algorithm. If it wasn't for Google with Android (that also uses Linux), the FCC would be dealing with an Apple monopoly on smartphones. I could cite other examples on open source serving as an economic spoiler that a mostly free market like the United States relies on to function in the 21st century. But... the FCC should already be aware of this; if the FCC is not, it is not serving the public interest and that is a severe concern of mine.

My recommendation is that parts (well most) of 18, 20, and others, should be removed. Other portions of your proposal, with my suggestions already address it.

-Digital Certification
Once again, your proposal is vague and poorly defined which many in the community had issue with. This goes outside my knowledge and I would defer to a trusted organization like the EFF or the Software Freedom Law Center. I think they many are worried that vendors may store certification on the writable flash or the hard drive and installing a new operating system would wipe out the certification. The FCC should be very concerned with this as this would be a very significant security issue and would render moot many technological preventions on user changes of software. Malicious actors could take this certification firmware and modify it to harmful ends. A better solution would be in a lower level storage such as the read only memory (ROM). Vendors may apply for exceptions for new technology.

-Certification by Installers and Resellers
b. Devices With Software-Based Capabilities 29 Seems unnecessary under my current understanding of the law. If a person runs a device in a frequency they are unauthorized to use that degrades the frequency or frequencies they are prohibited it already is illegal. This new rule seems that you want to make resellers liable for changes:

"that party becomes responsible for the modified device's compliance and must obtain a new FCC ID for its product."

This at first seems reasonable, but what about driver updates? Drivers control the SDR. If an ebay reseller downloads an Android update that contains an improved driver from Google onto a Samsung phone for the customer's security and convince, does that ebay reseller have to obtain an FCC ID? 24. might address this, but it's in a different section than 18 and must be clarified to address this concern and for the courts. What about community maintained drivers? Linux relies on volunteers to write drivers that often work better than the original device manufacturer. Do they need to seek recertification, for an entire device, for each driver, for each update?

Better clarification might be to merge this part of 18 and 24 as such:

"the party becomes responsible if the modified device compliance goes outside the original approved certification that might produce interference or harm and must obtain a new FCC ID for its product"

38, 39, and 40 should be removed completely. Why should a third party seek permission from the original certifier to modify a device they own? Why is the FCC mandating this when they already require the third party to assume liability and compliance? This seems like a kickback given to original vendors and concerns me on the relationship they have with the FCC and what benefit the FCC sees from this. It also seems to contradict the purpose of 18. If 38-40 is removed, 41 should be as well.

42's specification language seems very vague with SDR. Do you mean the exact original software? Or do you mean the operating parameters of the radio frequency? Once again, the update issue. This is difficult for me to tell as a software engineer which is a problem others will have and the FCC should take note.

- Ending Statement

Most of your rules seemed geared towards the assumption that consumers will buy a wireless device such as a phone or a USB stick and throw it away in a few years and do not care to improve or change it in areas the FCC does not concern it with. These rules ignore community focused software development such as Linux or FreeBSD that have a no budget for recertification and rely on the community to write drivers that often work better than the original device manufacturer.

After your pleasant reversal on net neutrality, endorsing net neutrality, and community owned fiber, I had hoped the FCC would push back and favor citizens over large telecommunication companies. Sadly, this is not the case with device manufacturers would profit heavily from your current proposal and damage the open source community. If your intention was not this, then please clarify your rules

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Ryan
Last Name: Collins
Mailing Address: 49 Bard Drive #106
City: Hudson
Country: United States
State or Province: OH
ZIP/Postal Code: 44236
Email Address: ryan@ryanmcollins.com
Organization Name:
Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This could seriously stifle students, entrepreneurs, developers, and prevent consumers from making perfectly reasonable modifications to their own devices, such as to implement a security fix on a device a manufacturer has stopped supporting or failed to support. There are many more reasons to consider:

-Wireless networking research depends on the ability of researchers to investigate and modify their devices.
-Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
-Not fixing security holes either feeds cyberthreats or increases electronic waste.
-Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
-There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This could seriously stifle students, entrepreneurs, developers, and prevent consumers from making perfectly reasonable modifications to their own devices, such as to implement a security fix on a device a manufacturer has stopped supporting or failed to support. There are many more reasons to consider:

-Wireless networking research depends on the ability of researchers to investigate and modify their devices.
-Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
-Not fixing security holes either feeds cyberthreats or increases electronic waste.
-Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
-There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

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: Bryan
Last Name: English
Mailing Address: 5800 N 42nd Ave #204
City: Robbinsdale
Country: United States
State or Province: MN
ZIP/Postal Code: 55422
Email Address: benglish320@gmail.com
Organization Name:
Comment: I would be extremely unhappy if these rules were implemented, I believe not only would they restrict my freedom to use and modify my electronic equipment, and as an electrical engineering student it is crucial for me to be able to customize equipment. I firmly believe that these rules will be abused by manufacturers as well as the NSA and will lead to less secure networks.

I would be extremely unhappy if these rules were implemented, I believe not only would they restrict my freedom to use and modify my electronic equipment, and as an electrical engineering student it is crucial for me to be able to customize equipment. I firmly believe that these rules will be abused by manufacturers as well as the NSA and will lead to less secure networks.

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: Jeffrey
Last Name: Merejildo
Mailing Address: 424 57st
City: Brooklyn
Country: United States
State or Province: NY
ZIP/Postal Code: 11220
Email Address: merejildo.j@gmail.com
Organization Name:
Comment: Please FCC, do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

by taking away these abilities, you're infringing on future American ingenuity, entrepreneurship and innovation in the sector of technology.

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

by taking away these abilities, you're infringing on future American ingenuity, entrepreneurship and innovation in the sector of technology.

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: Tim
Last Name: Robinson
Mailing Address: 1436 Fishers mill court
City: Herndon
Country: United States
State or Province: VA
ZIP/Postal Code: 22170
Email Address:
Organization Name:
Comment: I understand that the FCC must perceive a need for this directive, however the cons vastly outweigh the pros.

The world, and the United States in particular, is already suffering from a chronic lack of computer scientists, information technologists, software engineers, and many other professions that work in computing. Your rule would not only stifle the ability of existing enthusiasts and workers to innovate privately, but it would vastly raise the barrier to entry in computing. This would absolutely cause fewer people to consider a career in the aforementioned fields.

There's also the issue of the rights of consumers to do what they wish with things they buy. Being unable to install a different operating system on a new computer or router would be a very large invasion of the FCC's authority into my home.

Please do not pass this rule, it is offensive and infringes upon my rights to work on my computer hardware as I wish.

I understand that the FCC must perceive a need for this directive, however the cons vastly outweigh the pros.

The world, and the United States in particular, is already suffering from a chronic lack of computer scientists, information technologists, software engineers, and many other professions that work in computing. Your rule would not only stifle the ability of existing enthusiasts and workers to innovate privately, but it would vastly raise the barrier to entry in computing. This would absolutely cause fewer people to consider a career in the aforementioned fields.

There's also the issue of the rights of consumers to do what they wish with things they buy. Being unable to install a different operating system on a new computer or router would be a very large invasion of the FCC's authority into my home.

Please do not pass this rule, it is offensive and infringes upon my rights to work on my computer hardware as I wish.

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: Joshua
Last Name: Garner
Mailing Address: 883 Roberts Mill Pond RD
City: Pell City
Country: United States
State or Province: AL
ZIP/Postal Code: 35128
Email Address: joshuakgarner@gmail.com
Organization Name:
Comment: To arbitrarily restrict modification of wireless devices is a violation of basic human rights. People have a right to do with their property with whatever they wish. One might draw comparisons with communist states if the government doesn't allow someone to do with their property as they please.

To arbitrarily restrict modification of wireless devices is a violation of basic human rights. People have a right to do with their property with whatever they wish. One might draw comparisons with communist states if the government doesn't allow someone to do with their property as they 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: Erica
Last Name: Schmitt
Mailing Address: 665 OVERHILL DR
City: HAYWARD
Country: United States
State or Province: CA
ZIP/Postal Code: 94544
Email Address: vulpin@gmail.com
Organization Name: null
Comment: I'm objecting in the strongest manner to this proposed rule. I see it as a rule that will stifle creativity in the technical fields, reduce end-user control of their own property, and further restrict progress towards staying competitive in the world.

As a user of Linux both in the workplace and at home, the rules particularly concern me. Similarly, the lack of being able to control the operation of devices at a time when more and more cybercriminals are exploiting commercially available technologies is very concerning; locking devices down to manufacturer-installed operating systems leaves major vulnerabilities open to the whims of the manufacturer(s) in question, and in the case of multi-vendor systems the rules become increasingly difficult to parse.

Again, please do not put this rule in place. Our nation has always prided itself on invention, creative repurposing, and innovation.

I'm objecting in the strongest manner to this proposed rule. I see it as a rule that will stifle creativity in the technical fields, reduce end-user control of their own property, and further restrict progress towards staying competitive in the world.

As a user of Linux both in the workplace and at home, the rules particularly concern me. Similarly, the lack of being able to control the operation of devices at a time when more and more cybercriminals are exploiting commercially available technologies is very concerning; locking devices down to manufacturer-installed operating systems leaves major vulnerabilities open to the whims of the manufacturer(s) in question, and in the case of multi-vendor systems the rules become increasingly difficult to parse.

Again, please do not put this rule in place. Our nation has always prided itself on invention, creative repurposing, and innovation.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Alexander
Last Name: Foster
Mailing Address: 4700 Dexter Dr
City: Goleta
Country: United States
State or Province: CA
ZIP/Postal Code: 93110
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,
It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.
The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.
On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.
Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.
The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.
I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,
It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.
The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their

own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Gerson
Last Name: Zuniga
Mailing Address: 9017 Judwin street
City: Houston
Country: United States
State or Province: TX
ZIP/Postal Code: 77075
Email Address: Gersonz8406@yahoo.com
Organization Name:
Comment: I don't see why the fcc would want to do this.I paid for my equipment and I have the right to do what I want with it.

I don't see why the fcc would want to do this.I paid for my equipment and I have the right to do what I want with it.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Joshua
Last Name: Freigenberg
Mailing Address: 2237 Monarch Dr.
City: Park city
Country: United States
State or Province: UT
ZIP/Postal Code: 84060
Email Address: jtflsf@gmail.com
Organization Name:
Comment: Please don't let this go through. In the long run all this will do is hurt people who use either custom programs they have created. I'm not as well versed in this subject as others you have probably received comments from, but from what i do know is restrictions like this won't protect anyone. The only people i can imagine this would help is the big software and hardware developers and in the long run would make it harder for start ups to enter the market. Thank you for your time and i hope you don't have to read to many comments that attack you.

Please don't let this go through. In the long run all this will do is hurt people who use either custom programs they have created. I'm not as well versed in this subject as others you have probably received comments from, but from what i do know is restrictions like this won't protect anyone. The only people i can imagine this would help is the big software and hardware developers and in the long run would make it harder for start ups to enter the market. Thank you for your time and i hope you don't have to read to many comments that attack you.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Johnny
Last Name: Batres
Mailing Address: 9438 Green Park Valley Drive
City: Saint Louis
Country: United States
State or Province: MO
ZIP/Postal Code: 63123
Email Address:
Organization Name:
Comment: I do not agree with the proposed new regulations because I do not think that the Operating System I am using has a negative impact on anyone else and the proposed regulations seem like an example of government overreach.

Furthermore, 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. Such has been the case with microsoft and other products.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. In this day and age, it is simply not wise to take it on faith that your system is 100% secure (I'm sure the US government has learned this the hard way).

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 ask that these regulation not be implemented lest they do a great harm to an important digital information resource.

I do not agree with the proposed new regulations because I do not think that the Operating System I am using has a negative impact on anyone else and the proposed regulations seem like an example of government overreach.

Furthermore, 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. Such has been the case with microsoft and other products.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. In this day and age, it is simply not wise to take it on faith that your system is 100% secure (I'm sure the US government has learned this the hard way).

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 ask that these regulation not be implemented lest they do a great harm to an important digital information resource.

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: Slemp
Mailing Address: 212 Cades Ct.
City: Clovis
Country: United States
State or Province: NM
ZIP/Postal Code: 88101
Email Address: jonathan.slemp@gmail.com
Organization Name:
Comment: I'm unable to understand the rationale behind this legislation. My hardware is my property; Neither the OEM or the Government have any right to tell me what software I can or can't install as long as I have a valid license and the software isn't created for the purpose of breaking the law. There are many of us who don't have any desire to use proprietary operating systems Like Windows or OSX, we prefer to use open source operating systems that we can install and configure to our own preferences, because we know that this is the best way to ensure security and protect our privacy. Please reconsider this potentially disastrous regulation.

I'm unable to understand the rationale behind this legislation. My hardware is my property; Neither the OEM or the Government have any right to tell me what software I can or can't install as long as I have a valid license and the software isn't created for the purpose of breaking the law. There are many of us who don't have any desire to use proprietary operating systems Like Windows or OSX, we prefer to use open source operating systems that we can install and configure to our own preferences, because we know that this is the best way to ensure security and protect our privacy. Please reconsider this potentially disastrous regulation.

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: Novafed
Mailing Address: 4378 State Street
City: Ann Arbor
Country: United States
State or Province: MI
ZIP/Postal Code: 48105
Email Address:
Organization Name:
Comment: It absolutely does not warrant the rule change. Devices from manufacturers are quick to market, are riddled with bugs, and have their built-in hardware based feature sets disabled in software.

This rule change is un-warranted, un-wanted, and un-American. This benefits only the companies that manufacture these devices and not the consumers that use them.

DO NOT pass this.

It absolutely does not warrant the rule change. Devices from manufacturers are quick to market, are riddled with bugs, and have their built-in hardware based feature sets disabled in software.

This rule change is un-warranted, un-wanted, and un-American. This benefits only the companies that manufacture these devices and not the consumers that use them.

DO NOT pass this.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Ben
Last Name: Betzold
Mailing Address: 6150 Briardale Court
City: Fridley
Country: United States
State or Province: MN
ZIP/Postal Code: 55432
Email Address:
Organization Name:
Comment: This bill will invariably stifle the use of open source firmware for routers.

It will further strengthen the reach of companies that produce routers; with competition gone they will increase their prices.

And this bill inadvertently does these things and others with the purpose of redundancy. It is already illegal to maliciously turn the router to Ham frequencies.

This bill will invariably stifle the use of open source firmware for routers.

It will further strengthen the reach of companies that produce routers; with competition gone they will increase their prices.

And this bill inadvertently does these things and others with the purpose of redundancy. It is already illegal to maliciously turn the router to Ham frequencies.

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: Tyler
Last Name: Corrigan
Mailing Address: 446 Maloney Ct
City: Suisun City
Country: United States
State or Province: CA
ZIP/Postal Code: 94585
Email Address: tyler.b.corrigan@gmail.com
Organization Name:
Comment: The ability to perform the actions on devices as listed has been the sole supporting factor for an unimaginable number of new technologies and products that enable growth in the tech marketplace. There are entire long-running multi million and multi billion dollar businesses that rely heavily on the ability to use hardware from manufacturers in new and exciting ways. The software development industry alone would feel enormous pain should these restrictions go into place, as there is no good for the advancement of technologies with a proposal containing rules with such broad coverage. The issue claimed to be addressed needs attention and action. However, I cannot agree with how this is written.

The ability to perform the actions on devices as listed has been the sole supporting factor for an unimaginable number of new technologies and products that enable growth in the tech marketplace. There are entire long-running multi million and multi billion dollar businesses that rely heavily on the ability to use hardware from manufacturers in new and exciting ways. The software development industry alone would feel enormous pain should these restrictions go into place, as there is no good for the advancement of technologies with a proposal containing rules with such broad coverage. The issue claimed to be addressed needs attention and action. However, I cannot agree with how this is 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: Charles
Last Name: krell
Mailing Address: 1527 coleman rd.
City: Knoxville
Country: United States
State or Province: TN
ZIP/Postal Code: 37909
Email Address: Candidlamaa@gmail.com
Organization Name:
Comment:
Public servants of the Federal Communications Commission,

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

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

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

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

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

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident

in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Daniel
Last Name: Goodwill
Mailing Address: 61 canvasback way
City: Hiram
Country: United States
State or Province: GA
ZIP/Postal Code: 30141
Email Address: eyeplayguitar@gmail.com
Organization Name:
Comment: This is a terrible idea. It would prevent the installation of alternative operating systems and kill research into more advanced wiifi technology. Nothing good can come from these rules.

This is a terrible idea. It would prevent the installation of alternative operating systems and kill research into more advanced wiifi technology. Nothing good can come from these rules.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Brent
Last Name: Taylor
Mailing Address: 54 Runnymede Road
City: Toronto
Country: Canada
State or Province: Ontario
ZIP/Postal Code: m6s2y2
Email Address:
Organization Name:
Comment: I respectfully request that you do not implement the rules limited the installation of custom software on to wireless devices.

The ability to change and modify our own purchased hardware has been a staple of american ingenuity for centuries. Taking what one person has done and modifying is the definition of building a better mouse trap, the foundation of entrepreneurship and commerce.

I respectfully request that you do not implement the rules limited the installation of custom software on to wireless devices.

The ability to change and modify our own purchased hardware has been a staple of american ingenuity for centuries. Taking what one person has done and modifying is the definition of building a better mouse trap, the foundation of entrepreneurship and commerce.

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: Tansey
Mailing Address: 10054 Esteppe Dr
City: Manassas
Country: United States
State or Province: VA
ZIP/Postal Code: 20111-2540
Email Address:
Organization Name:
Comment: Dear whomever it may concern,

I am a computer science student current attending a major public university. I still have 3+ years of school to complete. In this time, we have to take our personal laptops (be it windows or macs) and install Linux on it (optional for macsometimes). Linux being dual-booted (read: installed natively on a partition in the hard drive) is something many students choose to do in order to continue their studies and experience UNIX/Linux the best way possible.

Another issue is the mobile sector. Having an Android phone allows me to root and install custom firmware and OS flavors of Android. This includes updates to the latest version of software not yet released by the carrier (sometimes they don't ever upgrade if the phone is deemed not popular or too "old"). I take it upon myself to fix security holes, upgrade battery life, and tweak my device the way I choose to because it is my decision to do so.

I hope this proposed change does not follow through.

Thank you.

Dear whomever it may concern,

I am a computer science student current attending a major public university. I still have 3+ years of school to complete. In this time, we have to take our personal laptops (be it windows or macs) and install Linux on it (optional for macsometimes). Linux being dual-booted (read: installed natively on a partition in the hard drive) is something many students choose to do in order to continue their studies and experience UNIX/Linux the best way possible.

Another issue is the mobile sector. Having an Android phone allows me to root and install custom firmware and OS flavors of Android. This includes updates to the latest version of software not yet released by the carrier (sometimes they don't ever upgrade if the phone is deemed not popular or too "old"). I take it upon myself to fix security holes, upgrade battery life, and tweak my device the way I choose to because it is my decision to do so.

I hope this proposed change does not follow through.

Thank you.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Jason
Last Name: Taub
Mailing Address: 299 brandston ave
City: elyria
Country: United States
State or Province: OH
ZIP/Postal Code: 44035
Email Address: Shinoaburame26@gmail.com
Organization Name:
Comment: Please do not implement rules forbidding the use of custom software on computing devices. This freedom has allowed for rapid innovation in the computing and technology spheres, and implementing these rules would cause stagnation the likes of which we've not seen in america. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Included in this freedom is the ability to fix and patch any security holes they may find left in place by the manufacturer of said product.

Please do not implement rules forbidding the use of custom software on computing devices. This freedom has allowed for rapid innovation in the computing and technology spheres, and implementing these rules would cause stagnation the likes of which we've not seen in america. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Included in this freedom is the ability to fix and patch any security holes they may find left in place by the manufacturer of said product.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Justin
Last Name: Stokes
Mailing Address: 9 W 57th
City: New York
Country: United States
State or Province: NE
ZIP/Postal Code: 10019
Email Address: justin.stokes@gmail.com
Organization Name:
Comment: To whom it may concern:
While I understand the intention behind this proposed legislation, I fear the commission does not fully comprehend the ramifications. A great deal of technological progress stems from the types of projects this law would outlaw. As these types of projects would continue outside the borders of the United States, passing this would put our country at a disadvantage and stifle a great deal of innovation.
Please do not pass this or any similar regulation limiting or restricting the development and/or modification of devices and their requisite firmware.

To whom it may concern:
While I understand the intention behind this proposed legislation, I fear the commission does not fully comprehend the ramifications. A great deal of technological progress stems from the types of projects this law would outlaw. As these types of projects would continue outside the borders of the United States, passing this would put our country at a disadvantage and stifle a great deal of innovation.
Please do not pass this or any similar regulation limiting or restricting the development and/or modification of devices and their requisite firmware.

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: Kershner
Mailing Address: 6718 Inner Drive
City: Madison
Country: United States
State or Province: WI
ZIP/Postal Code: 53705
Email Address: Jonnykershner@gmail.com
Organization Name: None, personal
Comment: While this legislation touches on many subjects, the most alarming is the attempt to lock down open source or after market software replacement on consumer hardware with wifi. The ability to replace the vendor's often times terrible firmware/software makes otherwise useless hardware have value, and in many cases function significantly better than it would otherwise.

Not to mention the tyrannical slippery slope the US government is embarking on with this kind of legislation.

While this legislation touches on many subjects, the most alarming is the attempt to lock down open source or after market software replacement on consumer hardware with wifi. The ability to replace the vendor's often times terrible firmware/software makes otherwise useless hardware have value, and in many cases function significantly better than it would otherwise.

Not to mention the tyrannical slippery slope the US government is embarking on with this kind of legislation.

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: Cole
Last Name: Williams
Mailing Address: 12634 Hill Pine Rd
City: Midland
Country: United States
State or Province: NC
ZIP/Postal Code: 28107
Email Address: colewilliams83@gmail.com
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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