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: Kyle
Last Name: Jorgensen
Mailing Address: 1159 SE 56th ave 97123 Hillsboro OR
City: Hillsboro
Country: United States
State or Province: OR
ZIP/Postal Code: 97123
Email Address:
Organization Name:
Comment: Gnu/Linux is a very important operating system for many people. Linux is used by millions of people through-out the world. Linux is the backbone for many servers, schools, business and many other things that people need.

Gnu/Linux is a very important operating system for many people. Linux is used by millions of people through-out the world. Linux is the backbone for many servers, schools, business and many other things that people need.

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: Omar-Fara
Last Name: Norgaisse
Mailing Address: 23412 Joe May Road
City: Denham Springs
Country: United States
State or Province: LA
ZIP/Postal Code: 70726
Email Address: omarfara.norgaisse@gmail.com
Organization Name:
Comment: Greetings,

I would like to begin by simply asking the FCC to not implement any rules that would negatively impact the consumer experience. The rules outlined in this proposal would negatively impact consumers by disabling the ability to install the software of their choosing on their computing devices. It should be noted that computing devices have gone far and beyond the desktop computer or the laptop. These devices are also smartwatches, mobile/smart phones, wireless access points, etc.

In addition, by modifying one's own computing device, the consumer is able to ensure that issues that can damage or hamper the user experience (such as security holes and poorly optimized code) is indeed minimized or eliminated without having to wait for a manufacturer to issue a fix or patch (if one is actually realized by the manufacturer).

It should also be pointed out that by hampering the customization of consumer electronics, the field of innovation and development can and will diminish as a result. This also diminishes consumer choice, which is a major economic driver (choice in turn promotes competition and improvement).

Thank you for your time and attention.

Greetings,

I would like to begin by simply asking the FCC to not implement any rules that would negatively impact the consumer experience. The rules outlined in this proposal would negatively impact consumers by disabling the ability to install the software of their choosing on their computing devices. It should be noted that computing devices have gone far and beyond the desktop computer or the laptop. These devices are also smartwatches, mobile/smart phones, wireless access points, etc.

In addition, by modifying one's own computing device, the consumer is able to ensure that issues that can damage or hamper the user experience (such as security holes and poorly optimized code) is indeed minimized or eliminated without having to wait for a manufacturer to issue a fix or patch (if one is actually realized by the manufacturer).

It should also be pointed out that by hampering the customization of consumer electronics, the field of innovation and development can and will diminish as a result. This also diminishes consumer choice, which is a major economic driver (choice in turn promotes competition and improvement).

Thank you for your time and attention.

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: Nicholas
Last Name: Basso
Mailing Address: 2714 Bridgewatch Ln
City: Hilliard
Country: United States
State or Province: OH
ZIP/Postal Code: 43026
Email Address: gedrean@yahoo.com
Organization Name:
Comment: Please do not implement rules that would take away the ability of users to install software of their choosing on electronics devices that they own.

These rules would hamper innovation and technological development in a variety of ways.

- Wireless networking research and development depends on the ability of researches to modify their own devices.
- Manufacturers frequently choose not to fix security holes in devices, leading to a forced upgrade, and consumers need the ability to fix these security flaws rather than being forced to pay more money to a corporation.
- In the past, several issues and bugs in wireless software and drivers have been fixed by individual users whose actions would be prevented under these rules.
- These issues not being fixed can lead to serious cybersecurity threats, and at the least can generate electronic waste.
- Billions of dollars in commerce, such as secure wifi vendors and retail hotspot vendors, fully depend upon the ability to install software of the users' and vendors' choosing.
- There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. There is evidence that closed-source firmware has contributed to and caused more security threats and issues than open-source firmware.

In summation, the proposed changes would stifle innovation, place a chilling effect on the software development community as a whole, endanger billions of dollars, and place many Americans' security on the internet and elsewhere at GREAT risk.

Please do not implement rules that would take away the ability of users to install software of their choosing on electronics devices that they own.

These rules would hamper innovation and technological development in a variety of ways.

- Wireless networking research and development depends on the ability of researches to modify their own devices.
- Manufacturers frequently choose not to fix security holes in devices, leading to a forced upgrade, and consumers need the ability to fix these security flaws rather than being forced to pay more money to a corporation.
- In the past, several issues and bugs in wireless software and drivers have been fixed by individual users whose actions would be prevented under these rules.
- These issues not being fixed can lead to serious cybersecurity threats, and at the least can generate electronic waste.
- Billions of dollars in commerce, such as secure wifi vendors and retail hotspot vendors, fully depend upon the ability to install software of the users' and vendors' choosing.

- There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. There is evidence that closed-source firmware has contributed to and caused more security threats and issues than open-source firmware.

In summation, the proposed changes would stifle innovation, place a chilling effect on the software development community as a whole, endanger billions of dollars, and place many Americans' security on the internet and elsewhere at GREAT risk.

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: Luetkemeyer
Mailing Address: 1300 Meadowlark Dr
City: Little Elm
Country: United States
State or Province: TX
ZIP/Postal Code: 75068
Email Address: john.luetkemeyer@gmail.com
Organization Name:
Comment: This rule will stifle innovation and is an unneeded addition to an already large assortment of rules for manufacturers to follow. Requiring security measures to prevent consumers from modifying software on products that they own is an overreach of the government, and may not be something that the manufacturer even supports or wants to implement. The ability to modify a lawfully owned device should not be hindered in any way, as this is how innovation happens. A prime example of this is the ASUSWRT firmware that the manufacturer ASUS uses on their WiFi router devices (https://github.com/RMerl/asuswrt-merlin/wiki/About-Asuswrt) -- it was actually started as a firmware called Tomato and DD-WRT which was developed in response to Linksys routers being hacked with custom upgraded firmware in the early 2000's. Without that type of development being done by the community in the early 2000's, many of the features that people use on their home WiFi equipment today would not be available.

This rule will stifle innovation and is an unneeded addition to an already large assortment of rules for manufacturers to follow. Requiring security measures to prevent consumers from modifying software on products that they own is an overreach of the government, and may not be something that the manufacturer even supports or wants to implement. The ability to modify a lawfully owned device should not be hindered in any way, as this is how innovation happens. A prime example of this is the ASUSWRT firmware that the manufacturer ASUS uses on their WiFi router devices (https://github.com/RMerl/asuswrt-merlin/wiki/About-Asuswrt) -- it was actually started as a firmware called Tomato and DD-WRT which was developed in response to Linksys routers being hacked with custom upgraded firmware in the early 2000's. Without that type of development being done by the community in the early 2000's, many of the features that people use on their home WiFi equipment today would not be available.

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: Siskonen
Mailing Address: 21411 Deepwood Terrace Apt 304
City: Ashburn
Country: United States
State or Province: VA
ZIP/Postal Code: 20148
Email Address: esiskonen@gmail.com
Organization Name:
Comment: I believe the FCC made the appropriate judgement in regards to net neutrality. Please do not let us down now by making an absolutely wrong and misguided judgement to remove consumers ability to freely use products they purchase as they see fit. Locking down devices will not only hinder technology growth, ability to freely choose what software runs on your hardware, and greatly reduce our ability to stay competitive in a crucial market place, but it will also put the general public at much greater security risks than necessary. Time and time again it has been proven that the openness of the technology community helps to make things better and safer. I, myself, am a security professional who relies on the ability to run software that is not offered by vendors on basically every device I own. This proposal would limit my ability to do my job. It would also limit my ability to help protect the population at large with security research and consultation. It would also make it nearly impossible for me to run Linux on my machines as a primary operating system, which is a personal preference. I really do not like the attitude being taken lately that products purchased by consumers are not their own. Since when has it been acceptable to buy and own a product but not be legally capable of using the way you want to. This sets a very dangerous precedent that could creep into nearly every facet of our daily lives. Soon you will not be able to buy coffee machines to make any type of coffee you would like, because the vendor restricts your post purchase legal rights to force you into buying their specific coffee. It sounds ridiculous and it truly is, but that is the reality this type of proposal is putting forward.

I believe the FCC made the appropriate judgement in regards to net neutrality. Please do not let us down now by making an absolutely wrong and misguided judgement to remove consumers ability to freely use products they purchase as they see fit. Locking down devices will not only hinder technology growth, ability to freely choose what software runs on your hardware, and greatly reduce our ability to stay competitive in a crucial market place, but it will also put the general public at much greater security risks than necessary. Time and time again it has been proven that the openness of the technology community helps to make things better and safer. I, myself, am a security professional who relies on the ability to run software that is not offered by vendors on basically every device I own. This proposal would limit my ability to do my job. It would also limit my ability to help protect the population at large with security research and consultation. It would also make it nearly impossible for me to run Linux on my machines as a primary operating system, which is a personal preference. I really do not like the attitude being taken lately that products purchased by consumers are not their own. Since when has it been acceptable to buy and own a product but not be legally capable of using the way you want to. This sets a very dangerous precedent that could creep into nearly every facet of our daily lives. Soon you will not be able to buy coffee machines to make any type of coffee you would like, because the vendor restricts your post purchase legal rights to force you into buying their specific coffee. It sounds ridiculous and it truly is, but that is the reality this type of proposal is putting forward.

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: Jeremy
Last Name: Tilden
Mailing Address: 700 Birch St
City: Denver
Country: United States
State or Province: CO
ZIP/Postal Code: 80220
Email Address:
Organization Name:
Comment: I hereby respectfully ask that the FCC not implement rules that would remove from the ability of users to install the software of their choice on their own personal computing devices. Americans deserve the right to modify and control the electronic devices they purchase for themselves for personal use.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. The ability of American users to fix security holes in personal electronic devices should be protected when the manufacturer chooses to not do so. For many years, users have exercised vigilance by repairing serious bugs and security holes in their wifi drivers; a practice which would be banned under the NPRM.

Thank you,

Jeremy Tilden

I hereby respectfully ask that the FCC not implement rules that would remove from the ability of users to install the software of their choice on their own personal computing devices. Americans deserve the right to modify and control the electronic devices they purchase for themselves for personal use.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. The ability of American users to fix security holes in personal electronic devices should be protected when the manufacturer chooses to not do so. For many years, users have exercised vigilance by repairing serious bugs and security holes in their wifi drivers; a practice which would be banned under the NPRM.

Thank you,

Jeremy Tilden

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: Giddens
Mailing Address: 17315 EAGLE LEDGE DR.
City: TOMBALL
Country: United States
State or Province: TX
ZIP/Postal Code: 77377
Email Address: jgiddens@gmail.com
Organization Name: Jason Giddens
Comment: Dear FCC Commissioners,

As someone who is both an IT professional, and the guy who maintains my entire extended families computers, I respectfully ask that you not implement any rules that take away my ability to control and modify devices that use Wi-Fi. I have been able to stay ahead of dangerous hardware bugs that are very rarely patched by router manufacturers by using custom firmware on my consumer routers. I have been able to help friends with coffee shops setup revenue earning hot spots on routers that are affordable. As a hobbyist I have enjoyed experimenting with cool new router and switch tools. The ability to modify hardware that I bought and paid for is part of my right as an owner of property. Please do not take this away.

Dear FCC Commissioners,

As someone who is both an IT professional, and the guy who maintains my entire extended families computers, I respectfully ask that you not implement any rules that take away my ability to control and modify devices that use Wi-Fi. I have been able to stay ahead of dangerous hardware bugs that are very rarely patched by router manufacturers by using custom firmware on my consumer routers. I have been able to help friends with coffee shops setup revenue earning hot spots on routers that are affordable. As a hobbyist I have enjoyed experimenting with cool new router and switch tools. The ability to modify hardware that I bought and paid for is part of my right as an owner of property. Please do not take this away.

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: Darcey
Last Name: Kobs
Mailing Address: 5116 Bissonnet Street
City: Bellaire
Country: United States
State or Province: TX
ZIP/Postal Code: 77401
Email Address: dgkobs@gmail.com
Organization Name:
Comment: I respectfully ask the FCC to 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.

I respectfully ask the FCC to 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.

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: Jon
Last Name: Pastore
Mailing Address: 848 N Rainbow Blvd. #1145
City: Las Vegas
Country: United States
State or Province: NV
ZIP/Postal Code: 89107
Email Address:
Organization Name:
Comment: To whom it may concern,

The idea that we should not be allowed to modify a wifi device, (or any other device for that matter), after we have purchased it is ridiculous. The argument of intellectual property rights does not mean you cannot modify your physical property. The changing of an operating system or firmware is not a violation of anyone's intellectual property. As it is, I am appalled that we still have locked phones in this country.

This is the land of the free, and any attempt to move forward on a proposal to further lock down hardware is a move to make this the "land of the free to do as we tell you." Don't we have enough monopolies and tyranny? Are you and your board or comity Americana who believes in the principles of freedom and the constitution we were taught in school? Stop eroding our rights. They're supposed to inalienable, and such a proposal only further alienates our basic rights.

Deny any such proposal that limits our ability to access our own property we fairly purchased. With the gaping security flaws regularly found, we should have the right to take measures to protect ourselves and our privacy. This move to clamp down wifi hardware can only have the purpose to inject more corp/gov malware and prevent it's removal, as demonstrated with windows 10. The Apple protocol that allows for remote bricking was compromised and details about the extent of information accessible was disclosed. Many other "hidden" doors exist with secret keys sold in digital black markets. Nefarious people, who interface with/work for the government are responsible for forcing corps to comply or purchase zero hacks. The government spends $5b annually on buying zero day exploits. That doesn't mean they buy them exclusively. We should have a right to defend our information as it is the most valuable commodity traded without our consent as it is. Please help stop this!

Don't give me another reason to leave the country. I love America, but this government is showing how criminal and bought it really is with proposals such as this. When will it ever be for the people again?

To whom it may concern,

The idea that we should not be allowed to modify a wifi device, (or any other device for that matter), after we have purchased it is ridiculous. The argument of intellectual property rights does not mean you cannot modify your physical property. The changing of an operating system or firmware is not a violation of anyone's intellectual property. As it is, I am appalled that we still have locked phones in this country.

This is the land of the free, and any attempt to move forward on a proposal to further lock down hardware is a move to make this the "land of the free to do as we tell you." Don't we have enough monopolies and tyranny? Are you and your

board or comity Americana who believes in the principles of freedom and the constitution we were taught in school? Stop eroding our rights. They're supposed to inalienable, and such a proposal only further alienates our basic rights.

Deny any such proposal that limits our ability to access our own property we fairly purchased. With the gaping security flaws regularly found, we should have the right to take measures to protect ourselves and our privacy. This move to clamp down wifi hardware can only have the purpose to inject more corp/gov malware and prevent it's removal, as demonstrated with windows 10. The Apple protocol that allows for remote bricking was compromised and details about the extent of information accessible was disclosed. Many other "hidden" doors exist with secret keys sold in digital black markets. Nefarious people, who interface with/work for the government are responsible for forcing corps to comply or purchase zero hacks. The government spends $5b annually on buying zero day exploits. That doesn't mean they buy them exclusively. We should have a right to defend our information as it is the most valuable commodity traded without our consent as it is. Please help stop this!

Don't give me another reason to leave the country. I love America, but this government is showing how criminal and bought it really is with proposals such as this. When will it ever be for the people again?

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: Rowan
Last Name: Thompson
Mailing Address: 2088 regulus ave
City: Virginia beach
Country: United States
State or Province: VA
ZIP/Postal Code: 23461
Email Address: Rowandudleythompson@gmail.com
Organization Name: United States Navy
Comment: I am a member of the United States Navy and I oppose this measure. It would hamper one of the largest free markets in the world and give already established companies a monopoly over what can and cannot be installed on computers and other technology using wifi.

I am a member of the United States Navy and I oppose this measure. It would hamper one of the largest free markets in the world and give already established companies a monopoly over what can and cannot be installed on computers and other technology using wifi.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: steve
Last Name: froelich
Mailing Address: 1630 sw country club pl
City: corvallis
Country: United States
State or Province: OR
ZIP/Postal Code: 97333
Email Address: sffroelich@gmail.com
Organization Name: <n/a>
Comment: I respectfully urge you to abandon this proposal.

Locking down wireless devices, that are used for communication, encroaches on First and Fourth Amendment rights. We need to able to experiment and load software that the people trust onto their communication devices, simply put.

regards,

Stephen F. Froelich

I respectfully urge you to abandon this proposal.

Locking down wireless devices, that are used for communication, encroaches on First and Fourth Amendment rights. We need to able to experiment and load software that the people trust onto their communication devices, simply put.

regards,

Stephen F. Froelich

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: Wesley
Mailing Address: 415 Fern Avenue
City: Deptford
Country: United States
State or Province: NJ
ZIP/Postal Code: 08096
Email Address: kbjwes77@gmail.com
Organization Name: Xarrot Studios
Comment: I appreciate your concern to fight terrorists, but making something illegal will only make the "hackers" and "terrorists" find other ways to do so, but sneakier and more dangerous than ever.

This is a terrible proposal, and will do more damage than good. Everyone has a right to do as they please until they are harming someone else. Installing an alternative operating system on your own router, cell phone or personal computer is not dangerous or remotely harmful, so reconsider this.

I appreciate your concern to fight terrorists, but making something illegal will only make the "hackers" and "terrorists" find other ways to do so, but sneakier and more dangerous than ever.

This is a terrible proposal, and will do more damage than good. Everyone has a right to do as they please until they are harming someone else. Installing an alternative operating system on your own router, cell phone or personal computer is not dangerous or remotely harmful, so reconsider 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: Jacob
Last Name: Lowell
Mailing Address: 1817 West 13th Avenue
City: Anchorage
Country: United States
State or Province: AK
ZIP/Postal Code: 99501
Email Address:
Organization Name:
Comment: As someone who benefits from Gargoyle's internet throttling firmware for routers, I would like to know how this is possibly harmful to anyone around me. All it does is manage bandwidth to set priorities such as 30% for streaming, 15% for downloads, this machine has priority over this machine, etc. Or My friend, who has Linux installed on his laptop because he is a programmer. How is this harmful? I strongly disagree with the FCC's attempts to control our lives through the internet and other media sources.

As someone who benefits from Gargoyle's internet throttling firmware for routers, I would like to know how this is possibly harmful to anyone around me. All it does is manage bandwidth to set priorities such as 30% for streaming, 15% for downloads, this machine has priority over this machine, etc. Or My friend, who has Linux installed on his laptop because he is a programmer. How is this harmful? I strongly disagree with the FCC's attempts to control our lives through the internet and other media sources.

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: Mikal
Last Name: Pippins
Mailing Address: 37537 Weiss Rd
City: Denham Springs
Country: United States
State or Province: LA
ZIP/Postal Code: 70706
Email Address: mikal.pippins@gmail.com
Organization Name:
Comment: What software I choose to install on my personal equipment be it router, pc or whatever else is my business and not the business of the US Government.

Leave it alone.

What software I choose to install on my personal equipment be it router, pc or whatever else is my business and not the business of the US Government.

Leave it alone.

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: Carey
Last Name: Copeland
Mailing Address: 825 Greensboro Avenue
City: Virginia Beach
Country: United States
State or Province: VA
ZIP/Postal Code: 23451
Email Address: null
Organization Name: null
Comment: I am opposed to ANY proposal that would prevent or limit users from installing open-source firmware on WiFi routers. I do exactly that at home and at work and it is extremely important in both places. Open source firmware:

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

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

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

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

Please do not enact any type of regulation that would harm the ability for the open source community to extend their

software and support to WiFi routers. Thank You!

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Sean
Last Name: Zellers
Mailing Address: 2216 Quarry Rd
City: Ashton
Country: United States
State or Province: IL
ZIP/Postal Code: 61006
Email Address:
Organization Name:
Comment: While the FCC has an important job to do, requiring approval for firmware for wireless routers will stifle the safety of companies and individuals to create timely patches and updates the maintain the security of the gateway devices everyone relies on for safely accessing the internet.

The FCC should carefully weigh the need labelling authority and subsequent slow down in the patching for these devices against the fast moving and ever expanding pool of exploits for the vulnerabilities that exist.

I think the FCC while find that it is favourable not to require FCC approval of firmware for devices within the 802.11 spectrum.

While the FCC has an important job to do, requiring approval for firmware for wireless routers will stifle the safety of companies and individuals to create timely patches and updates the maintain the security of the gateway devices everyone relies on for safely accessing the internet.

The FCC should carefully weigh the need labelling authority and subsequent slow down in the patching for these devices against the fast moving and ever expanding pool of exploits for the vulnerabilities that exist.

I think the FCC while find that it is favourable not to require FCC approval of firmware for devices within the 802.11 spectrum.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Dave
Last Name: Buchwald
Mailing Address: 248 87th St
City: Brooklyn
Country: United States
State or Province: NY
ZIP/Postal Code: 11209
Email Address:
Organization Name:
Comment: THIS IS A REALLY BAD IDEA. The FCC should not have the jurisdiction to dictate what software can be run on a device. Period.

THIS IS A REALLY BAD IDEA. The FCC should not have the jurisdiction to dictate what software can be run on a device. Period.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Christopher
Last Name: Creason
Mailing Address: 123 Veranda Cir.
City: Pendleton
Country: United States
State or Province: SC
ZIP/Postal Code: 29670
Email Address:
Organization Name:
Comment: I feel like this is a bad idea. It feels restrictive to the freedom of speech in a sense, and is definitely counter to fair use, at least as far as I understand it.

I feel like this is a bad idea. It feels restrictive to the freedom of speech in a sense, and is definitely counter to fair use, at least as far as I understand 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: Daniel
Last Name: Wolstenholme
Mailing Address: 17142 Dahlgren Rd
City: King George
Country: United States
State or Province: VA
ZIP/Postal Code: 22485
Email Address: daniel@wolstenholme.net
Organization Name:
Comment: Hi, I am very concerned about this new rule and I think it's a very bad idea unless a lot of effort is invested in making sure it doesn't cause unintended consequences. It's understandable that the FCC needs to regulate wireless spectrum to prevent interference, however if that means that users are unable to modify their devices this is completely unacceptable. The problem with WiFi routers is that they are more than just radios, they are small computers which serve an important function in both communications as well as digital security, as they are the "gatekeeper" between a consumer's private network and the wide-open internet.

On a PC, rules like this generally aren't a problem, because the firmware that runs a WiFi adapter is very small and completely focused on the WiFi function only, nothing more, and is completely separate from the rest of the OS.

On a router, however, these devices are so small that the two can be tied together, and this rule could make it impossible for a user to upgrade or modify his router's software (legally or technically or both). This is a problem because, as we've all seen over and over and over, manufacturers frequently do a poor job with their software, and are lax about issuing security updates when new exploits are found. This is an absolutely huge problem with Android phones. Third-party router software like DD-WRT and OpenWRT allows owners of consumer routers to give their devices functions they did not have before with the manufacturer software, to avoid frequent bugs found in manufacturer software, and they also allow them to stay up-to-date with security fixes, since many manufacturers simply abandon support for these devices a short time after releasing them to the market.

How does the FCC intend to address the last point, above all? How will you force manufacturers to fix security problems in devices many years after they were sold, after the warranty period is over? How will you force them to fix bugs found? And how can you justify preventing people from upgrading their router's software to, for instance, implement wireless bridging, a function not normally found in consumer-grade router software? As long as third-party software such as DD-WRT does not run afoul of FCC radio rules, why should these things be prevented?

These same points all apply not only to WiFi routers, but also to smartphones, especially Android phones. These phones are infamous now for many models being completely abandoned by their manufacturers, and not having any software updates even though numerous extremely serious security vulnerabilities have been found and are being exploited. There seems to be no way to force these manufacturers to continue supporting these devices after they're sold with software updates, so it falls on the enthusiast community to make alternative software such as CyanogenMod so that users can keep using these devices safely.

I hope you will keep my comments in mind and look for a way to satisfy both the FCC as well as the users of these devices.

Finally, I would also like to propose simply allowing use of the restricted channels at the low powers that routers are capable of. It seems odd that (in the 2.4GHz band) channels 12-14 are disallowed (though it seems 12-13 are allowed at a very low power) in the US, however everywhere else in the world, 12-13 are permitted, and in Japan, all channels are permitted. Whatever the concern for interference is, no one else in the world seems to have this concern, and in an age of global travel and devices made for global markets, it would make more sense to try to homogenize all these regulations than to try to enforce a messy patchwork of them. As far as I can tell, the biggest source of interference at the upper 2.4GHz channels is the ubiquitous microwave oven. If WiFi users want to set their routers to those channels and then experience interference when their microwaves run, I don't see why that needs Federal action; surely software writers will quickly write their software to avoid those channels or come up with a scheme to automatically switch channels when such interference is seen.

Hi, I am very concerned about this new rule and I think it's a very bad idea unless a lot of effort is invested in making sure it doesn't cause unintended consequences. It's understandable that the FCC needs to regulate wireless spectrum to prevent interference, however if that means that users are unable to modify their devices this is completely unacceptable. The problem with WiFi routers is that they are more than just radios, they are small computers which serve an important function in both communications as well as digital security, as they are the "gatekeeper" between a consumer's private network and the wide-open internet.

On a PC, rules like this generally aren't a problem, because the firmware that runs a WiFi adapter is very small and completely focused on the WiFi function only, nothing more, and is completely separate from the rest of the OS.

On a router, however, these devices are so small that the two can be tied together, and this rule could make it impossible for a user to upgrade or modify his router's software (legally or technically or both). This is a problem because, as we've all seen over and over and over, manufacturers frequently do a poor job with their software, and are lax about issuing security updates when new exploits are found. This is an absolutely huge problem with Android phones. Third-party router software like DD-WRT and OpenWRT allows owners of consumer routers to give their devices functions they did not have before with the manufacturer software, to avoid frequent bugs found in manufacturer software, and they also allow them to stay up-to-date with security fixes, since many manufacturers simply abandon support for these devices a short time after releasing them to the market.

How does the FCC intend to address the last point, above all? How will you force manufacturers to fix security problems in devices many years after they were sold, after the warranty period is over? How will you force them to fix bugs found? And how can you justify preventing people from upgrading their router's software to, for instance, implement wireless bridging, a function not normally found in consumer-grade router software? As long as third-party software such as DD-WRT does not run afoul of FCC radio rules, why should these things be prevented?

These same points all apply not only to WiFi routers, but also to smartphones, especially Android phones. These phones are infamous now for many models being completely abandoned by their manufacturers, and not having any software updates even though numerous extremely serious security vulnerabilities have been found and are being exploited. There seems to be no way to force these manufacturers to continue supporting these devices after they're sold with software updates, so it falls on the enthusiast community to make alternative software such as CyanogenMod so that users can keep using these devices safely.

I hope you will keep my comments in mind and look for a way to satisfy both the FCC as well as the users of these devices.

Finally, I would also like to propose simply allowing use of the restricted channels at the low powers that routers are capable of. It seems odd that (in the 2.4GHz band) channels 12-14 are disallowed (though it seems 12-13 are allowed at a very low power) in the US, however everywhere else in the world, 12-13 are permitted, and in Japan, all channels are permitted. Whatever the concern for interference is, no one else in the world seems to have this concern, and in an age of global travel and devices made for global markets, it would make more sense to try to homogenize all these regulations than to try to enforce a messy patchwork of them. As far as I can tell, the biggest source of interference at

the upper 2.4GHz channels is the ubiquitous microwave oven. If WiFi users want to set their routers to those channels and then experience interference when their microwaves run, I don't see why that needs Federal action; surely software writers will quickly write their software to avoid those channels or come up with a scheme to automatically switch channels when such interference is seen.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Christopher
Last Name: Vienna
Mailing Address: 3334 N Fruit Ave #25
City: Fresno
Country: United States
State or Province: CA
ZIP/Postal Code: 93705
Email Address:
Organization Name:
Comment: As a computer enthusiast I want to be able to run my preferred set of instrunctions on my hardware. The world is moving into the future and almost everything has a wireless RF device in them. Locking down the firmware of something will ruin my form of business and entertainment. This also includes installing open sourced software on my computers and devices. I am against anything the makes something less useful or dampers innovation.

As a computer enthusiast I want to be able to run my preferred set of instrunctions on my hardware. The world is moving into the future and almost everything has a wireless RF device in them. Locking down the firmware of something will ruin my form of business and entertainment. This also includes installing open sourced software on my computers and devices. I am against anything the makes something less useful or dampers 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: Austen
Last Name: Gasparro
Mailing Address: 3697 Silver Oak Pl.
City: Danville
Country: United States
State or Province: CA
ZIP/Postal Code: 94506
Email Address: adgasparro@yahoo.com
Organization Name:
Comment: It is important to understand that a lockdown of devices is anti-consumer. The differences between Microsoft and Apple based Operating Systems may seem quite large, thus sufficient as the only options for consumers; However, operating systems such as Linux have bred many new businesses that are succeeding in the PC market. One such companies is Valve software, which has an entire network based off of Linux-based syntaxes. By locking down machines to specific hardwares, you remove not only the option for consumers to choose how they wish to use the hardware they purchase (not all hardware is purchased in bundles, many people build their computers from individual parts, with no OS attached), but also prevent the growth of computer-based companies from having self-reliance. Do you want all tech companies to rely off of other companies' software at all times? I don't.

We have the right to the hardware we purchase, there are many other things on this proposal I'm sure others are commenting on, but I don't have enough experience to argue about. I understand, though, that this procedure would prevent the installation of alternative operating systems such as Linux or FreeBSD, as well as custom firmware on mobile devices, such as Android-based phones.

Please be aware that this proposal restricts progress and innovation. I urge you to revise this thread carefully, or there will be public outcry among consumers.

It is important to understand that a lockdown of devices is anti-consumer. The differences between Microsoft and Apple based Operating Systems may seem quite large, thus sufficient as the only options for consumers; However, operating systems such as Linux have bred many new businesses that are succeeding in the PC market. One such companies is Valve software, which has an entire network based off of Linux-based syntaxes. By locking down machines to specific hardwares, you remove not only the option for consumers to choose how they wish to use the hardware they purchase (not all hardware is purchased in bundles, many people build their computers from individual parts, with no OS attached), but also prevent the growth of computer-based companies from having self-reliance. Do you want all tech companies to rely off of other companies' software at all times? I don't.

We have the right to the hardware we purchase, there are many other things on this proposal I'm sure others are commenting on, but I don't have enough experience to argue about. I understand, though, that this procedure would prevent the installation of alternative operating systems such as Linux or FreeBSD, as well as custom firmware on mobile devices, such as Android-based phones.

Please be aware that this proposal restricts progress and innovation. I urge you to revise this thread carefully, or there will be public outcry among consumers.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: James
Last Name: Gritton
Mailing Address: 1949 Park Ln E
City: Orem
Country: United States
State or Province: UT
ZIP/Postal Code: 84058
Email Address:
Organization Name:
Comment: This misthought restriction, like all opposition to individual control, will lead to poorer security. Without the possibility of open source, the inevitable security holes in the firmware can only remain uninvestigated and unpatched. They will certainly be known - by bad actors at least, just not by the general public.

Individuals have an interest in things working properly; corporations have only an interest in money. Side with those who are working to improve things.

This misthought restriction, like all opposition to individual control, will lead to poorer security. Without the possibility of open source, the inevitable security holes in the firmware can only remain uninvestigated and unpatched. They will certainly be known - by bad actors at least, just not by the general public.

Individuals have an interest in things working properly; corporations have only an interest in money. Side with those who are working to improve things.

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: Akshay
Last Name: Verma
Mailing Address: 2 Seminary Ave
City: Binghamton
Country: United States
State or Province: NY
ZIP/Postal Code: 13850
Email Address:
Organization Name:
Comment: Wireless networking research depends on the ability of researchers to investigate and modify their devices.

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Joo
Last Name: Silva
Mailing Address: Rua do Barraco
City: Leiria
Country: Portugal
State or Province: Leiria
ZIP/Postal Code: 2410
Email Address:
Organization Name:
Comment: Please don't implement the rules, since:
- Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- Americans (and others) need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please don't implement the rules, since:
- Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- Americans (and others) 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.