

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:  
First Name: John  
Last Name: Waugh  
Mailing Address: 20 Blonders Boulevard  
City: Ledyard  
Country: United States  
State or Province: CT  
ZIP/Postal Code: 06339  
Email Address: john.waugh@att.net  
Organization Name:  
Comment: Dear FCC,

Regarding the "Equipment Authorization and Electronic Labeling for Wireless Devices, identified by ET Docket No. 15-170":

I believe that end users (consumers, citizens, researchers, teachers, hobbyists, etc.) should have the freedom to create and add or remove software to computer, phone, and electronic devices (routers etc.) if they would like.

We are able to configure our own hardware and software the way we want it and also can identify security flaws, create patches and fixes and create new software under the current laws. If this changes, to prohibit changes to the software or 'locking' devices so they cannot be legally changed, then the end users (as listed above) would be breaking the law just to work on their own device. Wifi enabled devices encompass many facets of everyday life today and limiting the freedom of individuals to configure them the way they want is a bad idea. New technology and software is created and improved by people making their own changes.

Please consider the end users and the freedom to choose for the end user.

Thank you.

Dear FCC,

Regarding the "Equipment Authorization and Electronic Labeling for Wireless Devices, identified by ET Docket No. 15-170":

I believe that end users (consumers, citizens, researchers, teachers, hobbyists, etc.) should have the freedom to create and add or remove software to computer, phone, and electronic devices (routers etc.) if they would like.

We are able to configure our own hardware and software the way we want it and also can identify security flaws, create patches and fixes and create new software under the current laws. If this changes, to prohibit changes to the software or 'locking' devices so they cannot be legally changed, then the end users (as listed above) would be breaking the law just to work on their own device. Wifi enabled devices encompass many facets of everyday life today and limiting the freedom of individuals to configure them the way they want is a bad idea. New technology and software is created and improved by people making their own changes.

Please consider the end users and the freedom to choose for the end user.

Thank you.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Yarwood

Mailing Address: 11380 White Rock Road

City: Rancho Cordova

Country: United States

State or Province: CA

ZIP/Postal Code: 95742

Email Address: toaddawet@hotmail.com

Organization Name:

Comment: Please do not implement regulations that would prevent users from installing software of their choice on their computing devices. This limits freedom of choice for end users, and also prevents individuals from repairing things like security holes in software that manufacturers don't bother to do. In the past individuals have created security fixes themselves in situations like this and shared them with others online. This kind of sharing and help through individual initiative should be encouraged--it makes the internet a better place overall, and helps keep security tight for everyone. I feel strongly that implementing regulations banning such things will only hurt the consumer in the long run.

Please do not implement regulations that would prevent users from installing software of their choice on their computing devices. This limits freedom of choice for end users, and also prevents individuals from repairing things like security holes in software that manufacturers don't bother to do. In the past individuals have created security fixes themselves in situations like this and shared them with others online. This kind of sharing and help through individual initiative should be encouraged--it makes the internet a better place overall, and helps keep security tight for everyone. I feel strongly that implementing regulations banning such things will only hurt the consumer in the long run.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: William  
Last Name: Valentine  
Mailing Address: 220 Babbitt Hill Rd A2  
City: Pomfret Center  
Country: United States  
State or Province: CT  
ZIP/Postal Code: 06259  
Email Address: drbill28@gmail.com  
Organization Name:

Comment: I ask you to not take actions that harm the consumer. These actions would not only make it difficult to install the software one wishes on their owned devices. It would also do severe damage to free and open source software and make it difficult to use the software that has made many technology innovations possible. Even installing an open source OS would be in danger. The only effect here is for certain corporation to try to permanently install themselves as the players through the government instead of through innovation.

I ask you to not take actions that harm the consumer. These actions would not only make it difficult to install the software one wishes on their owned devices. It would also do severe damage to free and open source software and make it difficult to use the software that has made many technology innovations possible. Even installing an open source OS would be in danger. The only effect here is for certain corporation to try to permanently install themselves as the players through the government instead of through innovation.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: Jake  
Last Name: Strickek  
Mailing Address: 8502 E Ramsey Rd  
City: Hereford  
Country: United States  
State or Province: AZ  
ZIP/Postal Code: 85615  
Email Address:  
Organization Name:

Comment: I am leaving this comment today because I am worried about my freedom. I use alternative, Open Source Firmware and Operating Systems. The rules as they are proposed will limit that Freedom.

As with most new laws, they are broad and over reaching and at times convoluted. The FCC Needs to reach out to groups that are involved with Open Source Firmware and Operating Systems to make the laws work for the edge cases that might not have been considered when the draft law was wrote.

The turning points of lives are not the great moments. The real crises are often concealed in occurrences so trivial in appearance that they pass unobserved.

George Washington

I am leaving this comment today because I am worried about my freedom. I use alternative, Open Source Firmware and Operating Systems. The rules as they are proposed will limit that Freedom.

As with most new laws, they are broad and over reaching and at times convoluted. The FCC Needs to reach out to groups that are involved with Open Source Firmware and Operating Systems to make the laws work for the edge cases that might not have been considered when the draft law was wrote.

The turning points of lives are not the great moments. The real crises are often concealed in occurrences so trivial in appearance that they pass unobserved.

George Washington

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

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

Submitter Info:

First Name: Hank

Last Name: Hill

Mailing Address: 897 smith street

City: davisburg

Country: United States

State or Province: MI

ZIP/Postal Code: 48350

Email Address:

Organization Name:

Comment: There is enough government intrusion into the personal lives of Americans.

Please keep your hands off our computers.

Our forefathers would be shocked at the bravado this committee is showing.

There is enough government intrusion into the personal lives of Americans.

Please keep your hands off our computers.

Our forefathers would be shocked at the bravado this committee is showing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Killingsworth

Mailing Address: 1305 Summerton Pl

City: Yukon

Country: United States

State or Province: OK

ZIP/Postal Code: 73099-5451

Email Address:

Organization Name:

Comment: Please do not restrict the ability of consumers to install third party firmware on their wireless devices. The ability to install third party firmware allows people to extend the usefulness of devices and more importantly, allows people to fix security holes that remain after manufacturers abandon their products. Considering the ever increasing number of security flaws found in consumer electronics this is an extremely important right for consumers to have.

Please do not restrict the ability of consumers to install third party firmware on their wireless devices. The ability to install third party firmware allows people to extend the usefulness of devices and more importantly, allows people to fix security holes that remain after manufacturers abandon their products. Considering the ever increasing number of security flaws found in consumer electronics this is an extremely important right for consumers to have.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: John

Last Name: Doe

Mailing Address: 55 Franklin Street, 5th floor

City: Boston

Country: United States

State or Province: MA

ZIP/Postal Code: 02110

Email Address: info@fsf.org

Organization Name: FSF

Comment: Preventing people from changing the software for their wireless device won't stop people from changing it. People will still be able to operate wireless devices outside of regulatory limitations.

What these laws will do is prevent companies from selling devices with OpenWRT or libreCMC installed. It will also affect laptop sellers, since laptops often come with wifi chips in them.

What you should do instead is fine people who are caught not following the regulations. Crime prevention is a good thing, but only when it doesn't affect the freedom of non-criminals.

Things to consider:

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

Preventing people from changing the software for their wireless device won't stop people from changing it. People will still be able to operate wireless devices outside of regulatory limitations.

What these laws will do is prevent companies from selling devices with OpenWRT or libreCMC installed. It will also affect laptop sellers, since laptops often come with wifi chips in them.

What you should do instead is fine people who are caught not following the regulations. Crime prevention is a good thing, but only when it doesn't affect the freedom of non-criminals.

Things to consider:

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

and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: Thomas  
Last Name: Ammons  
Mailing Address: 9430 87th st  
City: Vero Beach  
Country: United States  
State or Province: FL  
ZIP/Postal Code: 32967  
Email Address: mintzone@outlook.com  
Organization Name:

Comment: I have some choice comments about this proposal from my limited knowledge about it. I'm slightly confused about the layout of this website, and I haven't been able to find the actual proposal- I'm sure it is rather annoying when people only interact with the aid of news coverage, but I feel the need to comment. Apologies if I say something that isn't relevant.

It seems to me that this proposal will disincentivize the allowance of Open Source software in routers. This threatens to weaken the security of all the routers consumers will buy. Routers are already notoriously abandoned and left to rot in favor of newer, more profitable routers.

Custom firmware for these routers allows users to remain secure after hardware manufacturers refuse to update anymore.

I understand the necessity to curb the threat of certain transmissions. This should be done in hardware instead of software, however. I also wonder about how effective extreme limitation of hardware and software will actually be. The kind of people who would want to do damage have the knowledge to do so without off the shelf software.

While I'm writing this, I'd also like to request that it be considered for router manufacturers to require the ability to load off the shelf firmware in their routers. I want my purchase of a router to be worthwhile long after the manufacturer doesn't.

I have some choice comments about this proposal from my limited knowledge about it. I'm slightly confused about the layout of this website, and I haven't been able to find the actual proposal- I'm sure it is rather annoying when people only interact with the aid of news coverage, but I feel the need to comment. Apologies if I say something that isn't relevant.

It seems to me that this proposal will disincentivize the allowance of Open Source software in routers. This threatens to weaken the security of all the routers consumers will buy. Routers are already notoriously abandoned and left to rot in favor of newer, more profitable routers.

Custom firmware for these routers allows users to remain secure after hardware manufacturers refuse to update anymore.

I understand the necessity to curb the threat of certain transmissions. This should be done in hardware instead of software, however. I also wonder about how effective extreme limitation of hardware and software will actually be. The

kind of people who would want to do damage have the knowledge to do so without off the shelf software.

While I'm writing this, I'd also like to request that it be considered for router manufacturers to require the ability to load off the shelf firmware in their routers. I want my purchase of a router to be worthwhile long after the manufacturer doesn't.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: Les  
Last Name: Shigley  
Mailing Address: 537 s jordan way  
City: Lehi  
Country: United States  
State or Province: UT  
ZIP/Postal Code: 84043  
Email Address: fcc@shigles.33mail.com  
Organization Name:

Comment: The FCC wording is too vague and will restrict the ability of the end user's flexibility in operating systems on computers and ROM on android phones.

This would to greatly restrict the consumer freedoms

The FCC wording is too vague and will restrict the ability of the end user's flexibility in operating systems on computers and ROM on android phones.

This would to greatly restrict the consumer freedoms

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: jonathan  
Last Name: wigglesworth  
Mailing Address: 77 william street, apt. 2  
City: new haven  
Country: United States  
State or Province: CT  
ZIP/Postal Code: 06511  
Email Address:  
Organization Name:

Comment: Please do not pass this regulation, limiting the ability of consumers to load custom firmware and software onto devices with software controlled radios. I understand and respect the need for the FCC to prevent such devices from interfering other approved communications devices, and especially for the uninterrupted service necessary for emergency personnel such as police, fire departments, an emergency medical services. However, an overbroad regulation such as this one that limits all such software, instead of limiting only those features that cause interference (such as increasing the transmit power, or allowing transmission on unapproved channels) has the potential to lead to several unintended consequences.

Potential readings of the regulation as it is currently written would forbid installing apps on smart phones, unlocking or rooting phones, installing third party operating systems (such as linux) on laptops, etc. While it's easy to argue that this is obviously not the intent of such a regulation, it must be admitted that frequently, regulations are enforced according to interpretations out of step with their original intent. Any regulation intending to reduce interference by consumer devices must be written in such a way as not to prohibit what are daily activities for a majority of consumers. Specifically, they should be written to explicitly prohibit only those functions which are causing interference: using unapproved channels and unapproved transmission power.

Any less specific wording is guaranteed to lead unintended negative consequences.

Please do not pass any regulation that would prohibit installing custom software. Thank you.

Please do not pass this regulation, limiting the ability of consumers to load custom firmware and software onto devices with software controlled radios. I understand and respect the need for the FCC to prevent such devices from interfering other approved communications devices, and especially for the uninterrupted service necessary for emergency personnel such as police, fire departments, an emergency medical services. However, an overbroad regulation such as this one that limits all such software, instead of limiting only those features that cause interference (such as increasing the transmit power, or allowing transmission on unapproved channels) has the potential to lead to several unintended consequences.

Potential readings of the regulation as it is currently written would forbid installing apps on smart phones, unlocking or rooting phones, installing third party operating systems (such as linux) on laptops, etc. While it's easy to argue that this is obviously not the intent of such a regulation, it must be admitted that frequently, regulations are enforced according to interpretations out of step with their original intent. Any regulation intending to reduce interference by consumer devices must be written in such a way as not to prohibit what are daily activities for a majority of consumers. Specifically, they should be written to explicitly prohibit only those functions which are causing interference: using

unapproved channels and unapproved transmission power.

Any less specific wording is guaranteed to lead unintended negative consequences.

Please do not pass any regulation that would prohibit installing custom software. Thank you.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:  
First Name: Eugnee  
Last Name: Miller  
Mailing Address: 3331 Belaire Av  
City: Cheyenne  
Country: United States  
State or Province: WY  
ZIP/Postal Code: 82001  
Email Address: theerm@gmail.com  
Organization Name: N?A  
Comment: Hello, Thanks for your time.

I use open source software every day, it is also how I make my living. I don't know how to be an effective commenter. What I do know is that I like having wifi on my laptop that is running open source software.

I also run DD-WRT on my buffalo router. It's the best router I've bought in years. (I own 2.) I've bought other routers for more that did less. DD-WRT is by far the best router OS I've ran, and it's open source.

If you do this you are going to make it illegal to run open source software like linux on any device that has wifi.

Linux is the #1 os in the world it's used on more devices than any other OS on the planet. Eventually cars are going to be running it, and being forced to solve this problem isn't going to help the consumer. It's going to raise prices of routers & laptops exponentially, and really hurt America.

Let's put it this way if this were a car and we wanted to put a new engine in it you'd let us right? Well that's what we want. We want to be able to tinker and modify, upgrade & improve. Most of us stay within the confines of the law. I know I don't use channel 14.

Erm

Hello, Thanks for your time.

I use open source software every day, it is also how I make my living. I don't know how to be an effective commenter. What I do know is that I like having wifi on my laptop that is running open source software.

I also run DD-WRT on my buffalo router. It's the best router I've bought in years. (I own 2.) I've bought other routers for more that did less. DD-WRT is by far the best router OS I've ran, and it's open source.

If you do this you are going to make it illegal to run open source software like linux on any device that has wifi.

Linux is the #1 os in the world it's used on more devices than any other OS on the planet. Eventually cars are going to be running it, and being forced to solve this problem isn't going to help the consumer. It's going to raise prices of

routers & laptops exponentially, and really hurt America.

Let's put it this way if this were a car and we wanted to put a new engine in it you'd let us right? Well that's what we want. We want to be able to tinker and modify, upgrade & improve. Most of us stay within the confines of the law. I know I don't use channel 14.

Erm

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

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

Submitter Info:

First Name: michael

Last Name: tuohy

Mailing Address: 33 maplewood blvd

City: suffern

Country: United States

State or Province: NY

ZIP/Postal Code: 10901

Email Address:

Organization Name:

Comment: Stop taking away our freedom. If we own something we should be able to have access to it. If i want to put a piece of tape over the manufacturer's logo of my router that is my business. If I want to remove one of the housing screws from my router and use it to hang a picture that is also my business.If I want to remove the pattern of electro magnetic zeros and one's that reside in my router that is most certainly my business. If I want to add my own zeros and one's in place of the preinstalled zeros and one's in my router that is absolutely my business.

Stop taking away our freedom. If we own something we should be able to have access to it. If i want to put a piece of tape over the manufacturer's logo of my router that is my business. If I want to remove one of the housing screws from my router and use it to hang a picture that is also my business.If I want to remove the pattern of electro magnetic zeros and one's that reside in my router that is most certainly my business. If I want to add my own zeros and one's in place of the preinstalled zeros and one's in my router that is absolutely my business.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: Tim

Last Name: Coalson

Mailing Address: 1965 Beacongrove Dr

City: St Louis

Country: United States

State or Province: MO

ZIP/Postal Code: 63146

Email Address:

Organization Name:

Comment: \*) These rules are overly broad in their requirements on device manufacturers, in a way that is near-certain to make them remove important user control over devices sold. In particular, these rules are extremely similar to the existing U-NII rules, to which manufacturers responded by preventing users from installing any operating system the manufacturer had not pre-approved, or from being able to modify the drivers, even if those drivers were open-source.

\*) Being able to modify the drivers or install a different operating system is crucial for user freedom (cyanogen mod and countless other android-based phone OSes), security research, and for advanced users to be able to add features (like mesh networking) and fix problems they identify with the provided software/operating system (often by replacing a proprietary OS with an open-source one). The open-source community relies on this ability to modify software, and among its key visible developments is the linux kernel, which is heavily used in industry for everything from high-performance computing, to serving websites, to cell phones, to embedded devices. On the other hand, the OS/firmware shipped with consumer wifi routers is notorious for security problems that go unfixed for years, for instance default admin passwords, lack of DNS security, and update checks that don't use encryption. By adopting these rules in their current form, manufacturers would be encouraged to make devices such that not even the most well-informed and skilled user would be able to do anything to secure their device, other than turning it off.

\*) Instead, it is in fact the user, and not the manufacturer, that is ultimately responsible for ensuring that equipment which they modify adheres to regulations. Instead of encouraging manufacturers to take away user rights, we should encourage them to warn those advanced users that do modify their devices, that doing so could result in breaking the law, and of the penalties associated with doing so. Users that do not have the necessary knowledge to modify drivers or install operating systems do not need this warning, and simply shouldn't be presented with simple options that could result in breaking the law. That is, friendly user interfaces, such as web interfaces, to wireless radios should not present options that would cause the device to break regulations. This is entirely sufficient for all cases in which the user wants to obey regulations. Advanced users that do not want to obey regulations can fairly easily build radios from scratch, meaning that restricting what lawful users can do with their approved devices will have little to no effect on bad actors, at significant and unacceptable cost to user freedom.

\*) For a detailed explanation of the main problems with the proposed rules, please see:  
<http://prpl.works/2015/09/21/yes-the-fcc-might-ban-your-operating-system/>

\*) These rules are overly broad in their requirements on device manufacturers, in a way that is near-certain to make them remove important user control over devices sold. In particular, these rules are extremely similar to the existing U-NII rules, to which manufacturers responded by preventing users from installing any operating system the manufacturer had not pre-approved, or from being able to modify the drivers, even if those drivers were open-source.

\*) Being able to modify the drivers or install a different operating system is crucial for user freedom (cyanogen mod and countless other android-based phone OSes), security research, and for advanced users to be able to add features (like mesh networking) and fix problems they identify with the provided software/operating system (often by replacing a proprietary OS with an open-source one). The open-source community relies on this ability to modify software, and among its key visible developments is the linux kernel, which is heavily used in industry for everything from high-performance computing, to serving websites, to cell phones, to embedded devices. On the other hand, the OS/firmware shipped with consumer wifi routers is notorious for security problems that go unfixed for years, for instance default admin passwords, lack of DNS security, and update checks that don't use encryption. By adopting these rules in their current form, manufacturers would be encouraged to make devices such that not even the most well-informed and skilled user would be able to do anything to secure their device, other than turning it off.

\*) Instead, it is in fact the user, and not the manufacturer, that is ultimately responsible for ensuring that equipment which they modify adheres to regulations. Instead of encouraging manufacturers to take away user rights, we should encourage them to warn those advanced users that do modify their devices, that doing so could result in breaking the law, and of the penalties associated with doing so. Users that do not have the necessary knowledge to modify drivers or install operating systems do not need this warning, and simply shouldn't be presented with simple options that could result in breaking the law. That is, friendly user interfaces, such as web interfaces, to wireless radios should not present options that would cause the device to break regulations. This is entirely sufficient for all cases in which the user wants to obey regulations. Advanced users that do not want to obey regulations can fairly easily build radios from scratch, meaning that restricting what lawful users can do with their approved devices will have little to no effect on bad actors, at significant and unacceptable cost to user freedom.

\*) For a detailed explanation of the main problems with the proposed rules, please see:  
<http://prpl.works/2015/09/21/yes-the-fcc-might-ban-your-operating-system/>

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

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

Submitter Info:

First Name: Tyler

Last Name: Whiting

Mailing Address: 110 East Center Street

City: Spanish Fork

Country: United States

State or Province: UT

ZIP/Postal Code: 84660

Email Address: tyler.whiting3@gmail.com

Organization Name:

Comment: Limiting alteration of software on devices is an infringement of liberty. I purchased the hardware, and now I want to use free software. Often times Linux Operating Systems have higher security than what ships with the device. Taking away my ability to do this limits my growth in the workplace and stops community teams from solving problems. What if this was in place when Bill Gates was developing Windows?

Limiting alteration of software on devices is an infringement of liberty. I purchased the hardware, and now I want to use free software. Often times Linux Operating Systems have higher security than what ships with the device. Taking away my ability to do this limits my growth in the workplace and stops community teams from solving problems. What if this was in place when Bill Gates was developing Windows?

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: w. Patrick  
Last Name: Reagan  
Mailing Address: po box 5306  
City: arlington  
Country: United States  
State or Province: VA  
ZIP/Postal Code: 22205  
Email Address:  
Organization Name:

Comment: I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168> The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq\_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt> The result of this multi-year effort was a major advance in performance for all routers. The fq\_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) Finally, I want to address the FCC's original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has

caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve Americas airwaves.

I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168>. The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq\_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt> The result of this multi-year effort was a major advance in performance for all routers. The fq\_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) Finally, I want to address the FCCs original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve Americas airwaves.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:  
First Name: Sebastian  
Last Name: McMorrow  
Mailing Address: 1158 Myrtle Avenue  
City: Brooklyn  
Country: United States  
State or Province: NY  
ZIP/Postal Code: 11221  
Email Address: mcmorrow@airmail.cc  
Organization Name:

Comment: As an amateur webmaster, I like to be able to control the tools that I use in order to expand upon my knowlage of networks. One such tool is OpenWRT, a tool that would become illegal if what is proposed comes into effect. This tool has taught me more than anything else, by allowing me to have total control over my home network. As a consumer, I feel that when I buy a device I should be able to use what is it that I want to use the device for. When I can no longer repurpose old computers into access points, these old computers are waste. This is not only a problem for us enthusiasts, it is a problem for those who have an intrest in the enviroment. When we no longer allow old products to be used as a powerful router, we take an option out from the free market. Will there be new companies that sell access points with open software installed? Yes. However, that simply creates a new thing to buy and throw away, something that happens all to often in our disposable society. So I implore you, as a hobbyist, a consumer, a capitalist, a supporter of the Free Software Foundation, and someone who has a stake in the enviroment, do not allow make my computers illegal.

As an amateur webmaster, I like to be able to control the tools that I use in order to expand upon my knowlage of networks. One such tool is OpenWRT, a tool that would become illegal if what is proposed comes into effect. This tool has taught me more than anything else, by allowing me to have total control over my home network. As a consumer, I feel that when I buy a device I should be able to use what is it that I want to use the device for. When I can no longer repurpose old computers into access points, these old computers are waste. This is not only a problem for us enthusiasts, it is a problem for those who have an intrest in the enviroment. When we no longer allow old products to be used as a powerful router, we take an option out from the free market. Will there be new companies that sell access points with open software installed? Yes. However, that simply creates a new thing to buy and throw away, something that happens all to often in our disposable society. So I implore you, as a hobbyist, a consumer, a capitalist, a supporter of the Free Software Foundation, and someone who has a stake in the enviroment, do not allow make my computers illegal.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

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

Submitter Info:

First Name: Matthew  
Last Name: Nuzum  
Mailing Address: 510 NE Trilein Dr  
City: Ankeny  
Country: United States  
State or Province: IA  
ZIP/Postal Code: 50021  
Email Address:  
Organization Name:

Comment: Hello, I'm concerned that this regulation would have serious negative consequences. In particular:

\* I like to use computers that run the Linux operating system, which often utilization open source, community managed wireless networking drivers. Because these are not managed by a corporation there is no one who can digitally sign them

\* I like to customize and repurpose older hardware to ensure that it continues to be useful after the manufacturer stops providing software updates. Many people that I know who also do this feel this reduces electronic devices going to landfills

\* I personally manage a router that has been customized in order to provide guest access to a wireless network at a restaurant. I have used open source firmware to add the functionality that requires users to agree to terms of service before they can make use of the network. These new rules would make the solution impossible.

\* My fear is that, by making it harder for vendors to update their firmware for their devices then fewer vendors will update the firmware.

I would like the FCC to re-consider this proposal in light of how it will affect the above aspects.

Hello, I'm concerned that this regulation would have serious negative consequences. In particular:

\* I like to use computers that run the Linux operating system, which often utilization open source, community managed wireless networking drivers. Because these are not managed by a corporation there is no one who can digitally sign them

\* I like to customize and repurpose older hardware to ensure that it continues to be useful after the manufacturer stops providing software updates. Many people that I know who also do this feel this reduces electronic devices going to landfills

\* I personally manage a router that has been customized in order to provide guest access to a wireless network at a restaurant. I have used open source firmware to add the functionality that requires users to agree to terms of service before they can make use of the network. These new rules would make the solution impossible.

\* My fear is that, by making it harder for vendors to update their firmware for their devices then fewer vendors will

update the firmware.

I would like the FCC to re-consider this proposal in light of how it will affect the above aspects.