

OZ0CD

Hello,

The implications of limiting the ability to replace and/or modify the embedded software ("firmware") of wireless devices are quite severe. I would like for you to reconsider.

You have to consider that there are multiple types of modification:

1. Replace the firmware in the wireless device (e.g. a WiFi-enabled router), for the purpose of a different user experience/functionality, without modifying any radio capabilities, either by simply not touching the relevant parts, or due to the radio with firmware being a completely separate internal device.
2. Replace firmware in the wireless device with the intention of modifying radio capabilities. This is already covered by FCC regulations, and is only done with regards to research.

The first is a decade-old practice, done to enable devices that are broken, bad, or long forgotten by their manufacturers to get back into a usable, or even better shape. It is done to experiment with new features. It is done to patch security holes that would otherwise leave you vulnerable to either stolen data or at least breaking into your WiFi, such as the silly "WPS" feature that leaves your WiFi amusingly insecure, with a 100% guarantee for successful break-in. Modifying the software running on a WiFi-enabled router is also no different than running an different application on a WiFi-enabled laptop. Touching the embedded software of "the unit" does not mean modifying the firmware of the radio itself, and limiting the modification of such firmware is as peculiar an idea as limiting the development of applications on a laptop without FCC approval.

Ensuring that the FCC regulations regarding the usage of the radio spectrum is met is important to ensure that everyone can use the spectrum as intended. But carelessly impeding on the right to modify and innovate using devices that a person rightfully owns, when it has nothing to do with abusing the radio spectrum, is a bad idea.

Such a bad idea that people from around the world are upset by it. Not because the regulations will apply, but because any of the "security" features that this regulation requires, while most likely easy to break, will limit our ability to fix a router, as manufacturers develop devices meant for the global market. News sites used by "makers" and "hackers" (In the good sense, not the evil one) are outraged by it, and campaigns against this regulation are being made.

Please reconsider.

Best regards,
Kenny Levinsen
OZ0CD

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: Caleb

Last Name: Smith

Mailing Address: 1095 George Road

City: Westfield

Country: United States

State or Province: NC

ZIP/Postal Code: 27053

Email Address: caleb_smith@emiimaging.com

Organization Name: N/A

Comment: I understand the reasons why some would think this rule would be beneficial, however there is a lot more harm here than good. There are lots of WiFi routers that use open wrt and dd-wrt firmwares including devices like WiFi Pineapple, Arduino Yun, and more. But I will focus on the Arduino Yun which runs OpenWrt. Even if the Yun is not specifically banned, the OpenWrt community will dwindle out because of this rule which will hurt Arduino which will hurt American children interested in building devices for the internet of things. Unfortunately a lot of legitimate businesses will suffer because of this, tinkerers will suffer because of this, the open software movement will suffer, the Internet of Things will suffer, and consumers will not get a neat wifi toaster oven because the guy who wants to make that toaster oven will have to jump through more hoops than he is willing. Please reconsider this rule. It will hurt everything from the Internet of Things to custom Android firmware like Cyanogen Mod. We have the right to modify our own devices, if we start broadcasting 5Ghz in ways that break the existing FCC rules then come get that person. Don't create a broad rule that will hurt legitimate business and open software

I understand the reasons why some would think this rule would be beneficial, however there is a lot more harm here than good. There are lots of WiFi routers that use open wrt and dd-wrt firmwares including devices like WiFi Pineapple, Arduino Yun, and more. But I will focus on the Arduino Yun which runs OpenWrt. Even if the Yun is not specifically banned, the OpenWrt community will dwindle out because of this rule which will hurt Arduino which will hurt American children interested in building devices for the internet of things. Unfortunately a lot of legitimate businesses will suffer because of this, tinkerers will suffer because of this, the open software movement will suffer, the Internet of Things will suffer, and consumers will not get a neat wifi toaster oven because the guy who wants to make that toaster oven will have to jump through more hoops than he is willing. Please reconsider this rule. It will hurt everything from the Internet of Things to custom Android firmware like Cyanogen Mod. We have the right to modify our own devices, if we start broadcasting 5Ghz in ways that break the existing FCC rules then come get that person. Don't create a broad rule that will hurt legitimate business and open software

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Steve

Last Name: Morrow

Mailing Address: 2505 E Wisconsin Ave

City: Appleton

Country: United States

State or Province: WI

ZIP/Postal Code: 54911

Email Address:

Organization Name:

Comment: Please do NOT implement rules that take away the ability of users to install the software of their choosing on their computing devices. Removing this existing ability is a huge step backward in technology and will hinder innovation in unforeseen ways.

Please do NOT implement rules that take away the ability of users to install the software of their choosing on their computing devices. Removing this existing ability is a huge step backward in technology and will hinder innovation in unforeseen ways.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jay

Last Name: Collett

Mailing Address: 1589 Wellesley Dr

City: Lexington

Country: United States

State or Province: KY

ZIP/Postal Code: 40513

Email Address: jay.collett@gmail.com

Organization Name:

Comment: I would respectfully ask that the FCC reconsider implementing rules that limit consumers ability to install soffftware of thier choosing on computing devices. The hopefully unintentional sides effects have a chilling effect on the community of security aware, educational and maker consumers that help drive inovation and security.

I would respectfully ask that the FCC reconsider implementing rules that limit consumers ability to install soffftware of thier choosing on computing devices. The hopefully unintentional sides effects have a chilling effect on the community of security aware, educational and maker consumers that help drive inovation and security.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Cary

Last Name: Ciavolella

Mailing Address: Do Not Wish to Disclose

City: NA

Country: United States

State or Province: VA

ZIP/Postal Code: 20171

Email Address:

Organization Name:

Comment: Here again we see the rule of unintended consequences rearing its ugly head. Before regulations like this are even drafted, don't they go through some kind of expert panel? And I don't mean a panel of Senators, because if we learned anything from Ted Stevens it's that those in charge of regulation rarely understand the science.

This is an incredibly destructive piece of regulation. Many radios operating in the 5GHz range require users to install custom firmware. There are many businesses whose sole operating purpose is to create and customize such firmware. Companies rely on this service to keep their networks operating in a manner that they desire, and to keep them secure from exploits or flaws the manufacturer doesn't have time or expense to repair.

Additionally, the researches who discover these exploits, and bring them to the public attention require the ability to customize radio firmware. Without the ability to make changes, security vulnerabilities may go undiscovered for far longer. Criminal elements won't be deterred by regulation, and will discover weaknesses in commercial routers. Without the ability for law abiding researches to discover those vulnerabilities, countless homes and businesses are at risk.

I still haven't even touched on how this negatively impacts custom operating systems for mobile phones.

Please consider the science, and the necessity for firmware modification. It drives an entire section of industry that you are not even considering (or are just unaware of).

Here again we see the rule of unintended consequences rearing its ugly head. Before regulations like this are even drafted, don't they go through some kind of expert panel? And I don't mean a panel of Senators, because if we learned anything from Ted Stevens it's that those in charge of regulation rarely understand the science.

This is an incredibly destructive piece of regulation. Many radios operating in the 5GHz range require users to install custom firmware. There are many businesses whose sole operating purpose is to create and customize such firmware. Companies rely on this service to keep their networks operating in a manner that they desire, and to keep them secure from exploits or flaws the manufacturer doesn't have time or expense to repair.

Additionally, the researches who discover these exploits, and bring them to the public attention require the ability to customize radio firmware. Without the ability to make changes, security vulnerabilities may go undiscovered for far longer. Criminal elements won't be deterred by regulation, and will discover weaknesses in commercial routers. Without the ability for law abiding researches to discover those vulnerabilities, countless homes and businesses are at risk.

I still haven't even touched on how this negatively impacts custom operating systems for mobile phones.

Please consider the science, and the necessity for firmware modification. It drives an entire section of industry that you are not even considering (or are just unaware of).

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: William

Last Name: Roberts

Mailing Address: 1300 E. Bradford Parkway

City: Springfield

Country: United States

State or Province: MO

ZIP/Postal Code: 65804

Email Address:

Organization Name: Burrell Behavioral Health

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Removing the ability to do so will leave many people even more vulnerable to attacks by hackers. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Removing the ability to do so will leave many people even more vulnerable to attacks by hackers. 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: David

Last Name: Burns

Mailing Address: 29001 Cedar Road, Suite 615

City: Mayfield

Country: United States

State or Province: OH

ZIP/Postal Code: 44143

Email Address: davidsburns@yahoo.com

Organization Name:

Comment: Please not implement rules that take away the ability of users to install the software of their choosing on their computing devices. There are many reasons to do this:

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 not implement rules that take away the ability of users to install the software of their choosing on their computing devices. There are many reasons to do this:

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: Brian

Last Name: Mofmland

Mailing Address: 95 Parkview Street

City: South Weymouth

Country: United States

State or Province: MA

ZIP/Postal Code: 02190

Email Address:

Organization Name:

Comment: This is a security and privacy issue that cannot be understated. Custom firmware is the only way to ensure protection in many cases and that ability must be maintained.

This is a security and privacy issue that cannot be understated. Custom firmware is the only way to ensure protection in many cases and that ability must be maintained.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Graham

Last Name: Braly

Mailing Address: 5567 Coronado Way

City: Rocklin

Country: United States

State or Province: CA

ZIP/Postal Code: 95677

Email Address: GBraly5567@gmail.com

Organization Name:

Comment: Dear Sirs and Ma'ams,

The proposed FCC regulation that would require WiFi equipment manufacturers to lock down WiFi devices through hardware and software security is a ineffective policy that will only restrict technological development and the economy within the United States. By taking away the right to modify or verify the state of the code running on our own devices we Americans lose the ability to make sure manufacturers are adequately caring about our security when they design the devices we buy and further taking away the right for us to modify that code to further protect us or provide us with more functionality. If the FCC wants to lower 5GHz spectrum interference there are more effective ways to do so like lowering the maximum RF power output of routers or encouraging the use of direction antennas that would not radiate RF power away from the house or place of business it is being used in. But regulating the the way in which manufacturers are required to construct consumer equipment restricts our freedoms as Americans and takes away the right to modify and confirm the effectiveness of the equipment that we ourselves own. I sincerely hope the FCC rethinks this proposed regulation and stops in from moving forward, it is in the best interests of the American people that this regulation not pass.

Sincerely, a concerned citizen.

Dear Sirs and Ma'ams,

The proposed FCC regulation that would require WiFi equipment manufacturers to lock down WiFi devices through hardware and software security is a ineffective policy that will only restrict technological development and the economy within the United States. By taking away the right to modify or verify the state of the code running on our own devices we Americans lose the ability to make sure manufacturers are adequately caring about our security when they design the devices we buy and further taking away the right for us to modify that code to further protect us or provide us with more functionality. If the FCC wants to lower 5GHz spectrum interference there are more effective ways to do so like lowering the maximum RF power output of routers or encouraging the use of direction antennas that would not radiate RF power away from the house or place of business it is being used in. But regulating the the way in which manufacturers are required to construct consumer equipment restricts our freedoms as Americans and takes away the right to modify and confirm the effectiveness of the equipment that we ourselves own. I sincerely hope the FCC rethinks this proposed regulation and stops in from moving forward, it is in the best interests of the American people that this regulation not pass.

Sincerely, a concerned citizen.

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: Dylan

Last Name: Gray

Mailing Address: 5817A Leslie Ave

City: Nashville

Country: United States

State or Province: TN

ZIP/Postal Code: 37209

Email Address:

Organization Name:

Comment: Why 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. The rules would likely: (1) Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc. (2) Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes. (3) Ban installation of custom phone firmware. (4) Discourage the development of alternative free and open source WiFi firmware, like OpenWrt. (5) Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster. & (6) Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses. Please reconsider

Why 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. The rules would likely: (1) Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc. (2) Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes. (3) Ban installation of custom phone firmware. (4) Discourage the development of alternative free and open source WiFi firmware, like OpenWrt. (5) Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster. & (6) Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses. Please reconsider

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: Brian

Last Name: Fabiano

Mailing Address: 78 Eastwood Drive Apt 413

City: South Burlington

Country: United States

State or Province: VT

ZIP/Postal Code: 05403

Email Address:

Organization Name:

Comment: Please do not move forward with requiring security features to ban the flashing custom firmware of wireless router &/or cell phones. While I understand the desire to control end users ability to operate their devices radio's outside of the permitted specifications, I feel that this proposed rule is not the best way to achieve these results. Flashing custom firmware can sometimes be a necessity to receive security updates that the device manufacturers either will not release or release too late to be effective, especially for older devices. For example look at Android's fragmentation due to carrier/manufacture delays in updates. I own a Samsung Galaxy S3 on AT&T's network and the latest Android update I can receive is Android 4.4.2, which was released in November 2014 (source: <http://www.att.com/esupport/article.jsp?sid=KB415621&cv=820>). The phone is still in good working condition but due the lack of official updates I've had to stop using the device. If I couldn't have afforded a new phone, I would have been forced to use a vulnerable version of Android because the carrier/manufacture doesn't care to release any more updates for it. But if flashed the phone with a custom firmware I could manually update it to Android 5.1.1. In conclusion, custom firmware's on devices can be a necessity and the ability to flash them at will should not be taken away from the public.

Please do not move forward with requiring security features to ban the flashing custom firmware of wireless router &/or cell phones. While I understand the desire to control end users ability to operate their devices radio's outside of the permitted specifications, I feel that this proposed rule is not the best way to achieve these results. Flashing custom firmware can sometimes be a necessity to receive security updates that the device manufacturers either will not release or release too late to be effective, especially for older devices. For example look at Android's fragmentation due to carrier/manufacture delays in updates. I own a Samsung Galaxy S3 on AT&T's network and the latest Android update I can receive is Android 4.4.2, which was released in November 2014 (source: <http://www.att.com/esupport/article.jsp?sid=KB415621&cv=820>). The phone is still in good working condition but due the lack of official updates I've had to stop using the device. If I couldn't have afforded a new phone, I would have been forced to use a vulnerable version of Android because the carrier/manufacture doesn't care to release any more updates for it. But if flashed the phone with a custom firmware I could manually update it to Android 5.1.1. In conclusion, custom firmware's on devices can be a necessity and the ability to flash them at will should not be taken away from the public.

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: Josh

Last Name: Bartley

Mailing Address: 340 S Lemon Ave #4355

City: Walnut

Country: United States

State or Province: CA

ZIP/Postal Code: 91789-2706

Email Address:

Organization Name:

Comment: I work in the information technology industry and a rule proposed as this would be disastrous for the industry and consumers. As a consumer, I have modified the firmware on my wireless router to receive extra functionality, like VPN, DNS, and a guest network for visitors to my house. Never to skirt the rules of the FCC. Time and time again the rules and regulations have been designed to prevent a situation that causes more harm than good. Manufactures would have one of two options to prevent modification, add a separate chip, or add a layer of cryptography that increases costs while not adding functionality. Furthermore, manufactures frequently stop supporting older hardware and custom firmware is the only way to patch security holes without further spending more on the consumer. From old WiFi routers, to older Android phones, streaming devices, home automation equipment, RC cars or model airplanes would all be negatively affected without any actual, detectable, improvement in the 5ghz radio range. In my opinion, this proposal should be reconsidered and instead focus on education of consumers along with easier to follow rules and regulations on spectrum usage.

I work in the information technology industry and a rule proposed as this would be disastrous for the industry and consumers. As a consumer, I have modified the firmware on my wireless router to receive extra functionality, like VPN, DNS, and a guest network for visitors to my house. Never to skirt the rules of the FCC. Time and time again the rules and regulations have been designed to prevent a situation that causes more harm than good. Manufactures would have one of two options to prevent modification, add a separate chip, or add a layer of cryptography that increases costs while not adding functionality. Furthermore, manufactures frequently stop supporting older hardware and custom firmware is the only way to patch security holes without further spending more on the consumer. From old WiFi routers, to older Android phones, streaming devices, home automation equipment, RC cars or model airplanes would all be negatively affected without any actual, detectable, improvement in the 5ghz radio range. In my opinion, this proposal should be reconsidered and instead focus on education of consumers along with easier to follow rules and regulations on spectrum usage.

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: Travis

Last Name: Swaim

Mailing Address: 103 Asbill Ave.

City: Yukon

Country: United States

State or Province: OK

ZIP/Postal Code: 73099

Email Address: cheeto4493@gmail.com

Organization Name: null

Comment: Please DO NOT pass this regulation that will restrict users from fixing the bugs left in software provided by vendors. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Wifi routers have more usage when the software can be modified to the user's needs while still staying within current regulations of radio power and channel usage. 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 pass this regulation that will restrict users from fixing the bugs left in software provided by vendors. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Wifi routers have more usage when the software can be modified to the user's needs while still staying within current regulations of radio power and channel usage. 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: Shawn

Last Name: Baker

Mailing Address: 2400 Britain Ct

City: Carrollton

Country: United States

State or Province: TX

ZIP/Postal Code: 75006

Email Address: grillDOS@gmail.com

Organization Name:

Comment: Please continue to allow purchasers of hardware to install software of their choosing on their devices, including devices that operate on radio frequencies apportioned to WiFi technology.

Thank you.

Please continue to allow purchasers of hardware to install software of their choosing on their devices, including devices that operate on radio frequencies apportioned to WiFi technology.

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: Christopher

Last Name: Milliken

Mailing Address: 874 Cranbrook Drive

City: Highland Heights

Country: United States

State or Province: OH

ZIP/Postal Code: 44143

Email Address: c.milliken@ameritech.net

Organization Name:

Comment: I respectfully request that you elect to NOT implement rules that restrict the ability of private citizens and users to install software of their choosing on wireless devices and routers. Wireless networking research depends on the ability of researchers to investigate and modify their devices and stifling this research inhibits job growth. Further, Americans need the ability to fix security holes in their devices when the manufacturer chooses or is unable to do so. History has shown the individual users have fixed serious bugs in their wifi drivers, a practice which would be banned under the NPRM.

Please do not implement rules that will restrict software modifications to wireless devices. Thank you.

I respectfully request that you elect to NOT implement rules that restrict the ability of private citizens and users to install software of their choosing on wireless devices and routers. Wireless networking research depends on the ability of researchers to investigate and modify their devices and stifling this research inhibits job growth. Further, Americans need the ability to fix security holes in their devices when the manufacturer chooses or is unable to do so. History has shown the individual users have fixed serious bugs in their wifi drivers, a practice which would be banned under the NPRM.

Please do not implement rules that will restrict software modifications to wireless devices. 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: Danylo

Last Name: Kharmyshev

Mailing Address: 126 Prince Street

City: Boston

Country: United States

State or Province: MA

ZIP/Postal Code: 02113

Email Address:

Organization Name:

Comment: I have a router that's more functional and secure because of an open source community that maintains the firmware. If this rule had been implemented I'd have to toss it into the recycling bin.

That's great for router companies, bad for consumers.

I have a router that's more functional and secure because of an open source community that maintains the firmware. If this rule had been implemented I'd have to toss it into the recycling bin.

That's great for router companies, bad for 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: Maxwell

Last Name: Petersen

Mailing Address: 1444 S Busse Rd

City: Mount Prospect

Country: United States

State or Province: IL

ZIP/Postal Code: 60056

Email Address:

Organization Name:

Comment: In my opinion this rule should not be put in place as by requiring these "security" features to be put in place it will in fact open up a whole plethora of issues with making sure the original Firmware is secure enough to prevent being hacked itself. I myself have flashed my own router and will continue to do so even with these "security" programs in place. I trust myself to maintain a higher level of security off of the Open Source Firmware than I do the de facto Firmware given to me by the Manufacturer. So all in all by imposing these "security" rules you are making it more difficult to allow people to be able to verify that their own router is safe and secure from any form of malicious attacks.

In my opinion this rule should not be put in place as by requiring these "security" features to be put in place it will in fact open up a whole plethora of issues with making sure the original Firmware is secure enough to prevent being hacked itself. I myself have flashed my own router and will continue to do so even with these "security" programs in place. I trust myself to maintain a higher level of security off of the Open Source Firmware than I do the de facto Firmware given to me by the Manufacturer. So all in all by imposing these "security" rules you are making it more difficult to allow people to be able to verify that their own router is safe and secure from any form of malicious attacks.

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: Walker

Mailing Address: 2919 W 92nd St

City: Leawood

Country: United States

State or Province: KS

ZIP/Postal Code: 66206

Email Address: chopperwalker@yahoo.com

Organization Name:

Comment: I believe this proposal oversteps the boundaries of regulation. There are rules that already govern of use of these devices. Restricting technology add another layer of protection can inhibit development and is overkill. A comparison is that it's already illegal to steal, but I don't have to have my hands bound when I enter a store.

I believe this proposal oversteps the boundaries of regulation. There are rules that already govern of use of these devices. Restricting technology add another layer of protection can inhibit development and is overkill. A comparison is that it's already illegal to steal, but I don't have to have my hands bound when I enter a store.

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: Alex

Last Name: Goven

Mailing Address: 884 S Nicholas Ave

City: White Cloud

Country: United States

State or Province: MI

ZIP/Postal Code: 49349-9736

Email Address: alexgoven@gmail.com

Organization Name:

Comment: Third party open source firmware should be allowed to run on networking devices such as routers. My reasoning is simple: There is no such thing as a longer lasting security update support than from open source software. To this very day, there is still support for the WRT54GL. Banning such open source firmware would pose a greater national security risk because you cannot realistically expect companies to release security updates decades after a router is released. You would realize this is the case if you into my claims.

If you want to keep up national security against hackers abroad, that requires citizens and small companies to be able to protect themselves when they cannot afford to upgrade their hardware for nothing more than a new lease on security updates. Banning open source firmware would in effect be a grave mistake.

Third party open source firmware should be allowed to run on networking devices such as routers. My reasoning is simple: There is no such thing as a longer lasting security update support than from open source software. To this very day, there is still support for the WRT54GL. Banning such open source firmware would pose a greater national security risk because you cannot realistically expect companies to release security updates decades after a router is released. You would realize this is the case if you into my claims.

If you want to keep up national security against hackers abroad, that requires citizens and small companies to be able to protect themselves when they cannot afford to upgrade their hardware for nothing more than a new lease on security updates. Banning open source firmware would in effect be a grave mistake.

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: Greg

Last Name: Betz

Mailing Address: 1659 Hulman Waye Ct

City: TERRE HAUTE

Country: United States

State or Province: IN

ZIP/Postal Code: 47803

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: Patrick

Last Name: Cloke

Mailing Address: 425 Broadway, Apt. 14

City: Somerville

Country: United States

State or Province: MA

ZIP/Postal Code: 02145

Email Address:

Organization Name:

Comment: I would respectfully ask the FCC to reconsider the implications of these rules in the ability of end-users to install the software of their choosing on their computing devices. There are a variety of reasons that a user might wish to do this:

- * 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.
- * It gives large corporations complete control over another area of American lives.

Thanks for your time!

I would respectfully ask the FCC to reconsider the implications of these rules in the ability of end-users to install the software of their choosing on their computing devices. There are a variety of reasons that a user might wish to do this:

- * 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.
- * It gives large corporations complete control over another area of American lives.

Thanks for your time!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Florent

Last Name: Tainturier

Mailing Address: 109, quai de la Banquiere

City: Saint Andre de la Roche

Country: France

State or Province: Provence-Alpes-Cote d'Azur

ZIP/Postal Code: 06730

Email Address: florent.tainturier@gmail.com

Organization Name:

Comment: Dear,

The rules described in this project go against the creativity movement of free Engineer as I am. Openhardware and Opensoftware will be impacted by such policy.

Whereas, open movement are the base of very new business (arduino, raspeberry, etc...) and of new tool for everyone (Blender, The gimp, etc...).

I beg the FCC to renonce to its policy.

Dear,

The rules described in this project go against the creativity movement of free Engineer as I am. Openhardware and Opensoftware will be impacted by such policy.

Whereas, open movement are the base of very new business (arduino, raspeberry, etc...) and of new tool for everyone (Blender, The gimp, etc...).

I beg the FCC to renonce to its policy.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Wood

Mailing Address: 997 Ridge Road

City: Queensbury

Country: United States

State or Province: NY

ZIP/Postal Code: 12804

Email Address: jbevren@gmail.com

Organization Name: I'm an individual citizen concerned about us losing our rights.

Comment: Some of the verbage in this document will make it illegal to flash custom or modified firmware to WiFi routers. This is an issue for citizens as explained below.

First, many routers come with portions of outdated software that are a security risk. The manufacturer in many cases refuses to provide an updated firmware, forcing the hardware's owner to go to third party providers to flash custom firmware into the router to maintain security. As a case in point, I own an older ubiquiti wireless AP that only supports SSL version 3. This version of SSL is insecure to the extent that any up-to-date web browser won't even support a secure and encrypted connection to the router, requiring me to send administrative passwords over the air in plain text.

Second, as a member of the free market in the united states I fully understand the need to maintain trade secrets. However when I purchase a tangible object such as a home wifi router, I have reason to believe that this device is mine to do with as I please, limited to restrictions already provided by current and applicable laws.

Third, many routers simply do not provide the functionality needed by more advanced home network users, including but not limited to increased security configurations such as built-in VPN support without relying on a potentially hacked PC to provide it, an advanced automatic configuration of the home network based on options not at all available in most manufacturers' firmware.

Please reject this proposal and request that it is rewritten in a way that guarantees the freedom that everyone in the United States is so proud of our country for. The freedom to ensure our home networks are secure and to modify a device that Americans spent legal U.S. monies on. The freedom to use third-party updates in routers to help prevent devices containing harmful chemicals from being sent to landfills even though they could be updated with third party software to return them to a secure and useful state.

Thank you for your time.

David Wood

Some of the verbage in this document will make it illegal to flash custom or modified firmware to WiFi routers. This is an issue for citizens as explained below.

First, many routers come with portions of outdated software that are a security risk. The manufacturer in many cases refuses to provide an updated firmware, forcing the hardware's owner to go to third party providers to flash custom firmware into the router to maintain security. As a case in point, I own an older ubiquiti wireless AP that only supports

SSL version 3. This version of SSL is insecure to the extent that any up-to-date web browser won't even support a secure and encrypted connection to the router, requiring me to send administrative passwords over the air in plain text.

Second, as a member of the free market in the united states I fully understand the need to maintain trade secrets. However when I purchase a tangible object such as a home wifi router, I have reason to believe that this device is mine to do with as I please, limited to restrictions already provided by current and applicable laws.

Third, many routers simply do not provide the functionality needed by more advanced home network users, including but not limited to increased security configurations such as built-in VPN support without relying on a potentially hacked PC to provide it, an advanced automatic configuration of the home network based on options not at all available in most manufacturers' firmware.

Please reject this proposal and request that it is rewritten in a way that guarantees the freedom that everyone in the United States is so proud of our country for. The freedom to ensure our home networks are secure and to modify a device that Americans spent legal U.S. monies on. The freedom to use third-party updates in routers to help prevent devices containing harmful chemicals from being sent to landfills even though they could be updated with third party software to return them to a secure and useful state.

Thank you for your time.

David Wood

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: Patrick

Last Name: ONeil

Mailing Address: 6300 W 400 S

City: Westpoint

Country: United States

State or Province: IN

ZIP/Postal Code: 47992

Email Address: patrickoneil650@gmail.com

Organization Name:

Comment: When I purchase a WiFi router or smartphone, I own it in its entirety. If I desire to change the operating system (the firmware in this case) that is my right as the sole owner of my device. It is not for government, nor corporations, to restrict how I can use my private property. I will purchase WiFi routers and change the firmware to opensource firmware, both because it is my right, as a means of improving my control and knowledge of how and what my device is doing, as a learning tool to better understand the workings of MY device and software, and to help further innovation. The Internet itself is a creation of opensource software research. All protocols used are open, all innovation comes from independent developers. I ALWAYS alter the software on my computers, smartphones, and WiFi routers because I can, because I enjoy it, because it is my right, and nothing will stop it. Do not attempt to destroy innovation and perpetual rights for the sake of profits for a few creaky corrosive or as flailing, wrong-headed attempt to improve security.

When I purchase a WiFi router or smartphone, I own it in its entirety. If I desire to change the operating system (the firmware in this case) that is my right as the sole owner of my device. It is not for government, nor corporations, to restrict how I can use my private property. I will purchase WiFi routers and change the firmware to opensource firmware, both because it is my right, as a means of improving my control and knowledge of how and what my device is doing, as a learning tool to better understand the workings of MY device and software, and to help further innovation. The Internet itself is a creation of opensource software research. All protocols used are open, all innovation comes from independent developers. I ALWAYS alter the software on my computers, smartphones, and WiFi routers because I can, because I enjoy it, because it is my right, and nothing will stop it. Do not attempt to destroy innovation and perpetual rights for the sake of profits for a few creaky corrosive or as flailing, wrong-headed attempt to improve security.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Donald

Last Name: Bindner

Mailing Address: 22463 State Highway H

City: Kirksville

Country: United States

State or Province: MO

ZIP/Postal Code: 63501

Email Address: don.bindner@gmail.com

Organization Name:

Comment: This proposal is a terrible and shortsighted idea. Banning the modification of software on a router prevents or hinders the use of any open source alternative. This is no small issue, as proprietary routers have a notorious history of security vulnerabilities and long-term unresolved bugs.

Some companies have based their router lines around adapting open source firmwares to their hardware and could be effectively run out of business (the GPL license is for example strictly incompatible with "locking down" of the firmware). This is effectively the FCC choosing winners among the wireless router vendors.

Open source firmwares allow for experimentation and academic research that is prevented by cryptographically locking down a router. Great strides have been made in recent years on the issue of "buffer bloat," for example, by researchers using open source firmwares. This rule will prevent and hinder that kind of work.

And this rule can't possibly hope to prevent boosting of signal, because it can still be accomplished with modified antennas and amplifiers. The scenario of someone taking a router and adjusting the software just to boost the signal is obscure by comparison, and trying to attack that one vector at the expense of all the other benefits that come from open source firmwares just doesn't make sense.

It makes much more sense for circuitry to be power limited, or for limits to be built into the chips themselves, so the firmware on a device can be as flexible as possible.

This model has worked well for GPS devices, which typically communicate using a simple open protocol but refuse to operate under "ballistic missile" conditions. Nothing prevents a GPS device from being used with open source software in a high altitude balloon research situation, yet safety is maintained. A router should similarly be able to work with open firmware, even if there is an interest served by limiting power output.

This proposal is a terrible and shortsighted idea. Banning the modification of software on a router prevents or hinders the use of any open source alternative. This is no small issue, as proprietary routers have a notorious history of security vulnerabilities and long-term unresolved bugs.

Some companies have based their router lines around adapting open source firmwares to their hardware and could be effectively run out of business (the GPL license is for example strictly incompatible with "locking down" of the firmware). This is effectively the FCC choosing winners among the wireless router vendors.

Open source firmwares allow for experimentation and academic research that is prevented by cryptographically locking

down a router. Great strides have been made in recent years on the issue of "buffer bloat," for example, by researchers using open source firmwares. This rule will prevent and hinder that kind of work.

And this rule can't possibly hope to prevent boosting of signal, because it can still be accomplished with modified antennas and amplifiers. The scenario of someone taking a router and adjusting the software just to boost the signal is obscure by comparison, and trying to attack that one vector at the expense of all the other benefits that come from open source firmwares just doesn't make sense.

It makes much more sense for circuitry to be power limited, or for limits to be built into the chips themselves, so the firmware on a device can be as flexible as possible.

This model has worked well for GPS devices, which typically communicate using a simple open protocol but refuse to operate under "ballistic missile" conditions. Nothing prevents a GPS device from being used with open source software in a high altitude balloon research situation, yet safety is maintained. A router should similarly be able to work with open firmware, even if there is an interest served by limiting power output.

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: Eggleston

Mailing Address: 7130 Gladstone Dr

City: Madison

Country: United States

State or Province: WI

ZIP/Postal Code: 53719

Email Address: eggled@outlook.com

Organization Name:

Comment: I have used (and will use again) custom firmware to get the most from my home network router. This includes better security features than the stock router, like vpns and firewalls, and also advanced networking features like DNS servers and multiple AP mode for wireless networks.

The affordable routers that benefit so heavily from this custom firmware are all SoC-based, including the wireless radios. As a result, this regulation would make it very difficult and/or expensive to get a router with the features I mentioned. I think this is a disservice to consumers, and I think it will do little to address the real problem (since there will always be those who can work around the safeguards added due to this proposed rule).

I have used (and will use again) custom firmware to get the most from my home network router. This includes better security features than the stock router, like vpns and firewalls, and also advanced networking features like DNS servers and multiple AP mode for wireless networks.

The affordable routers that benefit so heavily from this custom firmware are all SoC-based, including the wireless radios. As a result, this regulation would make it very difficult and/or expensive to get a router with the features I mentioned. I think this is a disservice to consumers, and I think it will do little to address the real problem (since there will always be those who can work around the safeguards added due to this proposed rule).

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nathaniel

Last Name: Hatley

Mailing Address: 12683 Stony Creek Lane

City: Locust

Country: United States

State or Province: NC

ZIP/Postal Code: 28097

Email Address: Nathaniel.Hatley@gmail.com

Organization Name:

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

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

Last Name: Highet

Mailing Address: 4 Teakwood Ln

City: Barnegat

Country: United States

State or Province: NJ

ZIP/Postal Code: 08005-1817

Email Address: chrish78@gmail.com

Organization Name: null

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Public servants of the Federal Communications Commission,

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

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nathan

Last Name: Reed

Mailing Address: 3505 Pleasant Ave

City: Allentown

Country: United States

State or Province: PA

ZIP/Postal Code: 18103

Email Address:

Organization Name:

Comment: These rules do not seem like a good idea. They will make it harder for Americans and others to innovate and learn about new technologies by blocking hobbyist implementations. Blocking custom router firmware and other unsigned code with access to wifi firmware will allow router companies to restrict features in their firmware without any fear of customers being able to unlock them. Overall, these rules are more restrictive on the American customer who wishes to modify and hack on their own hardware that they purchased.

These rules do not seem like a good idea. They will make it harder for Americans and others to innovate and learn about new technologies by blocking hobbyist implementations. Blocking custom router firmware and other unsigned code with access to wifi firmware will allow router companies to restrict features in their firmware without any fear of customers being able to unlock them. Overall, these rules are more restrictive on the American customer who wishes to modify and hack on their own hardware that they purchased.

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: Van Giang

Last Name: Ho

Mailing Address: 42 Fleetwood Circuit

City: Woodvale

Country: Australia

State or Province: WA

ZIP/Postal Code: 6026

Email Address: giangho@gmail.com

Organization Name:

Comment: Vote Against.

Firmware are the same as software which needs to be maintained. If there were bugs or security vulnerability discovered but not fixed it could lead to disastrous consequences.

Please don't pass this regulation. Ask instead companies to release the firmware to open source community when they no longer provide updates.

Thanks

Vote Against.

Firmware are the same as software which needs to be maintained. If there were bugs or security vulnerability discovered but not fixed it could lead to disastrous consequences.

Please don't pass this regulation. Ask instead companies to release the firmware to open source community when they no longer provide updates.

Thanks

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: Roel

Last Name: van Westerop

Mailing Address: Herman de Manlaan 6

City: Rosmalen

Country: Netherlands

State or Province: Noord-Brabant

ZIP/Postal Code: 5242CW

Email Address: rvwesterop@hotmail.com

Organization Name:

Comment: Hereby I would like to 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.

Additional points of emphasis:

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

Hereby I would like to 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.

Additional points of emphasis:

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

Last Name: Brown

Mailing Address: 100 Institute Road

City: Worcester

Country: United States

State or Province: MA

ZIP/Postal Code: 01609

Email Address: lebrown@wpi.edu

Organization Name:

Comment: Any rule that limits the software that a user can install on their own devices is at odds with preserving their freedom, and unreasonably limits innovation. Customization in software and hardware is an integral part of American innovation and ingenuity. Additionally, as most development kits are priced out of feasibility for individuals, this takes away the potential for new products to be developed.

Any rule that limits the software that a user can install on their own devices is at odds with preserving their freedom, and unreasonably limits innovation. Customization in software and hardware is an integral part of American innovation and ingenuity. Additionally, as most development kits are priced out of feasibility for individuals, this takes away the potential for new products to be developed.

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: Ernest

Mailing Address: 902 S Walden St

City: Aurora

Country: United States

State or Province: CO

ZIP/Postal Code: 80017

Email Address: null

Organization Name: null

Comment: This is a bad rule that will limit and curtail personal freedom to use enhanced functionality of many devices. Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This ruling could open up vulnerabilities in older hardware that will likely be exploited.

This ruling will also limit what users may do with their personal devices. 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 pass this onerous legislation.

This is a bad rule that will limit and curtail personal freedom to use enhanced functionality of many devices. Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This ruling could open up vulnerabilities in older hardware that will likely be exploited.

This ruling will also limit what users may do with their personal devices. 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 pass this onerous legislation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Maximus

Last Name: Zeebra

Mailing Address: Street

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32811

Email Address: null

Organization Name: null

Comment: This is a terrible idea in practice and a step in the wrong direction. There need not be further restrictions on hardware/software, rather further loosening up in regards to installing whatever software you want, on any given piece of hardware.

This pretty much restricts everyone from installing any operating system of their choice on ANY device which have wireless. This includes ALL computer, all mobile devices and many more.

In real freedom, no hardware should come restricted with one operating system. Ideally ALL users should be presented with many options of which operating system they want to install. Such a proposal as this is draconic and pretty much buries the idea of cooperating on hardware firmware/drivers and letting the user install anything they want on top of that.

This proposal removes freedoms of the user, freedom that does not really exist very much today, but at least still is possible.

In an ideal world all electronic devices would be delivered with a single kernel, which all hardware companies worked on and integrated their drivers/firmware in. This would leave it entirely up to the user, on ANY device, which type of operating system they want to have on their device, including Android, Ios, Windows, GNU or any other system.

This is a terrible idea in practice and a step in the wrong direction. There need not be further restrictions on hardware/software, rather further loosening up in regards to installing whatever software you want, on any given piece of hardware.

This pretty much restricts everyone from installing any operating system of their choice on ANY device which have wireless. This includes ALL computer, all mobile devices and many more.

In real freedom, no hardware should come restricted with one operating system. Ideally ALL users should be presented with many options of which operating system they want to install. Such a proposal as this is draconic and pretty much buries the idea of cooperating on hardware firmware/drivers and letting the user install anything they want on top of that.

This proposal removes freedoms of the user, freedom that does not really exist very much today, but at least still is possible.

In an ideal world all electronic devices would be delivered with a single kernel, which all hardware companies worked on and integrated their drivers/firmware in. This would leave it entirely up to the user, on ANY device, which type of operating system they want to have on their device, including Android, Ios, Windows, GNU or any other system.

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: Josh

Last Name: Lovison

Mailing Address: 275 E Green St #1640

City: Los Angeles

Country: United States

State or Province: CA

ZIP/Postal Code: 91101

Email Address: jlovison@gmail.com

Organization Name: null

Comment: A great deal of the innovation in the software that runs on hardware with radios (routers, and especially smartphone), is very heavily influenced by open source or community driven modifications.

Heck, Apple's original AppStore was a near exact copy of the community "Installer.app" that was used on jailbroken iPhones at a time when Apple was saying that web apps were sufficient for mobile app needs.

Android is even more heavily influenced by community mods, and it is arguable that those modifications are a considerable factor in its competitive edge against Apple (many of the features unique to Android in official updates were first developed in community modifications).

So while radios being improperly used on disallowed bands, etc, is not ideal, this needs to be weighed against the extreme benefit of having a hobbist niche doing the heavy lifting of prototyping concepts through modifications that manufactures later incorporate. Without this element, the progress of new ideas in the software space for devices with radios will slow greatly.

A great deal of the innovation in the software that runs on hardware with radios (routers, and especially smartphone), is very heavily influenced by open source or community driven modifications.

Heck, Apple's original AppStore was a near exact copy of the community "Installer.app" that was used on jailbroken iPhones at a time when Apple was saying that web apps were sufficient for mobile app needs.

Android is even more heavily influenced by community mods, and it is arguable that those modifications are a considerable factor in its competitive edge against Apple (many of the features unique to Android in official updates were first developed in community modifications).

So while radios being improperly used on disallowed bands, etc, is not ideal, this needs to be weighed against the extreme benefit of having a hobbist niche doing the heavy lifting of prototyping concepts through modifications that manufactures later incorporate. Without this element, the progress of new ideas in the software space for devices with radios will slow greatly.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: david

Last Name: milbut

Mailing Address: 139 shoemaker st

City: dunmore

Country: United States

State or Province: PA

ZIP/Postal Code: 18512

Email Address: aikodude@yahoo.com

Organization Name: null

Comment: NO. leave the freedom to tinker, repair and modify our bought and paid for devices alone. please stop all the meddling in the markets!

maybe you can take a year or so off from making new regulations and decide on a several hundred existing regulations that you can retire!

NO. leave the freedom to tinker, repair and modify our bought and paid for devices alone. please stop all the meddling in the markets!

maybe you can take a year or so off from making new regulations and decide on a several hundred existing regulations that you can retire!

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: Chad

Last Name: Valente

Mailing Address: 1645 East Thomas Rd.

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85016

Email Address: insignificantuser@gmail.com

Organization Name: null

Comment: This rule is ridiculous. I bought a thing, it should be mine to do with how I like. This is on par with being unable to do my own car maintenance or modification because the car might be used to commit a crime. I can't think of more than one way to say unnecessary governmental overreach, so instead I'm just going to copy it five times.

Unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach. Please don't do this.

This rule is ridiculous. I bought a thing, it should be mine to do with how I like. This is on par with being unable to do my own car maintenance or modification because the car might be used to commit a crime. I can't think of more than one way to say unnecessary governmental overreach, so instead I'm just going to copy it five times. Unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach, unnecessary governmental overreach. Please don't do this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Anonymous

Mailing Address: 15836 Strickland Ct

City: Charlotte

Country: United States

State or Province: NC

ZIP/Postal Code: 28277

Email Address: mt_xing@live.com

Organization Name: null

Comment: This is a bad idea. Please don't.

This is a bad idea. Please don't.

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: Hector

Last Name: Hernandez

Mailing Address: 409 High St SE, Apt A

City: Albuquerque

Country: United States

State or Province: NM

ZIP/Postal Code: 87102

Email Address: hectorgabehernandez@gmail.com

Organization Name: null

Comment: This is not such a good idea. Sure, Mr. Joe Consumer won't really want (or know how) to unlock their phone's bootloader to install a custom operating system. They won't really need to side-boot Linux on their Mac or PC. Sure. But this regulation would severely hurt the people who do.

There is no reason to limit this sort of customization if it doesn't hurt the manufacturer / ISP/ service provider directly or indirectly. This is a hobby for a lot of people - for others, it's a livelihood. Many people do this simply because they do not like a few aspects of a phone (whether it be jailbreaking an iPhone or rooting an Android device). This companies create their operating systems on the basis of what their market research has told them what the majority of consumers like. But that's just it; if there is a majority there will always be a minority. And that minority shouldn't suffer by having their right to tinker and customize their devices taken away. They have purchased these devices outright and should be able to customize them as they please.

This is not such a good idea. Sure, Mr. Joe Consumer won't really want (or know how) to unlock their phone's bootloader to install a custom operating system. They won't really need to side-boot Linux on their Mac or PC. Sure. But this regulation would severely hurt the people who do.

There is no reason to limit this sort of customization if it doesn't hurt the manufacturer / ISP/ service provider directly or indirectly. This is a hobby for a lot of people - for others, it's a livelihood. Many people do this simply because they do not like a few aspects of a phone (whether it be jailbreaking an iPhone or rooting an Android device). This companies create their operating systems on the basis of what their market research has told them what the majority of consumers like. But that's just it; if there is a majority there will always be a minority. And that minority shouldn't suffer by having their right to tinker and customize their devices taken away. They have purchased these devices outright and should be able to customize them as they please.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: sean

Last Name: peat

Mailing Address: 4248 moraga st

City: san francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94122

Email Address: truks755@gmail.com

Organization Name: null

Comment: please dont allow manufacturers to lock devices and not allow modifications.

please dont allow manufacturers to lock devices and not allow modifications.

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: will

Last Name: rogers

Mailing Address: 2323 9th ave se

City: olympia

Country: United States

State or Province: WA

ZIP/Postal Code: 98502

Email Address: null

Organization Name: null

Comment: Do not lock down anything. We have a right to ownership and by that we are allowed to tinker with things we own. Don't give that right away because of fear

Do not lock down anything. We have a right to ownership and by that we are allowed to tinker with things we own. Don't give that right away because of fear

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Anonymous

Mailing Address: 1402 Holloman Dr

City: College Station

Country: United States

State or Province: TX

ZIP/Postal Code: 77845

Email Address: null

Organization Name: null

Comment: There is never a need to lock down or restrict a device. Why limit a device and its capabilities when technology is there to advance us as a society? How can we as a society advance with roadblocks we set up for ourselves. Leaving technology open source doesn't create danger or vulnerability, hindering a person and their will does.

There is never a need to lock down or restrict a device. Why limit a device and its capabilities when technology is there to advance us as a society? How can we as a society advance with roadblocks we set up for ourselves. Leaving technology open source doesn't create danger or vulnerability, hindering a person and their will does.

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: Bill

Last Name: Conn

Mailing Address: 44686 301st St

City: Volin

Country: United States

State or Province: SD

ZIP/Postal Code: 57072

Email Address: null

Organization Name: null

Comment: I understand the intentions of these proposed rules and agree that limiting devices from interfering with spectrum space they shouldn't have access to is a good thing. However requiring that devices have locked firmware will have the unacceptable affect of locking hardware owners out of controlling their own hardware. This is also a huge blow to open source software and development of open source wireless solutions. The onus of following the laws and regulations should stay on the owners of the device where it currently is. The vast majority of users aren't even going to think about flashing their firmware, only the tinkerers and enthusiasts who drive much innovation through theses open source communities attempt these sorts of things. These are people who are already familiar with the rules in place for spectrum sharing and would be at a low risk for violating them. The proposed rules for locking firmware will close down many avenues that these enthusiasts use to innovate and experiment. Please reconsider implementing the proposed firmware locking rules for Wireless Devices.

Thank you,

Bill Conn

I understand the intentions of these proposed rules and agree that limiting devices from interfering with spectrum space they shouldn't have access to is a good thing. However requiring that devices have locked firmware will have the unacceptable affect of locking hardware owners out of controlling their own hardware. This is also a huge blow to open source software and development of open source wireless solutions. The onus of following the laws and regulations should stay on the owners of the device where it currently is. The vast majority of users aren't even going to think about flashing their firmware, only the tinkerers and enthusiasts who drive much innovation through theses open source communities attempt these sorts of things. These are people who are already familiar with the rules in place for spectrum sharing and would be at a low risk for violating them. The proposed rules for locking firmware will close down many avenues that these enthusiasts use to innovate and experiment. Please reconsider implementing the proposed firmware locking rules for Wireless Devices.

Thank you,

Bill Conn

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Person

Mailing Address: 200 Campbell St.

City: Durand

Country: United States

State or Province: MI

ZIP/Postal Code: 48429

Email Address:

Organization Name: null

Comment: I would be very opposed to locking down devices with "modular wireless radios" because it takes away from the freedom of the user.

Freedom is something that is prevalent in the United States and as such, it should continue to be so, in any way shape or form. By locking down electronic devices you are taking away from the freedom of the user.

Jailbreaking or rooting is a form of expression of freedom, by locking down these devices, you are removing the ability to express that freedom. The purchaser of an electronic device should be allowed full control over their device and not be mandated to follow strict governmental guidelines pertaining to the use of the device.

On one hand, the advantage of locking down devices is that they are more secure, and are therefore less vulnerable to attack from a malicious party. On the other hand, freedom of control over electronic devices is taken away. Please do not take away our freedom. I urge you not to take action regarding this.

I would be very opposed to locking down devices with "modular wireless radios" because it takes away from the freedom of the user.

Freedom is something that is prevalent in the United States and as such, it should continue to be so, in any way shape or form. By locking down electronic devices you are taking away from the freedom of the user.

Jailbreaking or rooting is a form of expression of freedom, by locking down these devices, you are removing the ability to express that freedom. The purchaser of an electronic device should be allowed full control over their device and not be mandated to follow strict governmental guidelines pertaining to the use of the device.

On one hand, the advantage of locking down devices is that they are more secure, and are therefore less vulnerable to attack from a malicious party. On the other hand, freedom of control over electronic devices is taken away. Please do not take away our freedom. I urge you not to take action regarding this.