

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: Aharon

Last Name: Weidner

Mailing Address: 4937 Royal Palm Drive

City: Estero

Country: United States

State or Province: FL

ZIP/Postal Code: 33928

Email Address: aharonwe@excite.com

Organization Name: Mr.

Comment: I don't see why the FCC needs to intervene on behalf of big tech companies to prevent me from using the hardware that I purchase for legal purposes. If I want to improve my own security this measure restricts my ability. If you support this measure it is obvious that you have been bribed. Bribery is illegal. I hope that you understand the consequences of committing illegal activities if you actually support this. The hardware itself (in any case i would use) prevents interference before the software has control. If you believe that it is a problem to install your own firmware on hardware you purchased than you must believe that you shouldn't install any after market part on anything ever. Please understand what this actually is. I hope that you actually listen to your voters.

I don't see why the FCC needs to intervene on behalf of big tech companies to prevent me from using the hardware that I purchase for legal purposes. If I want to improve my own security this measure restricts my ability. If you support this measure it is obvious that you have been bribed. Bribery is illegal. I hope that you understand the consequences of committing illegal activities if you actually support this. The hardware itself (in any case i would use) prevents interference before the software has control. If you believe that it is a problem to install your own firmware on hardware you purchased than you must believe that you shouldn't install any after market part on anything ever. Please understand what this actually is. I hope that you actually listen to your voters.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Pigott

Mailing Address: 2026 E Tecoma Rd

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85048

Email Address: jpscion2011@gmail.com

Organization Name: Self

Comment: I oppose the FCC's efforts to prohibit modification of my WiFi products and appliances. I install open source firmware such as DD-WRT on my routers. This does not let me bypass FCC restrictions (such as power output or channels), but removes manufacturer bugs, adds important features to improve the security of my network and enhances stability and performance of my router.

I oppose the FCC's efforts to prohibit modification of my WiFi products and appliances. I install open source firmware such as DD-WRT on my routers. This does not let me bypass FCC restrictions (such as power output or channels), but removes manufacturer bugs, adds important features to improve the security of my network and enhances stability and performance of my router.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Cotton

Mailing Address: 18831 20th Ave SE

City: Bothell

Country: United States

State or Province: WA

ZIP/Postal Code: 98012

Email Address: jasoncot@gmail.com

Organization Name:

Comment: To whom it may concern,

I would like to request that FCC not take away the ability for users to install software of their choosing on their computing devices, including those that are integrated with wireless hardware.

It is worth noting that researchers of wireless networking and technologies depend on the ability to investigate and modify their equipment. Limiting the ability to patch or fix security holes means there are fewer options available to users to take action when it comes to digital security. Also, users have been able to fix serious bugs in wireless drivers which would be banned under NRPM.

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

I believe that any limitations added to hardware, such as what is proposed under the NRPM means stifling innovation from researchers and those who choose to support hardware in the after-market economy; as seen in the wireless-g router market. I do not support the proposal and hope that users will retain the ability of installing the software of their choosing without breaking laws.

Thank you for your time.

To whom it may concern,

I would like to request that FCC not take away the ability for users to install software of their choosing on their computing devices, including those that are integrated with wireless hardware.

It is worth noting that researchers of wireless networking and technologies depend on the ability to investigate and modify their equipment. Limiting the ability to patch or fix security holes means there are fewer options available to users to take action when it comes to digital security. Also, users have been able to fix serious bugs in wireless drivers which would be banned under NRPM.

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

I believe that any limitations added to hardware, such as what is proposed under the NRPM means stifling innovation

from researchers and those who choose to support hardware in the after-market economy; as seen in the wireless-g router market. I do not support the proposal and hope that users will retain the ability of installing the software of their choosing without breaking laws.

Thank you 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: Darius

Last Name: Dauer

Mailing Address: 2728 Old Sugar Road

City: Durham

Country: United States

State or Province: NC

ZIP/Postal Code: 27707

Email Address: darius@axiomtechnical.com

Organization Name:

Comment: Please don't disallow my from modifying the equipment I purchase outright.

Part of my job as a network administrator is to foresee security issues with the technology I implement and as a course of business, one method of implementing security is to have have good passwords and encryption. The other method is through obscurity.

It's much more difficult to break into a system that you know nothing about.

When I build a network, I sometimes replace the software or firmware that comes with the hardware that I buy. I install non-standard firmware on some of my devices because I know the stock configuration has security issues or is missing some security features I need.

For Example: In 2014 a security bug in OpenSSL called Heartbleed was found that effected many websites, routers, VPNs and other IT systems. I found in the logs of my equipment that someone was attempting to use that bug to break into one of my systems but they were unsuccessful simply because I had changed the firmware on my devices to something the would-be hackers didn't expect.

I need to be able to interact with the hardware I buy at a low level to do my job. Any legislation that prevents me from doing that effectively makes the internet inherently less safe simply because once a hacker finds a bug, there are so many more standardized devices that it can be exploited on.

Please don't disallow my from modifying the equipment I purchase outright.

Part of my job as a network administrator is to foresee security issues with the technology I implement and as a course of business, one method of implementing security is to have have good passwords and encryption. The other method is through obscurity.

It's much more difficult to break into a system that you know nothing about.

When I build a network, I sometimes replace the software or firmware that comes with the hardware that I buy. I install non-standard firmware on some of my devices because I know the stock configuration has security issues or is missing some security features I need.

For Example: In 2014 a security bug in OpenSSL called Heartbleed was found that effected many websites, routers,

VPNs and other IT systems. I found in the logs of my equipment that someone was attempting to use that bug to break into one of my systems but they were unsuccessful simply because I had changed the firmware on my devices to something the would-be hackers didn't expect.

I need to be able to interact with the hardware I buy at a low level to do my job. Any legislation that prevents me from doing that effectively makes the internet inherently less safe simply because once a hacker finds a bug, there are so many more standardized devices that it can be exploited on.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: Bonte

Mailing Address: 1176 Bartlein Ct.

City: Menasha

Country: United States

State or Province: WI

ZIP/Postal Code: 54952

Email Address: jon_bonte@yahoo.com

Organization Name:

Comment: To whom it may concern,

As Computer Engineer employed in the electronics industry, I do not agree with the FCCs decision to prevent consumers from upgrading firmware on network equipment. Upgraded firmware gives many users increased security and reliability. Furthermore it allows enthusiasts to prototype new devices and test new designs. This could have a huge impact to the recent innovation we are seeing with more and more household electronic devices now connecting to the internet. Furthermore, such changes interfere with consumer rights to use purchased goods in a way that works for them. I actually believe this change will have a negative effect on RF interference as well because it will prevent consumers from tuning their product to work with their setup and force them to instead buy more wifi transmitters or repeaters and to look to higher power devices.

Thank you,

Jonathan M. Bonte

To whom it may concern,

As Computer Engineer employed in the electronics industry, I do not agree with the FCCs decision to prevent consumers from upgrading firmware on network equipment. Upgraded firmware gives many users increased security and reliability. Furthermore it allows enthusiasts to prototype new devices and test new designs. This could have a huge impact to the recent innovation we are seeing with more and more household electronic devices now connecting to the internet. Furthermore, such changes interfere with consumer rights to use purchased goods in a way that works for them. I actually believe this change will have a negative effect on RF interference as well because it will prevent consumers from tuning their product to work with their setup and force them to instead buy more wifi transmitters or repeaters and to look to higher power devices.

Thank you,

Jonathan M. Bonte

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: Keith

Last Name: Reynolds

Mailing Address: 19232 SE 43rd Street

City: Issaquah

Country: United States

State or Province: WA

ZIP/Postal Code: 98027

Email Address:

Organization Name:

Comment: Please do not implement any rules that prevent users from installing their own choice of software on their network or computing devices. It is critical that users be allowed to fix security holes that vendors choose not to, which is all too common.

Please do not implement any rules that prevent users from installing their own choice of software on their network or computing devices. It is critical that users be allowed to fix security holes that vendors choose not to, which is all too common.

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: Douglas

Last Name: Perkins

Mailing Address: 1112 Cottonwood St

City: Grand Forks

Country: United States

State or Province: ND

ZIP/Postal Code: 58201

Email Address: contact@dperkins.org

Organization Name: null

Comment: Please do not make laws or rules keeping us from playing with WiFi devices. There are many reasons. First, we payed for them, so you should not be telling us what to do with them. Second, security demands openness. Independent and third-party security researchers must be able to modify a device if they are to find weaknesses that need fixing. People in other countries will do this regardless of what people in the U.S. do, so at best we're throwing in the towel on security if we lock down modifications. Third, innovation is built on modification. So much of what we do with technology is taking yesterday's technology and using it in an unexpected way. You can't do that if the law prevents it. Let us decide how to use our devices. Government restrictions can only lead to badness.

Please do not make laws or rules keeping us from playing with WiFi devices. There are many reasons. First, we payed for them, so you should not be telling us what to do with them. Second, security demands openness. Independent and third-party security researchers must be able to modify a device if they are to find weaknesses that need fixing. People in other countries will do this regardless of what people in the U.S. do, so at best we're throwing in the towel on security if we lock down modifications. Third, innovation is built on modification. So much of what we do with technology is taking yesterday's technology and using it in an unexpected way. You can't do that if the law prevents it. Let us decide how to use our devices. Government restrictions can only lead to badness.

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: Marc

Last Name: Teale

Mailing Address: 3414 40th Ave SW

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98116

Email Address: marc.teale@gmail.com

Organization Name:

Comment: Implementing this rule would be a terrible mistake. It would ensure that devices purchased by users can never be improved by anyone other than the original manufacturer. Vibrant user communities like DD-WRT, OpenWRT, and Tomato would all immediately become illegal. It would destroy the ability of owners to fully utilize and *own* the products that they have purchased.

Please do not pass this. It would make me and thousands of other ordinary users into criminals simply because we want to tinker with devices that we already own.

Implementing this rule would be a terrible mistake. It would ensure that devices purchased by users can never be improved by anyone other than the original manufacturer. Vibrant user communities like DD-WRT, OpenWRT, and Tomato would all immediately become illegal. It would destroy the ability of owners to fully utilize and *own* the products that they have purchased.

Please do not pass this. It would make me and thousands of other ordinary users into criminals simply because we want to tinker with devices that we already own.

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: Izurieta

Mailing Address: 353 Washington Avenue

City: Brooklyn

Country: United States

State or Province: NY

ZIP/Postal Code: 11238

Email Address: jamesalejandro@gmail.com

Organization Name:

Comment: It is unacceptable to remove the option for people to manage the software that manages the radio equipment they own, and has already been certified as hardware to conform to existing FCC regulations. You created this problem by being sloppy in your certification process, and certifying equipment that does not actually conform to FCC regs as hardware but can be artificially governed through a specific software implementation. People have the right to do with the hardware what they will provided they do not materially alter the hardware to exceed regulations. Updating firmware to better extract value from their own possessions is in the best interest of everyone. You need to take this issue you have to the people that caused this in the first place by not actually building conforming hardware - the manufacturers. Just because it's cheaper for them to build one device model and restrict functionality in an artificial way does not mean the consumer should suffer. Either there is something worth reviewing about your existing compliance requirements to make them less restrictive, or you need to uphold the intent of your remit and place the burden where it belongs - on the manufacturers.

It is unacceptable to remove the option for people to manage the software that manages the radio equipment they own, and has already been certified as hardware to conform to existing FCC regulations. You created this problem by being sloppy in your certification process, and certifying equipment that does not actually conform to FCC regs as hardware but can be artificially governed through a specific software implementation. People have the right to do with the hardware what they will provided they do not materially alter the hardware to exceed regulations. Updating firmware to better extract value from their own possessions is in the best interest of everyone. You need to take this issue you have to the people that caused this in the first place by not actually building conforming hardware - the manufacturers. Just because it's cheaper for them to build one device model and restrict functionality in an artificial way does not mean the consumer should suffer. Either there is something worth reviewing about your existing compliance requirements to make them less restrictive, or you need to uphold the intent of your remit and place the burden where it belongs - on the manufacturers.

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: Robert

Last Name: Adams

Mailing Address: 218 W Market St

City: Warrensburg

Country: United States

State or Province: MO

ZIP/Postal Code: 64093-1630

Email Address: radams45@charter.net

Organization Name:

Comment: As a user of a router that I installed different firmware on to take advantage of the benefits of said firmware (benefits that go way beyond the standard firmware by the original manufacturer) I believe your new rules will jeopardize my ability to put different firmware on any future router I may purchase. I should not be limited to ONLY what the manufacturer can provide in the way of firmware, if other firmware can be created then I should be able to reap the benefits of it. Do not implement rules to curtail my use of open firmware on my home router. Do not.

As a user of a router that I installed different firmware on to take advantage of the benefits of said firmware (benefits that go way beyond the standard firmware by the original manufacturer) I believe your new rules will jeopardize my ability to put different firmware on any future router I may purchase. I should not be limited to ONLY what the manufacturer can provide in the way of firmware, if other firmware can be created then I should be able to reap the benefits of it. Do not implement rules to curtail my use of open firmware on my home router. Do not.

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: Philip

Last Name: Lee

Mailing Address: 4700 N Western Ave Apt 4C

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60625

Email Address:

Organization Name:

Comment: This proposal is bad.

The most secure firmware is open-source firmware, not locked-down proprietary firmware. Please support the open and free history of the internet and do not pass this.

This proposal is bad.

The most secure firmware is open-source firmware, not locked-down proprietary firmware. Please support the open and free history of the internet and do not pass this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: joshua

Last Name: silver

Mailing Address: 20060 peach tree lane

City: cupertino

Country: United States

State or Province: CA

ZIP/Postal Code: 95014

Email Address:

Organization Name:

Comment: Please strike the requirement to lock down 5GHz radios: "(10) Applications for certification of U-NII devices in the 5.15-5.35 GHz and the 5.47-5.85 GHz bands must include a high level operational description of the security procedures that control the radio frequency operating parameters and ensure that unauthorized modifications cannot be made."

As someone on the internet said better than me, "because of the economics of cheap routers, nearly every router is designed around a System on Chip a CPU and radio in a single package. Banning the modification of one inevitably bans the modification of the other, and eliminates the possibility of installing proven Open Source firmware on any device."

I've been running open source firmware on my router for years, because the default firmware that came with my device is figuratively shit. It's just awful. Upgrading to a device with better firmware would significantly increase the cost of the router, because many of the features I use are only available on enterprise-grade devices. I don't need enterprise-grade devices. I just need software that actually support all the features my hardware is capable of, instead of a badly made UI that hides all the advanced features because most consumers don't need them.

Please strike the requirement to lock down 5GHz radios: "(10) Applications for certification of U-NII devices in the 5.15-5.35 GHz and the 5.47-5.85 GHz bands must include a high level operational description of the security procedures that control the radio frequency operating parameters and ensure that unauthorized modifications cannot be made."

As someone on the internet said better than me, "because of the economics of cheap routers, nearly every router is designed around a System on Chip a CPU and radio in a single package. Banning the modification of one inevitably bans the modification of the other, and eliminates the possibility of installing proven Open Source firmware on any device."

I've been running open source firmware on my router for years, because the default firmware that came with my device is figuratively shit. It's just awful. Upgrading to a device with better firmware would significantly increase the cost of the router, because many of the features I use are only available on enterprise-grade devices. I don't need enterprise-grade devices. I just need software that actually support all the features my hardware is capable of, instead of a badly made UI that hides all the advanced features because most consumers don't need them.

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: Rico

Last Name: Giove

Mailing Address: 1 main stree

City: Dallas

Country: United States

State or Province: TX

ZIP/Postal Code: 75226

Email Address: null

Organization Name: U. S, Taspayer

Comment: Not only are the proposed rules and the existing rules will make our wifi routers worthless and probably putting thousands of people out of jobs.

Software firmware for routers from vendors is always out of date leaving individuals defenseless against wifi hacks. That is why there is third party software/firmware for routers and other third party devices. is being developed. If we can not keep our equipment updated. **THEY ARE WORTHLESS.** This will kill wifi use. Is that what you want?????

Ham radio operators will be also affected also and thereby crippling helping people in emergency situations. So if anyone dies because of the rules, their blood will be on your hands,

Not only are the proposed rules and the existing rules will make our wifi routers worthless and probably putting thousands of people out of jobs.

Software firmware for routers from vendors is always out of date leaving individuals defenseless against wifi hacks. That is why there is third party software/firmware for routers and other third party devices. is being developed. If we can not keep our equipment updated. **THEY ARE WORTHLESS.** This will kill wifi use. Is that what you want?????

Ham radio operators will be also affected also and thereby crippling helping people in emergency situations. So if anyone dies because of the rules, their blood will be on your hands,

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Kleinberg

Mailing Address: 515 NW 4th Street

City: Gainesville

Country: United States

State or Province: FL

ZIP/Postal Code: 32601

Email Address: ustice@gmail.com

Organization Name:

Comment: Please do not enact the rule that will take away my ability to install software on my devices that use wifi. In college, when I was poor, I was able to repurpose my wifi router to do several roles, including create a VPN so that I could access my files at home. This saved me more than once. Without the ability to install a third-party open source firmware, I simply wouldn't have been able to afford that feature.

As a software developer, this would now prevent me from being able to experiment and create better products in the future. I make it a habit to fix problems when I fix problems in open source software, and these rules would prevent me from doing that.

Listen to the EFF. This is a BAD move. This will hurt people and businesses, while simply protecting entrenched ones.

If you're worried about hackers like me causing interference, this is not going to work. Apple has been locking down the iPhone since it has been a product, and it's been jailbroken almost that entire time. (I'm typing this on a jailbroken device right now). We will find ways around the restrictions. This will NOT accomplish your goals.

Don't hurt open source software. Don't hurt businesses. Don't hurt college students who just want print out their homework. Don't enact these rules. Please.

Please do not enact the rule that will take away my ability to install software on my devices that use wifi. In college, when I was poor, I was able to repurpose my wifi router to do several roles, including create a VPN so that I could access my files at home. This saved me more than once. Without the ability to install a third-party open source firmware, I simply wouldn't have been able to afford that feature.

As a software developer, this would now prevent me from being able to experiment and create better products in the future. I make it a habit to fix problems when I fix problems in open source software, and these rules would prevent me from doing that.

Listen to the EFF. This is a BAD move. This will hurt people and businesses, while simply protecting entrenched ones.

If you're worried about hackers like me causing interference, this is not going to work. Apple has been locking down the iPhone since it has been a product, and it's been jailbroken almost that entire time. (I'm typing this on a jailbroken device right now). We will find ways around the restrictions. This will NOT accomplish your goals.

Don't hurt open source software. Don't hurt businesses. Don't hurt college students who just want print out their

homework. Don't enact these rules. 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: Sarah

Last Name: Rento

Mailing Address: 201 w Lakeview Ave

City: Columbus

Country: United States

State or Province: OH

ZIP/Postal Code: 43202

Email Address:

Organization Name:

Comment: I ask that you do not restrict wireless devices that I own.

I ask that you do not restrict wireless devices that I own.

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: Cheryl

Last Name: Jones

Mailing Address: 5801 Ashley Drive

City: Gardendale

Country: United States

State or Province: AL

ZIP/Postal Code: 35071

Email Address: chjones50@hotmail.com

Organization Name:

Comment: I oppose this regulation. If allowed, the FCC will make it illegal to flash the firmware on all routers in the US for the sake of "Security". This will greatly stifle innovation. We need to stimulate open source projects wherever possible!

I oppose this regulation. If allowed, the FCC will make it illegal to flash the firmware on all routers in the US for the sake of "Security". This will greatly stifle innovation. We need to stimulate open source projects wherever possible!

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: Robinson

Mailing Address: po box 234

City: LaGrange

Country: United States

State or Province: WY

ZIP/Postal Code: 82221

Email Address:

Organization Name:

Comment: I will not comply.

I will not comply.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Davidson

Mailing Address: 219 Grindstone Drive

City: Apex

Country: United States

State or Province: NC

ZIP/Postal Code: 27502

Email Address: smokes2345@gmail.com

Organization Name:

Comment: Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users

replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ian

Last Name: Davis

Mailing Address: 47674 Bannon Court

City: Fremont

Country: United States

State or Province: CA

ZIP/Postal Code: 94539

Email Address: gov@dogsbodynet.com

Organization Name: null

Comment:

I respectfully request rules NOT take away the ability of users to install software of their choice on their computing devices.

Wireless routers are often field upgraded, and because of the low-cost nature of their design the radio & compute functions are handled by a single piece of silicon.

Significant points of concern:

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

Thank you for your consideration.

-- Ian Davis

I respectfully request rules NOT take away the ability of users to install software of their choice on their computing devices.

Wireless routers are often field upgraded, and because of the low-cost nature of their design the radio & compute functions are handled by a single piece of silicon.

Significant points of concern:

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

2) Americans need the ability to fix security holes in their devices when the manufacturer abandon them or chooses to not do so.

3) Myself and others have in the past fixed serious bugs in their wifi drivers, all of which would be banned under the NPRM.

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

Thank you for your consideration.

-- Ian Davis

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: Kurt

Last Name: Gillespie

Mailing Address: 1409 Mayapple St

City: Pflugerville

Country: United States

State or Province: TX

ZIP/Postal Code: 78660

Email Address:

Organization Name:

Comment: Technically speaking, this is a backwards way to securing a device. 3rd party work through independent people and groups, through creative work and experimentation, help to move the industry forward where big corporations fail to experiment. Custom firmware is like a Kickstarter campaign, driving ideas and products to areas that big companies are afraid or too slow to achieve. Custom firmware on wifi routers is important to protect, not restrict.

Technically speaking, this is a backwards way to securing a device. 3rd party work through independent people and groups, through creative work and experimentation, help to move the industry forward where big corporations fail to experiment. Custom firmware is like a Kickstarter campaign, driving ideas and products to areas that big companies are afraid or too slow to achieve. Custom firmware on wifi routers is important to protect, not restrict.

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: Byron

Last Name: Guernsey

Mailing Address: 6713 Heritage Lane

City: Charlestown

Country: United States

State or Province: IN

ZIP/Postal Code: 47111

Email Address: bguernsey@me.com

Organization Name: None

Comment: I run DD-WRT on all of my home routers. the firmware is much better than the one that comes by default on many wi-fi routers and offers a higher level of security. The rule would make that impossible on future routers.

I also write software for arduinos, small embedded devices designed for building your own Internet of Things devices, and utilize various radios in the unlicensed spectrum to make my own networks. Presumably this would be impossible too if this rule was passed.

Please do not pass any rule which restricts a device from running a custom firmware.

I run DD-WRT on all of my home routers. the firmware is much better than the one that comes by default on many wi-fi routers and offers a higher level of security. The rule would make that impossible on future routers.

I also write software for arduinos, small embedded devices designed for building your own Internet of Things devices, and utilize various radios in the unlicensed spectrum to make my own networks. Presumably this would be impossible too if this rule was passed.

Please do not pass any rule which restricts a device from running a custom firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Daniel

Last Name: Eads

Mailing Address: 509 Linden Ave

City: Jackson

Country: United States

State or Province: MI

ZIP/Postal Code: 49203

Email Address:

Organization Name:

Comment: Allowing third-party firmware is the best way to ensure consumers have control over the hardware they have purchased. Open source firmware like OpenWRT is crucial to ensure networks are safe, secure, and follow FCC guidelines. Since hardware manufacturers put so little resources into creating their own safe and secure firmware, it is imperative that you continue to allow consumers to have the freedom and capability to administer their own hardware.

Allowing third-party firmware is the best way to ensure consumers have control over the hardware they have purchased. Open source firmware like OpenWRT is crucial to ensure networks are safe, secure, and follow FCC guidelines. Since hardware manufacturers put so little resources into creating their own safe and secure firmware, it is imperative that you continue to allow consumers to have the freedom and capability to administer their own hardware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Peter

Last Name: Burkimsher

Mailing Address: UCSB

City: Goleta

Country: United States

State or Province: CA

ZIP/Postal Code: 93117

Email Address:

Organization Name:

Comment: Dear FCC,

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.

Consumers 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.

See the iOS jailbreaking law:

Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works

The iPhone can act as a Personal Hotspot router, and allows alternative software to be installed. Ratifying your new proposal would lead to a contradictory legal status for jailbreaking.

Dear FCC,

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.

Consumers 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.

See the iOS jailbreaking law:

Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works

The iPhone can act as a Personal Hotspot router, and allows alternative software to be installed. Ratifying your new proposal would lead to a contradictory legal status for jailbreaking.

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: Sparklin

Mailing Address: 288 Yale Street

City: North Wilkesboro

Country: United States

State or Province: NC

ZIP/Postal Code: 28659

Email Address:

Organization Name:

Comment: I'll spare both of us the long-winded response. But I can't stress enough how disappointed I am that some of the provisions in this update are even under consideration.

That said, the most troubling is the proposed restrictions regarding the flashing/updating of WiFi hardware. Routers in particular are fraught with vulnerabilities, many of which are only found after a product is delivered to the end user.

Open source firmware helps to mitigate that, allowing end users to tailor their equipment to fit both their security and performance needs, both in the present and into the future. Often, these needs have been filled by individuals or third parties, not the manufacturers themselves.

Respectfully,
WS

I'll spare both of us the long-winded response. But I can't stress enough how disappointed I am that some of the provisions in this update are even under consideration.

That said, the most troubling is the proposed restrictions regarding the flashing/updating of WiFi hardware. Routers in particular are fraught with vulnerabilities, many of which are only found after a product is delivered to the end user.

Open source firmware helps to mitigate that, allowing end users to tailor their equipment to fit both their security and performance needs, both in the present and into the future. Often, these needs have been filled by individuals or third parties, not the manufacturers themselves.

Respectfully,
WS

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: Jack

Last Name: Ass

Mailing Address: nigger@niggers.com

City: You

Country: United States

State or Province: DE

ZIP/Postal Code: 311341

Email Address: null

Organization Name: null

Comment: Fuck You

Fuck 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: Jonathan

Last Name: Arndt

Mailing Address: 12 Pittsburg Hill Road

City: Conestoga

Country: United States

State or Province: PA

ZIP/Postal Code: 17516

Email Address: jdarndt@gmail.com

Organization Name:

Comment: Based on 10 years of professional experience in programming and system design, the proposed rule causes significant concern for information security and network infrastructure.

(The legitimate goals of the FCC could be achieved in an alternate manner such as the following: requiring that output power levels and any other critical parameters be limited to legal levels by a separate chip. This approach would be far superior to effectively banning proper security practice and updates for the ENTIRE firmware and any utilities on the device, as the current proposal does.)

The proposed rule which requires that manufacturers disallow firmware updates (other than signed manufacturer updates, typically provided for only a very short time), makes it much more difficult to prevent incidents such as the Target breach. In both cases, the victim companies were initially targeted because insecure WiFi devices were in use. To reduce future occurrences of such breaches, it is imperative to be able to update devices which use wireless networking. Especially when a vulnerability such as Shellshock is discovered, it is imperative that risks be mitigated immediately.

Updates provided by the manufacturer may at first seem to be a possible solution, but are not actually a viable solution for two reasons. Manufacturers generally do not provide long-term updates, updates for devices more than about one-two years old. In many cases, no updates are offered at all to handle issues after the date of sale. It is not reasonable to anticipate that organizations and families will replace their network gear every year or two - firmware updates are needed, including for devices which are a few years old: ESPECIALLY for devices which are a few years old.

Secondly, updates from the manufacturer are not a viable solution for more sensitive government and private organizations due to the response time required. In the first 24 hours after the release of Shellshock, thousands of systems were compromised. For many networks, it is critically important to mitigate the threat during this initial time frame. Manufacturer full updates were not available for several days to several months, as we first discussed the best long term solution and that solution propagated downstream from the authors, to the subsystem maintainers, distribution maintainers, OEM re-packagers, and finally out to customers after testing at each level. In the meantime, temporary MITIGATIONS were performed on-site by network engineers and security contractors. These vital mitigations which protected sensitive networks in the interim would be illegal and prevented by manufacturer locks under the proposed rule. In simple terms, the proposal makes it illegal to manufacturer equipment which can be quickly protected against new threats to our cyber security.

Another reason that the proposed rule is problematic is that the manufacturer default firmware, with all available features designed to be as easily accessible as possible, is not appropriate for any environment in which security is a concern. A central tenet of information security, and security in general, is that the attack surface should be as small as

possible - services not needed for a particular installation should not be installed and enabled. The only software which definitely cannot be exploited is software which is not installed or not enabled. Therefore, the most secure firmware tends to be that with as many features _removed_ as possible, with only those items required for the current role installed.

Manufacturer firmware does the exact opposite, for ease-of-use by ordinary consumers. All services which might be of use to any customer are installed, enabled, and wide open for use (and possibly abuse). In some devices, these features cannot be disabled using the manufacturer supplied firmware. Firmware must be able to be customized and trimmed down to provide only the required functions (and therefore the smallest attack surface). Again, it is possible for all of this upgrade-able firmware to be modified without affecting any of the critical RF parameters that are under FCC control.

Overall, the proposed rule is creates significant security problems in a number of ways. All of these issues could be avoided, and the radio emission still controlled, by instead requiring that radio output power or other essential RF parameters be limited by a chip separate from the (upgrade-able) main system, which includes all of the feature code, user interface, etc.

Based on 10 years of professional experience in programming and system design, the proposed rule causes significant concern for information security and network infrastructure.

(The legitimate goals of the FCC could be achieved in an alternate manner such as the following: requiring that output power levels and any other critical parameters be limited to legal levels by a separate chip. This approach would be far superior to effectively banning proper security practice and updates for the ENTIRE firmware and any utilities on the device, as the current proposal does.)

The proposed rule which requires that manufacturers disallow firmware updates (other than signed manufacturer updates, typically provided for only a very short time), makes it much more difficult to prevent incidents such as the Target breach. In both cases, the victim companies were initially targeted because insecure WiFi devices were in use. To reduce future occurrences of such breaches, it is imperative to be able to update devices which use wireless networking. Especially when a vulnerability such as Shellshock is discovered, it is imperative that risks be mitigated immediately.

Updates provided by the manufacturer may at first seem to be a possible solution, but are not actually a viable solution for two reasons. Manufacturers generally do not provide long-term updates, updates for devices more than about one-two years old. In many cases, no updates are offered at all to handle issues after the date of sale. It is not reasonable to anticipate that organizations and families will replace their network gear every year or two - firmware updates are needed, including for devices which are a few years old: **ESPECIALLY** for devices which are a few years old.

Secondly, updates from the manufacturer are not a viable solution for more sensitive government and private organizations due to the response time required. In the first 24 hours after the release of Shellshock, thousands of systems were compromised. For many networks, it is critically important to mitigate the threat during this initial time frame. Manufacturer full updates were not available for several days to several months, as we first discussed the best long term solution and that solution propagated downstream from the authors, to the subsystem maintainers, distribution maintainers, OEM re-packagers, and finally out to customers after testing at each level. In the meantime, temporary **MITIGATIONS** were performed on-site by network engineers and security contractors. These vital mitigations which protected sensitive networks in the interim would be illegal and prevented by manufacturer locks under the proposed rule. In simple terms, the proposal makes it illegal to manufacturer equipment which can be _quickly_ protected against new threats to our cyber security.

Another reason that the proposed rule is problematic is that the manufacturer default firmware, with all available features designed to be as easily accessible as possible, is not appropriate for any environment in which security is a concern. A central tenet of information security, and security in general, is that the attack surface should be as small as possible - services not needed for a particular installation should not be installed and enabled. The only software which definitely cannot be exploited is software which is not installed or not enabled. Therefore, the most secure firmware tends to be that with as many features _removed_ as possible, with only those items required for the current role

installed.

Manufacturer firmware does the exact opposite, for ease-of-use by ordinary consumers. All services which might be of use to any customer are installed, enabled, and wide open for use (and possibly abuse). In some devices, these features cannot be disabled using the manufacturer supplied firmware. Firmware must be able to be customized and trimmed down to provide only the required functions (and therefore the smallest attack surface). Again, it is possible for all of this upgrade-able firmware to be modified without affecting any of the critical RF parameters that are under FCC control.

Overall, the proposed rule is creates significant security problems in a number of ways. All of these issues could be avoided, and the radio emission still controlled, by instead requiring that radio output power or other essential RF parameters be limited by a chip separate from the (upgrade-able) main system, which includes all of the feature code, user interface, etc.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Elstein

Mailing Address: 4481 Maryland Ave

City: Saint Louis

Country: United States

State or Province: MO

ZIP/Postal Code: 63108

Email Address: aelstein3@gmail.com

Organization Name:

Comment: Please do not enact rules that ban individuals from installing software of their choice on the hardware they personally own.

In order to further research wireless networking capabilities, individuals need too be able to investigate, edit and install new software/firmware onto their devices.

When a manufacturer doesn't fix security issues in a timely manner, people need to be allowed to do so themselves.

In the past, individuals have successfully fixed critical bugs in their wifi drivers, illegal under the NPRM.

A large sector of the internet economy (i.e. vendors of retail hotspots and secure wifi) depend on the fundamental right of users to install software they wish to install.

I hope the FCC reconsiders these rules as they risk seriously harming consumers of wireless technologies, which most Americans do.

Thanks,

Andrew

Please do not enact rules that ban individuals from installing software of their choice on the hardware they personally own.

In order to further research wireless networking capabilities, individuals need too be able to investigate, edit and install new software/firmware onto their devices.

When a manufacturer doesn't fix security issues in a timely manner, people need to be allowed to do so themselves.

In the past, individuals have successfully fixed critical bugs in their wifi drivers, illegal under the NPRM.

A large sector of the internet economy (i.e. vendors of retail hotspots and secure wifi) depend on the fundamental right of users to install software they wish to install.

I hope the FCC reconsiders these rules as they risk seriously harming consumers of wireless technologies, which most

Americans do.

Thanks,

Andrew

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Charles

Last Name: Phillips

Mailing Address: 5577 13th Avenue South

City: Birmingham

Country: United States

State or Province: AL

ZIP/Postal Code: 35222

Email Address:

Organization Name:

Comment: Preventing open source software from being flashed to routers will make innovation much more difficult. Allowing the people to control their own hardware is an advantage for everyone, including security firms. Please do not allow this stifling action to take place!

Preventing open source software from being flashed to routers will make innovation much more difficult. Allowing the people to control their own hardware is an advantage for everyone, including security firms. Please do not allow this stifling action to take place!

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: Ralph

Last Name: Phillips

Mailing Address: 4716 Bruce Street

City: Bossier City

Country: United States

State or Province: LA

ZIP/Postal Code: 71111

Email Address: ralphp@philent.biz

Organization Name: Phillips Enterprises

Comment: I do not think this is a good rule.

There are too many places that a generic router/AP (such as the LinkSys WRT series) combined with custom firmware makes a much more reliable package.

Also, almost none of the consumer grade routers will do for some of the usages I have put them to over the years with the factory one-size-fits-all(-poorly) base firmwares. This is like saying that we have to eat at McDonald's, because we cannot prepare beef the way we want.

I would highly recommend the FCC stay away from regulations like this one.

RwP

I do not think this is a good rule.

There are too many places that a generic router/AP (such as the LinkSys WRT series) combined with custom firmware makes a much more reliable package.

Also, almost none of the consumer grade routers will do for some of the usages I have put them to over the years with the factory one-size-fits-all(-poorly) base firmwares. This is like saying that we have to eat at McDonald's, because we cannot prepare beef the way we want.

I would highly recommend the FCC stay away from regulations like this one.

RwP

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Danielson

Mailing Address: 1340 Merced Street

City: Richmond

Country: United States

State or Province: CA

ZIP/Postal Code: 94804

Email Address:

Organization Name:

Comment: If I can't modify the none RF controlling software on a router, I'm vulnerable to all the zero-day exploits against the manufacturer's software package. Unless the FCC will make manufacturers responsible for any and all flaws in the frozen software, this proposed regulation is only going to cause me and my business economic harm.

If I can't modify the none RF controlling software on a router, I'm vulnerable to all the zero-day exploits against the manufacturer's software package. Unless the FCC will make manufacturers responsible for any and all flaws in the frozen software, this proposed regulation is only going to cause me and my business economic harm.

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: Kevin

Last Name: Hamann

Mailing Address: 245 W Homestead

City: Medina

Country: United States

State or Province: OH

ZIP/Postal Code: 44256

Email Address:

Organization Name:

Comment: These changes will prevent innovation from the thriving open source community for third party firmware for routers and other wireless electronic devices, which often have portions that are used by the companies for upgrades to the OEM firmware.

These changes also impair the ability to fix security holes in the firmware.

These changes will prevent innovation from the thriving open source community for third party firmware for routers and other wireless electronic devices, which often have portions that are used by the companies for upgrades to the OEM firmware.

These changes also impair the ability to fix security holes in the firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brad

Last Name: Mears

Mailing Address: 8902 Melbourne Dr

City: Colorado Springs

Country: United States

State or Province: CO

ZIP/Postal Code: 80920

Email Address: Brad.Mears@gmail.com

Organization Name:

Comment: As a professional software engineer and electronics hobbyist, I design, build and operate small autonomous vehicles. An important goal of this effort is to keep costs low by using re-purposed commercially available hardware.

This hardware is used to provide a live telemetry feed for remote operation of the vehicle. To date, this has been accomplished by loading after-market software like OpenWRT and DD-WRT on various routers. I am also experimenting with my own custom software for low-end 315 MHz and 433 MHz transmitters and receivers as well as for the ESP8266 WiFi chips that are now available.

The proposed regulation would cripple this research by preventing the use of hardware in ways that, while not relevant to most consumers, are extremely valuable to the engineering community in this country.

I urge you to reject the proposed regulation.

As a professional software engineer and electronics hobbyist, I design, build and operate small autonomous vehicles. An important goal of this effort is to keep costs low by using re-purposed commercially available hardware.

This hardware is used to provide a live telemetry feed for remote operation of the vehicle. To date, this has been accomplished by loading after-market software like OpenWRT and DD-WRT on various routers. I am also experimenting with my own custom software for low-end 315 MHz and 433 MHz transmitters and receivers as well as for the ESP8266 WiFi chips that are now available.

The proposed regulation would cripple this research by preventing the use of hardware in ways that, while not relevant to most consumers, are extremely valuable to the engineering community in this country.

I urge you to reject the proposed regulation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eric

Last Name: Turpin

Mailing Address: 117 Summer Brooke

City: Peachtree City

Country: United States

State or Province: GA

ZIP/Postal Code: 30269

Email Address:

Organization Name:

Comment: 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.

Stop trying to control things that you clearly do not have even the slightest understanding of.

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.

Stop trying to control things that you clearly do not have even the slightest understanding 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: E

Last Name: March

Mailing Address: 278 Melwood Drive

City: Rochester

Country: United States

State or Province: NY

ZIP/Postal Code: 14626

Email Address:

Organization Name: Individual

Comment: I have been employed as a Software Engineer for over 30 years. From my perspective, Internet communications to the home has been and should continue to be; one of the most dramatic areas of innovation.

The advent of inexpensive Linux based routers has been a great enabler of new technology driving the "Internet of Things", security and convenience. Much of this innovation is being done by individuals and small groups. This work is enabled by open and reconfigurable firmware.

Any legislation that prevents this work from being performed is something I would be opposed to. You may contact me by mail if you would like to further understand my position.

Thank you for listening.

I have been employed as a Software Engineer for over 30 years. From my perspective, Internet communications to the home has been and should continue to be; one of the most dramatic areas of innovation.

The advent of inexpensive Linux based routers has been a great enabler of new technology driving the "Internet of Things", security and convenience. Much of this innovation is being done by individuals and small groups. This work is enabled by open and reconfigurable firmware.

Any legislation that prevents this work from being performed is something I would be opposed to. You may contact me by mail if you would like to further understand my position.

Thank you for listening.

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: Mason

Last Name: Barland

Mailing Address: 6601 41st Av N

City: Crystal

Country: United States

State or Province: MN

ZIP/Postal Code: 55427

Email Address: Mbarland@hotmail.com

Organization Name:

Comment: Please do not restrict in any way m ability as a consumer to modify my own equipment through simple software hacks.

Please do not restrict in any way m ability as a consumer to modify my own equipment through simple software hacks.

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: Jedediah

Last Name: Daiger

Mailing Address: 11434 Sugarmaple Ln.

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32821

Email Address:

Organization Name:

Comment: I respectfully submit that the FCC should not implement rules that take away the ability of users to install the software of their choosing on their computing devices, including WiFi routers. As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities.[6] In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

[1] <http://www.linksys.com/us/wireless-routers/c/wrt-wireless-routers/#fullstory>

[2] <https://www.codeaurora.org/xwiki/bin/QSDK/WebHome>

[3] <http://www.cavium.com/newsevents-Cavium-Delivers-Optimized-OpenWRT-on-OCTEON-III.html>

[4] <http://www.doghunter.org/>

[5] <http://mediatek.com/en/news-events/mediatek-news/mediatek-launches-mt7628-industrys-first-80211n-2t2r-ap-soc-for-home-router-smart-router-and-iot-gateway/>

[6] <http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

I respectfully submit that the FCC should not implement rules that take away the ability of users to install the software of their choosing on their computing devices, including WiFi routers. As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities.[6] In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

[1] <http://www.linksys.com/us/wireless-routers/c/wrt-wireless-routers/#fullstory>

[2] <https://www.codeaurora.org/xwiki/bin/QSDK/WebHome>

[3] <http://www.cavium.com/newsevents-Cavium-Delivers-Optimized-OpenWRT-on-OCTEON-III.html>

[4] <http://www.doghunter.org/>

[5] <http://mediatek.com/en/news-events/mediatek-news/mediatek-launches-mt7628-industrys-first-80211n-2t2r-ap-soc-for-home-router-smart-router-and-iot-gateway/>

[6] <http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

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: Anton

Last Name: Chaykin

Mailing Address: 607662

City: Nizhny novgorod

Country: Russia

State or Province: Nizhegorodskaya oblast

ZIP/Postal Code: 607662

Email Address:

Organization Name:

Comment: I want live in free world, don't block free and better firmware

I want live in free world, don't block free and better firmware

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Strachan

Mailing Address: 2736 State Route 9

City: Lake George

Country: United States

State or Province: NY

ZIP/Postal Code: 12845

Email Address:

Organization Name: Citizen

Comment: Dear FCC,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices and more specifically consumer wireless equipment.

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.

In the recent past, I have had to install open source software on my wifi routers to close security holes. The equipment manufacturer had no interest or financial incentive to provide firmware updates to protect my network. If these rules pass, I envision having to buy dozens of new routers every time a security flaw is found in my systems or abandon wifi.

Your rules sound like they were written by equipment manufacturers who are are pursuing a agenda driven by corporate greed.

As a government entity, the FCC should be making the world a better place for the citizens of this country and not lining the pockets of corporations.

Dear FCC,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices and more specifically consumer wireless equipment.

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.

In the recent past, I have had to install open source software on my wifi routers to close security holes. The equipment manufacturer had no interest or financial incentive to provide firmware updates to protect my network. If these rules pass, I envision having to buy dozens of new routers every time a security flaw is found in my systems or abandon wifi.

Your rules sound like they were written by equipment manufacturers who are pursuing a agenda driven by corporate greed.

As a government entity, the FCC should be making the world a better place for the citizens of this country and not lining the pockets of corporations.

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: Jim

Last Name: Sandman

Mailing Address: 334 13th Avenue

City: Santa Cruz

Country: United States

State or Province: CA

ZIP/Postal Code: 95062

Email Address:

Organization Name:

Comment: I am against these proposed rules.

I am concerned that this would prevent me from updating the firmware in my router to fix security bugs.

For example, on 1 Sep 2015, the Department of Homeland Security in conjunction with CERT, issued this bulletin, <http://www.kb.cert.org/vuls/id/201168>, that outlined multiple security vulnerabilities in a router that I had investigated for possible purchase.

I live in earthquake country and am concerned about emergency communication infrastructure in the event of a major earthquake. Mesh wifi networks offer a promising solution to this problem. These rules would prevent adequate research and development of such networks.

I am against these proposed rules.

I am concerned that this would prevent me from updating the firmware in my router to fix security bugs.

For example, on 1 Sep 2015, the Department of Homeland Security in conjunction with CERT, issued this bulletin, <http://www.kb.cert.org/vuls/id/201168>, that outlined multiple security vulnerabilities in a router that I had investigated for possible purchase.

I live in earthquake country and am concerned about emergency communication infrastructure in the event of a major earthquake. Mesh wifi networks offer a promising solution to this problem. These rules would prevent adequate research and development of such networks.