

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Willy

Last Name: Len

Mailing Address: Lomas de Angelpolis, puebla blanca

City: San Andrs Cholula

Country: Mexico

State or Province: Puebla

ZIP/Postal Code: 72830

Email Address: willylr89@gmail.com

Organization Name: null

Comment: I don't think that this is a measure, that benefits the consumer, if we buy a device it should be ours, and not being unable to modify it if it's our choice, that's why I reject this rule.

I don't think that this is a measure, that benefits the consumer, if we buy a device it should be ours, and not being unable to modify it if it's our choice, that's why I reject this 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: Anonymous

Last Name: Anonymous

Mailing Address: Ferdinand

City: Constanta

Country: Romania

State or Province: Constanta

ZIP/Postal Code: 900709

Email Address: filipomg@gmail.com

Organization Name: null

Comment: We should be free to do what we want with our devices. I'm against this measure

We should be free to do what we want with our devices. I'm against this measure

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: Zachary

Last Name: Hundley

Mailing Address: 9413 Faircrest Dr

City: Dallas

Country: United States

State or Province: TX

ZIP/Postal Code: 75238

Email Address: Piggyzach@gmail.com

Organization Name: null

Comment: To pass this rule would greatly infringe upon the right for android users to install custom firmware on their phones. In other words, these people's hobby is messing around with their phones software. This activity does not harm phone manufacturers or carriers, and should be allowed in a free nation like the United States. I beg of you, Do not pass this rule, or you will disadvantage a generation of phone developers.

To pass this rule would greatly infringe upon the right for android users to install custom firmware on their phones. In other words, these people's hobby is messing around with their phones software. This activity does not harm phone manufacturers or carriers, and should be allowed in a free nation like the United States. I beg of you, Do not pass this rule, or you will disadvantage a generation of phone developers.

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: Thomas

Last Name: Howe

Mailing Address: 42 Woodside Road

City: Norwich

Country: United Kingdom

State or Province: England

ZIP/Postal Code: NR79RP

Email Address: Tho7masPenguin@gmail.com

Organization Name: null

Comment: The focus of new regulations (and abolition of current ones) needs to be on the freedom of citizens/consumers and innovators. Mesh-net technology, router sharing, and open-source firmware efforts are being attacked by companies driven by profit and governments focused on spying. The P2P network is the deserving successor of the internet, but these regulations could trap everyone in an increasingly commercial and restrictive internet.

Due to the need for secure technology, all restrictive software (including firmware) needs to be banned. Phones manufactured without a way for the user to determine exactly what software is running or a way to replace the software should be seen as an invasion of privacy. Manufacturers have been known to implement back-doors, and allowing them to include closed-source blobs only encourages them to commit false advertising by claiming to be secure. US technology is generally regarded as insecure, and a complete ban on closed-source/locked-down firmware would reverse this damage. Restricted routers are already a hindrance to mesh-net technology, which are slowing down technological breakthroughs equivalent to the internet by decades. ISPs rely on the suppression of this technology, and therefore for the sake of progress need to be forced to stop removing the freedom such progress relies on.

If a device on the market is controlled by a company (closed-source/otherwise restricted baseband firmware) rather than the consumer (freely modifiable firmware), the power is taken away from the consumer. Ordinary consumers would not abuse this power, and exceptional cases of consumers mis-using frequency bands aren't prevented by the current restrictions. Companies, on the other hand, currently use this power to extort consumers and to spy on them, with the potential for further abuse.

Introducing effective 'license plates' in wireless devices could harm hobbyist activities - it would be a lot harder for someone to build their own router. Third parties could demand information unique to a wireless device to ensure that a consumer is not misusing a service - for example, having only one account on an online game. This would lead to device-unique information being sold online in bulk, allowing companies and other governments to identify individuals, thus making them an easy target.

The focus of new regulations (and abolition of current ones) needs to be on the freedom of citizens/consumers and innovators. Mesh-net technology, router sharing, and open-source firmware efforts are being attacked by companies driven by profit and governments focused on spying. The P2P network is the deserving successor of the internet, but these regulations could trap everyone in an increasingly commercial and restrictive internet.

Due to the need for secure technology, all restrictive software (including firmware) needs to be banned. Phones manufactured without a way for the user to determine exactly what software is running or a way to replace the software

should be seen as an invasion of privacy. Manufacturers have been known to implement back-doors, and allowing them to include closed-source blobs only encourages them to commit false advertising by claiming to be secure. US technology is generally regarded as insecure, and a complete ban on closed-source/locked-down firmware would reverse this damage. Restricted routers are already a hindrance to mesh-net technology, which are slowing down technological breakthroughs equivalent to the internet by decades. ISPs rely on the suppression of this technology, and therefore for the sake of progress need to be forced to stop removing the freedom such progress relies on.

If a device on the market is controlled by a company (closed-source/otherwise restricted baseband firmware) rather than the consumer (freely modifiable firmware), the power is taken away from the consumer. Ordinary consumers would not abuse this power, and exceptional cases of consumers mis-using frequency bands aren't prevented by the current restrictions. Companies, on the other hand, currently use this power to extort consumers and to spy on them, with the potential for further abuse.

Introducing effective 'license plates' in wireless devices could harm hobbyist activities - it would be a lot harder for someone to build their own router. Third parties could demand information unique to a wireless device to ensure that a consumer is not misusing a service - for example, having only one account on an online game. This would lead to device-unique information being sold online in bulk, allowing companies and other governments to identify individuals, thus making them an easy target.

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: Bennett

Last Name: Meares

Mailing Address: 17 High Cotton Lane

City: Pawleys Island

Country: United States

State or Province: SC

ZIP/Postal Code: 29585

Email Address: bennett.meares@gmail.com

Organization Name: null

Comment: THIS IS A BAD IDEA. Everything from modding communities to startup businesses rely on modification of hardware, especially with a wireless radio! Not only will this government-imposed manufacturer requirement disrupt the economy, it will also discourage innovation and ultimately lead to China surpassing the United States.

THIS IS A BAD IDEA. Everything from modding communities to startup businesses rely on modification of hardware, especially with a wireless radio! Not only will this government-imposed manufacturer requirement disrupt the economy, it will also discourage innovation and ultimately lead to China surpassing the United States.

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: Vicini

Mailing Address: 1123 MARGARET PL

City: NEW ORLEANS

Country: United States

State or Province: LA

ZIP/Postal Code: 701304311

Email Address: patricksmanycompanies@gmail.com

Organization Name: null

Comment: This is a terrible idea. We need to stop giving power to corporations and start putting it in the hands of people, the true innovators.

This is a terrible idea. We need to stop giving power to corporations and start putting it in the hands of people, the true innovators.

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: Drogbar

Last Name: Troll

Mailing Address: 700 Carpenters Xing, Folcroft, PA 19032

City: Folcroft

Country: United States

State or Province: PA

ZIP/Postal Code: 19032-2008

Email Address: drogbartroll@mail.ru

Organization Name: null

Comment: I think that the restriction on flashing devices is the worst thing that can happen for enthusiasts around the world. Don't limit people!

I think that the restriction on flashing devices is the worst thing that can happen for enthusiasts around the world. Don't limit people!

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: Oleksii

Last Name: Khmara

Mailing Address: Lopaninskiy st., 5/3

City: Kharkiv

Country: Ukraine

State or Province: Kharkivs'ka

ZIP/Postal Code: 61002

Email Address: alex.khmara@gmail.com

Organization Name: null

Comment: As IT professional I must say that this is very problematic regulation from security point of view.

1) In almost all cases devices come with firmware that is later found vulnerable to exploits, and usually manufacturer stops issuing updates long before devices are no more in widespread use. And as firmware becomes more and more complicated this will be even bigger problem in future.

2) There were many occasions when backdoors were found in manufacturer's firmware.

Often there is easy solution for both problems - open source firmware with much longer support, much more transparent development process and easy to audit , like OpenWRT.

P.S. While I'm not US citizen nor I live in US this regulation will probably affect me too, as many others, because companies tend to cut costs selling unified equipment if possible.

As IT professional I must say that this is very problematic regulation from security point of view.

1) In almost all cases devices come with firmware that is later found vulnerable to exploits, and usually manufacturer stops issuing updates long before devices are no more in widespread use. And as firmware becomes more and more complicated this will be even bigger problem in future.

2) There were many occasions when backdoors were found in manufacturer's firmware.

Often there is easy solution for both problems - open source firmware with much longer support, much more transparent development process and easy to audit , like OpenWRT.

P.S. While I'm not US citizen nor I live in US this regulation will probably affect me too, as many others, because companies tend to cut costs selling unified equipment if 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: Kristoffer

Last Name: Ryhl-Johansen

Mailing Address: Ryttervnet 2

City: Lyng

Country: Denmark

State or Province: Hovedstaden

ZIP/Postal Code: 3540

Email Address: kristoffer@ryhl.dk

Organization Name: null

Comment: The proposed changes in this proposed rule limit users ability to install the software of their choosing on their computing devices. This has several large consequences such as making research in wireless networking impossible in USA, disallowing users from fixing 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.

While I don't live in USA, these large changes will still affect me. The changes will stop the large part of the open source and research communities located in USA from providing better software for us outside the US, and from creating new research and technologies allowing everyone in the world access to better wifi.

I will stress the point that this ruling ensures that any new research in wifi and radio technology certainly wont have been created in the USA.

The proposed changes in this proposed rule limit users ability to install the software of their choosing on their computing devices. This has several large consequences such as making research in wireless networking impossible in USA, disallowing users from fixing 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.

While I don't live in USA, these large changes will still affect me. The changes will stop the large part of the open source and research communities located in USA from providing better software for us outside the US, and from creating new research and technologies allowing everyone in the world access to better wifi.

I will stress the point that this ruling ensures that any new research in wifi and radio technology certainly wont have been created in the USA.

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: Bennett

Mailing Address: 401 Sandstone Drive

City: Carson

Country: United States

State or Province: NV

ZIP/Postal Code: 89706

Email Address: lighthadron@gmail.com

Organization Name: null

Comment: To whom it may concern:

This is concerning the proposed rule: "Equipment Authorization and Electronic Labeling for Wireless Devices", document citation - 80 FR 46900.

I respectfully request that the FCC not take away my right, as a consumer who has paid for an electronic device that uses RF signals to communicate - i.e. WiFi, to install software or firmware of my choosing onto a device that may be implementing a flawed encryption schema or somehow otherwise leaking my private financial data to unintended recipients. For example: If a company that sells a wireless router does not wish to respond to security concerns about their firmware, I want to retain the right to proactively protect my data by installing a secure, open source firmware on that device. These situations would be illegal for the home consumer to fix were this proposed rule passed.

This would have some negative financial repercussions for devices that are targeted to operate on the unlicensed bands. Many agile startups filling the "internet of things" market space would be stifled by the extra costs associated with compliance testing; the time to work with this proposed extra layer of bureaucracy to obtain labeling would also be detrimental to smaller companies that are attempting to bring a product to market.

To restate - Please do not pass this proposed rule. It will only hurt not only the average consumer, but businesses that wish to offer wireless services to customers, and companies that wish to manufacture products that utilize these unlicensed bands.

Sincerely,  
Christopher Bennett

To whom it may concern:

This is concerning the proposed rule: "Equipment Authorization and Electronic Labeling for Wireless Devices", document citation - 80 FR 46900.

I respectfully request that the FCC not take away my right, as a consumer who has paid for an electronic device that uses RF signals to communicate - i.e. WiFi, to install software or firmware of my choosing onto a device that may be implementing a flawed encryption schema or somehow otherwise leaking my private financial data to unintended recipients. For example: If a company that sells a wireless router does not wish to respond to security concerns about their firmware, I want to retain the right to proactively protect my data by installing a secure, open source firmware on that device. These situations would be illegal for the home consumer to fix were this proposed rule passed.

This would have some negative financial repercussions for devices that are targeted to operate on the unlicensed bands. Many agile startups filling the "internet of things" market space would be stifled by the extra costs associated with compliance testing; the time to work with this proposed extra layer of bureaucracy to obtain labeling would also be detrimental to smaller companies that are attempting to bring a product to market.

To restate - Please do not pass this proposed rule. It will only hurt not only the average consumer, but businesses

that wish to offer wireless services to customers, and companies that wish to manufacture products that utilize these unlicensed bands.

Sincerely,  
Christopher Bennett

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: Anon

Last Name: Anon

Mailing Address: Anon

City: Anon

Country: United States

State or Province: IA

ZIP/Postal Code: Anon

Email Address: Anon@anon.Anon

Organization Name: null

Comment: They should be doing the exact opposite. It should be illegal for OEMs and ISPs to lock down devices they sell to consumers. The fact that my phone's bootloader is locked, preventing me from updating my phone's OS with security patches, is asinine. The FCC should be suing and fining the companies that do this because it's entirely anti-consumer.

Not to mention having a phone come pre-loaded with bloatware that you can't remove that can cause battery life to decrease substantially, can cause security issues, among other things isn't fair to the consumer. If anything providing the consumer with the choice to start with a basic operating system on their phone without the bloatware should be encouraged.

They should be doing the exact opposite. It should be illegal for OEMs and ISPs to lock down devices they sell to consumers. The fact that my phone's bootloader is locked, preventing me from updating my phone's OS with security patches, is asinine. The FCC should be suing and fining the companies that do this because it's entirely anti-consumer.

Not to mention having a phone come pre-loaded with bloatware that you can't remove that can cause battery life to decrease substantially, can cause security issues, among other things isn't fair to the consumer. If anything providing the consumer with the choice to start with a basic operating system on their phone without the bloatware should be encouraged.

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: Dudley

Mailing Address: 274 Jackson Pines Road

City: Jackson

Country: United States

State or Province: NJ

ZIP/Postal Code: 08527

Email Address: wfdudley@gmail.com

Organization Name:

Comment: Router and phone firmware should always be replaceable.

It is important to be able to change the firmware of routers and cellphones because often the factory supplied firmware has major design flaws and bugs, and the manufacturer often does not supply bug fix releases of the code, especially for older devices (more than 1 year old).

For example, the OpenWRT firmware project is replacement open source firmware for most consumer routers and it is far superior to the stock firmware, plus since it is open source, it can be examined to make sure that there are no back doors in the code. Another example is the Cyanogenmod Android code for smart phones -- most smart phones don't get factory updates from the carriers when bugs are discovered, so people end up running vulnerable software on their phones.

If you insist on locking down the radio firmware, then you must also insist on a rule that says that the non-radio software must be user upgradable. Otherwise, all consumer routers will be stuck with the buggy software they were shipped with.

William Dudley Jr.

Retired computer programmer

Router and phone firmware should always be replaceable.

It is important to be able to change the firmware of routers and cellphones because often the factory supplied firmware has major design flaws and bugs, and the manufacturer often does not supply bug fix releases of the code, especially for older devices (more than 1 year old).

For example, the OpenWRT firmware project is replacement open source firmware for most consumer routers and it is far superior to the stock firmware, plus since it is open source, it can be examined to make sure that there are no back doors in the code. Another example is the Cyanogenmod Android code for smart phones -- most smart phones don't get factory updates from the carriers when bugs are discovered, so people end up running vulnerable software on their phones.

If you insist on locking down the radio firmware, then you must also insist on a rule that says that the non-radio software must be user upgradable. Otherwise, all consumer routers will be stuck with the buggy software they were

shipped with.

William Dudley Jr.  
Retired computer programmer

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: Richard

Last Name: Nielsen

Mailing Address: 1204 Westchester Ridge NE

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30329

Email Address:

Organization Name:

Comment: Please do not take away the ability of the individual to update their wireless devices. It's a necessity when manufacturers leave us in a lurch and don't keep their products secure or updated. It's bad enough with phones as it is, and wireless devices are in an even worse state depending on manufacturers to take care of us. With the up coming internet of things, this seems like it could have drastic side effects with many devices having wireless capabilities and vendor lock in. Who's to say what looks like a wireless router in the future if multiple devices are communicating with each other around the house acting like a mesh network. Taking away after market choice is a terrible idea!

Thanks for your consideration

Please do not take away the ability of the individual to update their wireless devices. It's a necessity when manufacturers leave us in a lurch and don't keep their products secure or updated. It's bad enough with phones as it is, and wireless devices are in an even worse state depending on manufacturers to take care of us. With the up coming internet of things, this seems like it could have drastic side effects with many devices having wireless capabilities and vendor lock in. Who's to say what looks like a wireless router in the future if multiple devices are communicating with each other around the house acting like a mesh network. Taking away after market choice is a terrible idea!

Thanks for your consideration

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: Medema

Mailing Address: 7243 N 16th St

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85020

Email Address: john.medema@uniteddrugs.com

Organization Name: United Drugs

Comment: As a professional computer systems administrator, I am against this proposal. Specifically 2.1042 section (8)(e) and 2.935 section (d). While I can understand the FCC's desire to stop people from misusing the spectrum, this DRM solution is far too restrictive and usually ineffective.

In my job duties, I have often installed custom firmware on old wifi routers in order to implement a cost-effective wireless solution. These rules will also permanently lock out users from installing custom Operating Systems (linux) on laptops with wifi cards. These proposed restrictions will cost me significantly for no practical gain.

I often need to make changes to configuration files (linux) and the registry (windows) on wifi-enabled devices to improve networking performance (for example, disabling tcp offloading). Because the laptop manufacturers would be required to lock down the entire system (even my wired connections are affected), I would no longer be able to effectively manage my wired network.

I often want my company's phones and laptops to be on the most current kernel possible for security purposes, and this proposed rules will stop me from making hotfix changes when critical security issues are identified (think heartbleed).

Individual developers will be unable to work on open-source drivers for wireless networking devices. Driver-level bug fixes submitted by the open source community would be disallowed by this proposed rule.

As a professional computer systems administrator, I am against this proposal. Specifically 2.1042 section (8)(e) and 2.935 section (d). While I can understand the FCC's desire to stop people from misusing the spectrum, this DRM solution is far too restrictive and usually ineffective.

In my job duties, I have often installed custom firmware on old wifi routers in order to implement a cost-effective wireless solution. These rules will also permanently lock out users from installing custom Operating Systems (linux) on laptops with wifi cards. These proposed restrictions will cost me significantly for no practical gain.

I often need to make changes to configuration files (linux) and the registry (windows) on wifi-enabled devices to improve networking performance (for example, disabling tcp offloading). Because the laptop manufacturers would be required to lock down the entire system (even my wired connections are affected), I would no longer be able to effectively manage my wired network.

I often want my company's phones and laptops to be on the most current kernel possible for security purposes, and this proposed rules will stop me from making hotfix changes when critical security issues are identified (think heartbleed).

Individual developers will be unable to work on open-source drivers for wireless networking devices. Driver-level bug fixes submitted by the open source community would be disallowed by 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: Benjamin

Last Name: Kugler

Mailing Address: 118 E. Ridgeview Dr

City: Bloomington

Country: United States

State or Province: IN

ZIP/Postal Code: 47401

Email Address: ben@bkugler.com

Organization Name:

Comment: Thank you for reading my comment.

I have to ask that the FCC not implement the proposed restrictions on the ability of users to modify the firmware on their devices. I am a college student working on a degree in Computer Science, and have many times found myself at an advantage (compared to my peers) because of my familiarity with many of the systems on which we are taught: Linux systems. My familiarity comes from the fact that my laptop runs on ArchLinux, and that my Android device is rooted. Under the proposed restrictions, manufacturers would be required to implement security features that would make it impossible for me to do that. It would directly harm my ability to continue my studies and gain much-needed practice in the tasks for which I one day hope to be employed.

Thank you for reading my comment.

I have to ask that the FCC not implement the proposed restrictions on the ability of users to modify the firmware on their devices. I am a college student working on a degree in Computer Science, and have many times found myself at an advantage (compared to my peers) because of my familiarity with many of the systems on which we are taught: Linux systems. My familiarity comes from the fact that my laptop runs on ArchLinux, and that my Android device is rooted. Under the proposed restrictions, manufacturers would be required to implement security features that would make it impossible for me to do that. It would directly harm my ability to continue my studies and gain much-needed practice in the tasks for which I one day hope to be employed.

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: Snow

Mailing Address: 255 Florence

City: Troy

Country: United States

State or Province: MI

ZIP/Postal Code: 48098

Email Address: snowkilts@gmail.com

Organization Name:

Comment: I oppose this rule, as it would ban useful and proven open-source firmware for WiFi routers.

I oppose this rule, as it would ban useful and proven open-source firmware for WiFi routers.

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: Jackson

Mailing Address: 1506 S. Rock Hill

City: Webster Groves

Country: United States

State or Province: MO

ZIP/Postal Code: 63119

Email Address: nathan@jackson-group.biz

Organization Name:

Comment: The implementation of this rule would raise security and legal concerns for many individuals and small businesses. I do not want to be put in a scenario where I have to choose between making a software decision that I feel increases the security, reliability, and functionality of my network vs. potentially exposing myself to legal action under FCC regulations.

Using free and open firmware that is available to the public for review assures that we do not encounter security issues due to unsecured services (or intentional backdoors) in our firmware. It can also be used to enable features that are not available in manufactures firmware. Firmware from Netgear, Linksys, Asus, and other companies has repeatedly been found to expose network resources.

Not being able to fully control and modify firmware on a device that I own is not acceptable. Having to wait for a manufacturer to release a patch to secure a service I can't disable is not acceptable. I buy devices that I need to fill a specific set of needs, and manufactures provide firmware that is tailored to the widest variety of possible uses. Not being able to easily remove or disable features in a manufacturers firmware puts networks at risk!

The implementation of this rule would raise security and legal concerns for many individuals and small businesses. I do not want to be put in a scenario where I have to choose between making a software decision that I feel increases the security, reliability, and functionality of my network vs. potentially exposing myself to legal action under FCC regulations.

Using free and open firmware that is available to the public for review assures that we do not encounter security issues due to unsecured services (or intentional backdoors) in our firmware. It can also be used to enable features that are not available in manufactures firmware. Firmware from Netgear, Linksys, Asus, and other companies has repeatedly been found to expose network resources.

Not being able to fully control and modify firmware on a device that I own is not acceptable. Having to wait for a manufacturer to release a patch to secure a service I can't disable is not acceptable. I buy devices that I need to fill a specific set of needs, and manufactures provide firmware that is tailored to the widest variety of possible uses. Not being able to easily remove or disable features in a manufacturers firmware puts networks at risk!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: kyle

Last Name: ryans

Mailing Address: 3749 e taro lane

City: phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85050

Email Address: kyleryans32@gmail.com

Organization Name: independent

Comment: This submission is to 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.

What you need to understand, is that current generation WiFi routers are more computer, and less router. WiFi routers include functionality to provide firewall protection, anti-virus protection, media server functionality, VPN functionality, web server functionality, etc.

The above mentioned services (which is far from conclusive) introduce the potential for zero-day exploits. Removing the public's ability to protect their own environment (forcing them to rely upon vendor's to fix their devices) is an example of the government slowly eroding individuals freedom.

Further, many times a consumer decides to purchase a router based on it's hardware, with the intent to install customized firmware to provide functionality they need. By preventing this ability, you are simply making it less economical for potential consumers to find hardware and customize it to their liking.

From a risk perspective, why would the FCC feel such freedom generates an unacceptable risk, considering a consumer can go buy a car that goes 180 MPH? The parallel is, a consumer can do more harm with a car that is designed to brake nearly every practical law for the general use of an automobile, than to take a router with the ability to modify it and break US law. Trusting a driver not to speed is acceptable, while trusting a user of a wireless device to not modify it for illegal use isn't?

This submission is to 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.

What you need to understand, is that current generation WiFi routers are more computer, and less router. WiFi routers include functionality to provide firewall protection, anti-virus protection, media server functionality, VPN functionality, web server functionality, etc.

The above mentioned services (which is far from conclusive) introduce the potential for zero-day exploits. Removing the public's ability to protect their own environment (forcing them to rely upon vendor's to fix their devices) is an example of the government slowly eroding individuals freedom.

Further, many times a consumer decides to purchase a router based on it's hardware, with the intent to install customized

firmware to provide functionality they need. By preventing this ability, you are simply making it less economical for potential consumers to find hardware and customize it to their liking.

From a risk perspective, why would the FCC feel such freedom generates an unacceptable risk, considering a consumer can go buy a car that goes 180 MPH? The parallel is, a consumer can do more harm with a car that is designed to brake nearly every practical law for the general use of an automobile, than to take a router with the ability to modify it and break US law. Trusting a driver not to speed is acceptable, while trusting a user of a wireless device to not modify it for illegal use isn'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: Jason

Last Name: Howard

Mailing Address: 10224 Hile Street

City: Grass Valley

Country: United States

State or Province: CA

ZIP/Postal Code: 95945

Email Address:

Organization Name:

Comment: Hello-

I'm writing you today to voice my opinion that the FCC should make no rule that inhibits the public's ability to load their choice of firmware on their devices. Personally, this is very important to me, as I've run into several situations where the original device vendor's firmware is deficient or insecure in some way. Loading my own firmware on these devices was the only way to alleviate this issue.

Further, inhibiting the ability to load third party firmware will stifle innovation. Not everyone can build a wireless device. Many more, however, are able to write software. By locking down firmware, you essentially cut off the second group's ability to innovate.

Thank you for your time,  
Jason Howard, N6QED

Hello-

I'm writing you today to voice my opinion that the FCC should make no rule that inhibits the public's ability to load their choice of firmware on their devices. Personally, this is very important to me, as I've run into several situations where the original device vendor's firmware is deficient or insecure in some way. Loading my own firmware on these devices was the only way to alleviate this issue.

Further, inhibiting the ability to load third party firmware will stifle innovation. Not everyone can build a wireless device. Many more, however, are able to write software. By locking down firmware, you essentially cut off the second group's ability to innovate.

Thank you for your time,  
Jason Howard, N6QED

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: Heinrich

Mailing Address: 5934 Kingfisher Lane

City: Clarkston

Country: United States

State or Province: MI

ZIP/Postal Code: 48346

Email Address: David.Heinrich@gmail.com

Organization Name:

Comment: No this is wrong. This is just like changing a carburetor on an engine. If I own a piece of equipment, I own it. Locking the firmware to the manufacture changes it to a lease that I am not in control of even if I paid for it. Look at what John Deer is trying to do with tractors. Are you in the employment of big companies or the US citizens? Please stop this NOW.

No this is wrong. This is just like changing a carburetor on an engine. If I own a piece of equipment, I own it. Locking the firmware to the manufacture changes it to a lease that I am not in control of even if I paid for it. Look at what John Deer is trying to do with tractors. Are you in the employment of big companies or the US citizens? Please stop this NOW.

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: Adam

Last Name: Hughes

Mailing Address: 670 Louis Henna Blvd. Apt 2209

City: Round Rock

Country: United States

State or Province: TX

ZIP/Postal Code: 78664

Email Address: null

Organization Name: null

Comment: I am fully against this proposed regulation as a detriment to innovation and freedom of the internet as a medium. Please vote against passing these regulations.

I am fully against this proposed regulation as a detriment to innovation and freedom of the internet as a medium. Please vote against passing these regulations.

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: Overstreet

Mailing Address: 8711 Coral Dawn Ct

City: Temple Terrace

Country: United States

State or Province: FL

ZIP/Postal Code: 33637

Email Address:

Organization Name:

Comment: Depending on a hardware vendor to keep their shit together and supply security patches and software enhancements on existing platforms is quite possibly one of the worst ideas ever. A lot of the time, their promoted fix is to buy a new version of the device, instead of doing something silly like updating some software. Their track record for actually fixing something is usually not to do anything unless there is a massive public out-cry.

This sounds like an attempt to prevent people from modifying anything of a device they own, as long as, in this case, a 5GHz radio is installed. This would effectively stop already permitted activities like replacing the vendor rom on a cellphone. I do wonder what plans there are for going after SDRs broadcasting in the 5GHz range.

Hurray for vendor lock-in with planned obsolescence.

Depending on a hardware vendor to keep their shit together and supply security patches and software enhancements on existing platforms is quite possibly one of the worst ideas ever. A lot of the time, their promoted fix is to buy a new version of the device, instead of doing something silly like updating some software. Their track record for actually fixing something is usually not to do anything unless there is a massive public out-cry.

This sounds like an attempt to prevent people from modifying anything of a device they own, as long as, in this case, a 5GHz radio is installed. This would effectively stop already permitted activities like replacing the vendor rom on a cellphone. I do wonder what plans there are for going after SDRs broadcasting in the 5GHz range.

Hurray for vendor lock-in with planned obsolescence.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Bryan

Last Name: Prather-Huff

Mailing Address: 111 S Governor St.

City: Iowa City

Country: United States

State or Province: IA

ZIP/Postal Code: 52240

Email Address: bryan@pratherhuff.com

Organization Name: bryan@pratherhuff.com

Comment: While the spirit of this regulation may be protecting consumers and consumer products from damaging effects caused by misuse and misconfiguration, the realistic result of this legislation is a broad stroke of dangerous restriction on the ability for professionals and learned consumers to use their devices effectively. As a consumer and IT professional I find it disheartening that products which I rely on, on a near daily basis, such as Linux based router firmwares (Tomato, DDWRT), may suddenly be rendered illegal and impossible to use on new consumer devices. Regulations like this extend a large air of disrespect to well matured projects, especially Open Source, and are threatening to developers. In summary, DON'T PASS NEEDLESSLY BROAD LANGUAGED REGULATIONS.

While the spirit of this regulation may be protecting consumers and consumer products from damaging effects caused by misuse and misconfiguration, the realistic result of this legislation is a broad stroke of dangerous restriction on the ability for professionals and learned consumers to use their devices effectively. As a consumer and IT professional I find it disheartening that products which I rely on, on a near daily basis, such as Linux based router firmwares (Tomato, DDWRT), may suddenly be rendered illegal and impossible to use on new consumer devices. Regulations like this extend a large air of disrespect to well matured projects, especially Open Source, and are threatening to developers. In summary, DON'T PASS NEEDLESSLY BROAD LANGUAGED REGULATIONS.

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: Wing

Last Name: S

Mailing Address: PO Box 141

City: Pinehurst

Country: United States

State or Province: MA

ZIP/Postal Code: 01866

Email Address:

Organization Name:

Comment: Hello,

I am writing today to express my opposition to the proposal for "Equipment Authorization and Electronic Labeling for Wireless Devices." As I understand it these new rules would lock down WiFi devices so that their firmware could not be updated by the consumer as they wish.

While I understand that user-customizable firmware can be used in ways that are not legal and harmful to other devices, most users who use customizable firmware do not intend to use the firmware in this manner.

Instead, user-customizable firmware is an invaluable tool for consumers. It can be used for businesses to provide customers restricted WiFi access so that only paying customers use it. It can be used to create custom networks for research. And, perhaps most importantly, to ensure for a more secure Internet, often times user-customizable firmware can be used to patch security flaws in existing WiFi equipment. I have seen many routers whose manufacturers do not update their firmware, leaving them vulnerable to security flaws discovered after the router was released. Because user-customizable firmware is often quickly updated by the community, patches for routers are often released by the community first.

Hello,

I am writing today to express my opposition to the proposal for "Equipment Authorization and Electronic Labeling for Wireless Devices." As I understand it these new rules would lock down WiFi devices so that their firmware could not be updated by the consumer as they wish.

While I understand that user-customizable firmware can be used in ways that are not legal and harmful to other devices, most users who use customizable firmware do not intend to use the firmware in this manner.

Instead, user-customizable firmware is an invaluable tool for consumers. It can be used for businesses to provide customers restricted WiFi access so that only paying customers use it. It can be used to create custom networks for research. And, perhaps most importantly, to ensure for a more secure Internet, often times user-customizable firmware can be used to patch security flaws in existing WiFi equipment. I have seen many routers whose manufacturers do not update their firmware, leaving them vulnerable to security flaws discovered after the router was released. Because user-customizable firmware is often quickly updated by the community, patches for routers are often released by the community first.

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: Mayo

Mailing Address: 3356 Holly Dr

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95127

Email Address: jon@rm-f.net

Organization Name:

Comment: A requirement that prevents operators of a WiFi device from modifying, enhancing or repairing the software of a device provided by the original manufacturer is a troubling proposal.

Often we have to update firmware on devices that are no longer properly supported by the manufacturer to stay compliant with internet standards and remain good netizens. The problem of radio interference is not the only problem a device faces, as the internet protocols and websites themselves can suffer denial-of-service or unreliable behavior due to software defects. Many open source communities have form to repair software defects and add enhancements on the network layer to keep devices operating.

A requirement that prevents operators of a WiFi device from modifying, enhancing or repairing the software of a device provided by the original manufacturer is a troubling proposal.

Often we have to update firmware on devices that are no longer properly supported by the manufacturer to stay compliant with internet standards and remain good netizens. The problem of radio interference is not the only problem a device faces, as the internet protocols and websites themselves can suffer denial-of-service or unreliable behavior due to software defects. Many open source communities have form to repair software defects and add enhancements on the network layer to keep devices operating.

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: RobRoy

Last Name: kelly

Mailing Address: 212 N Sturgis

City: munkato

Country: United States

State or Province: MN

ZIP/Postal Code: 56001

Email Address:

Organization Name:

Comment: most commercial wifi routers have serious and numerous bugs most of which are not fixed or corrected in a timely manner. the open source router programs written to be installed on some of the more common wifi routers are the only way to maintain a secure and up to date system. why would you want to disable one of the better and cheaper ways to maintain internet security?

most commercial wifi routers have serious and numerous bugs most of which are not fixed or corrected in a timely manner. the open source router programs written to be installed on some of the more common wifi routers are the only way to maintain a secure and up to date system. why would you want to disable one of the better and cheaper ways to maintain internet 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: Karl

Last Name: Kurbjun

Mailing Address: 1304 Patton St.

City: Fort Collins

Country: United States

State or Province: CO

ZIP/Postal Code: 80524

Email Address: kkurbjun@gmail.com

Organization Name:

Comment: I understand the desire to prevent modification of the radio firmware, but anything beyond that is needlessly overstepping the FCC's charter.

This should not be used to prevent installing firmware such as DD-WRT as suggested by the SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES document: [https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking\\_number=39498](https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking_number=39498)

Having the ability to install DD-WRT in many cases results in a more secure router particularly with older routers that are not receiving firmware updates from the manufacturer but end up with published security vulnerabilities.

Again, I understand the purpose of locking down the SDR firmware, but that should not take priority over user's rights to devices they own.

I understand the desire to prevent modification of the radio firmware, but anything beyond that is needlessly overstepping the FCC's charter.

This should not be used to prevent installing firmware such as DD-WRT as suggested by the SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES document: [https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking\\_number=39498](https://apps.fcc.gov/kdb/GetAttachment.html?id=1UiSJRK869RsyQddPi5hpw%3D%3D&desc=594280%20D02%20U-NII%20Device%20Security%20v01r02&tracking_number=39498)

Having the ability to install DD-WRT in many cases results in a more secure router particularly with older routers that are not receiving firmware updates from the manufacturer but end up with published security vulnerabilities.

Again, I understand the purpose of locking down the SDR firmware, but that should not take priority over user's rights to devices they 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: Jon

Last Name: Tyler

Mailing Address: PO Box 757

City: Ocala

Country: United States

State or Province: FL

ZIP/Postal Code: 34478

Email Address:

Organization Name:

Comment: Government should not be in the business of removing the rights consumers to modify legally purchased products in any way we choose, so long as it does not violate the rights of others.

If I choose to repair a device that the manufacturer does not provide a fix for, that is my right. If you remove that right, you are forcing Americans to purchase a replacement product.

Government should not be in the business of removing the rights consumers to modify legally purchased products in any way we choose, so long as it does not violate the rights of others.

If I choose to repair a device that the manufacturer does not provide a fix for, that is my right. If you remove that right, you are forcing Americans to purchase a replacement product.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Stephen

Last Name: Deal

Mailing Address: 44 Rolling Hill Drive

City: Fairport

Country: United States

State or Province: NY

ZIP/Postal Code: 14450-9375

Email Address: devodl@gmail.com

Organization Name:

Comment: FCC please explain the existing problem you are trying to fix with the imposition of these rules. How extensive is the alleged problem that warrants such action?

In other words the FCC must JUSTIFY with accurate metrics the need for additional government regulation.

Americans demand the Freedom to choose and modify the firmware on their devices.

This Freedom does not imply that people will automatically violate FCC regulations. If the FCC chooses to impose these draconian measures then market forces will simply expand the availability of open source hardware and devices.

The proposed FCC 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.

FCC please explain the existing problem you are trying to fix with the imposition of these rules. How extensive is the alleged problem that warrants such action?

In other words the FCC must JUSTIFY with accurate metrics the need for additional government regulation.

Americans demand the Freedom to choose and modify the firmware on their devices.

This Freedom does not imply that people will automatically violate FCC regulations. If the FCC chooses to impose these draconian measures then market forces will simply expand the availability of open source hardware and devices.

The proposed FCC 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: Andrew

Last Name: Bradford

Mailing Address: 1870 Halesworth Ln

City: Ontario

Country: United States

State or Province: NY

ZIP/Postal Code: 14519

Email Address: bradfa@gmail.com

Organization Name:

Comment: Please do not restrict my ability to install software of my choosing on the computing devices which I have purchased.

I have owned 3 different wifi routers over the past decade. In all 3 cases, after about 1 year from when I purchased each router, the manufacturers all would decide to stop providing software updates for the routers. This left me with having a choice to do one of 3 things:

1. Buy another router.
2. Continue to use my router without any updates, exposing my router to known and published security vulnerabilities.
3. Install software on my router which was not provided by the router manufacturer.

For one of my routers, I decided to buy a different router. For another, I installed an open-source software distribution of Linux which was not provided by my router manufacturer which solved many of the outstanding security issues with that router and provided me with many years of service and software updates. In the 3rd case (my current wifi router), I have been running software on it which hasn't been updated by the manufacturer in 4 years and has known security vulnerabilities.

I'm currently shopping for a new router and I will not purchase one which does not have good support from a 3rd party open-source software distribution of Linux. This has proven to be the only way to keep my router software anywhere near up to date as the manufacturers do not continue to support products shortly after their launch.

The proposed new FCC rules will restrict my ability to have a secure network as I will not be able to install the software of my choosing and I will be stuck only using vendor provided software, which has been shown in 3 out of 3 of my last 10 years of wifi router ownership to be a very big letdown.

Please do not restrict my ability to install software of my choosing on the computing devices which I have purchased.

I have owned 3 different wifi routers over the past decade. In all 3 cases, after about 1 year from when I purchased each router, the manufacturers all would decide to stop providing software updates for the routers. This left me with having a choice to do one of 3 things:

1. Buy another router.
2. Continue to use my router without any updates, exposing my router to known and published security vulnerabilities.
3. Install software on my router which was not provided by the router manufacturer.

For one of my routers, I decided to buy a different router. For another, I installed an open-source software distribution of Linux which was not provided by my router manufacturer which solved many of the outstanding security issues with that router and provided me with many years of service and software updates. In the 3rd case (my current wifi router), I have been running software on it which hasn't been updated by the manufacturer in 4 years and has known security vulnerabilities.

I'm currently shopping for a new router and I will not purchase one which does not have good support from a 3rd party open-source software distribution of Linux. This has proven to be the only way to keep my router software anywhere near up to date as the manufacturers do not continue to support products shortly after their launch.

The proposed new FCC rules will restrict my ability to have a secure network as I will not be able to install the software of my choosing and I will be stuck only using vendor provided software, which has been shown in 3 out of 3 of my last 10 years of wifi router ownership to be a very big letdown.

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: Anthony

Last Name: Karakashian

Mailing Address: 124 Hartsdale Road

City: Rochester

Country: United States

State or Province: NY

ZIP/Postal Code: 14622

Email Address: savewifi@monstertruck.cc

Organization Name: NA

Comment: It's my understanding this proposed rule change would hinder my ability to flash devices I own with new versions of software that provide features the stock does not. This is not acceptable in any way.

First, as a user of Android-based products, I rely on the rich community of developers who produce custom versions of Android, so I can find the feature-set that more closely fits my needs. I buy a specific phone for the hardware specs, not the software it runs. If the software doesn't fit my needs, I can replace it, as it should be. You buy hardware for hardware, not the software that runs on it.

Second, as a person with a wifi network at home, I rely on the community to provide versions of the software for my router that provides a wider range of features. As a "computer" (for that is what it really is) that runs 24/7 in my house regardless of if it's being actively used, and is woefully underutilized for the majority of that time, I prefer it perform additional functions for me beyond simply routing packets to justify the electricity use in our current period of climate change.

I understand, the purpose of this rule is to ensure a piece of hardware equipped with a radio will never violate the levels it was shipped with; levels that were confirmed by the manufacturer to you as being acceptable to minimize interference with other products.

That's a reasonable requirement to make, however this rule is far over-compassing and would cause more damage in other areas and fields. Limit the rule to just modifying signal strength, as that's all you really want to do. Manufacturers can produce products that can't be modified through software, so make them do that and that alone. There. Easily fixed, and everyone's happy.

It's my understanding this proposed rule change would hinder my ability to flash devices I own with new versions of software that provide features the stock does not. This is not acceptable in any way.

First, as a user of Android-based products, I rely on the rich community of developers who produce custom versions of Android, so I can find the feature-set that more closely fits my needs. I buy a specific phone for the hardware specs, not the software it runs. If the software doesn't fit my needs, I can replace it, as it should be. You buy hardware for hardware, not the software that runs on it.

Second, as a person with a wifi network at home, I rely on the community to provide versions of the software for my router that provides a wider range of features. As a "computer" (for that is what it really is) that runs 24/7 in my house regardless of if it's being actively used, and is woefully underutilized for the majority of that time, I prefer it perform

additional functions for me beyond simply routing packets to justify the electricity use in our current period of climate change.

I understand, the purpose of this rule is to ensure a piece of hardware equipped with a radio will never violate the levels it was shipped with; levels that were confirmed by the manufacturer to you as being acceptable to minimize interference with other products.

That's a reasonable requirement to make, however this rule is far over-compassing and would cause more damage in other areas and fields. Limit the rule to just modifying signal strength, as that's all you really want to do. Manufacturers can produce products that can't be modified through software, so make them do that and that alone. There. Easily fixed, and everyone's happy.

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: Kelly

Last Name: Price

Mailing Address: 536 Greentree Terrace

City: Auburn

Country: United States

State or Province: AL

ZIP/Postal Code: 36832-2920

Email Address:

Organization Name:

Comment: Section 20 would prevent users from being able to fix software vulnerabilities in routers (a common occurrence). It would also stifle research into new wireless protocols. It is not acceptable.

Section 20 would prevent users from being able to fix software vulnerabilities in routers (a common occurrence). It would also stifle research into new wireless protocols. It is not acceptable.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Tyler

Last Name: McClure

Mailing Address: 228 Hunter Rd

City: Hayesville

Country: United States

State or Province: NC

ZIP/Postal Code: 28904

Email Address: t\_mcclure1@aol.com

Organization Name:

Comment: I completely disagree with your motion to control and in essence prohibit the "flashing" of firmware for routers and similar devices. You will only hold back innovation that allows us to advance in an ever changing world of technologies.

I completely disagree with your motion to control and in essence prohibit the "flashing" of firmware for routers and similar devices. You will only hold back innovation that allows us to advance in an ever changing world of technologies.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: cheryl

Last Name: miller

Mailing Address: 2704 Mintlaw ave

City: Henderson

Country: United States

State or Province: NV

ZIP/Postal Code: 89044

Email Address: cheraflu@yahoo.com

Organization Name:

Comment: the rule is way too general and applies to too many things that need to be modified by the owners of devices like routers. If you make it specific to modifications "proven to be designed to circumvent the law" or something it might not be so bad, but you should not be telling people they can't make any modifications.

the rule is way too general and applies to too many things that need to be modified by the owners of devices like routers.

If you make it specific to modifications "proven to be designed to circumvent the law" or something it might not be so bad, but you should not be telling people they can't make any 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: Derick

Last Name: Geisendorfer

Mailing Address: 2246 Meadowood Drive

City: Kronenwetter

Country: United States

State or Province: WI

ZIP/Postal Code: 54455

Email Address: dorfer21@hotmail.com

Organization Name:

Comment: This proposed regulation is bad and you should feel bad.

The decision to update/change the firmware on a router should remain with the consumer. To make it illegal to update firmware will open holes in unpatched routers as anytime a bug is found it would be up to the device manufacturer to release a patch. On devices as young as a year or two the manufacturer may not release a patch for the issue therefore keeping a known bug 'in the wild'.

They may not update the firmware on older routers anyway, but the user has then option to upload an Open Source firmware that doesn't have that vulnerability.

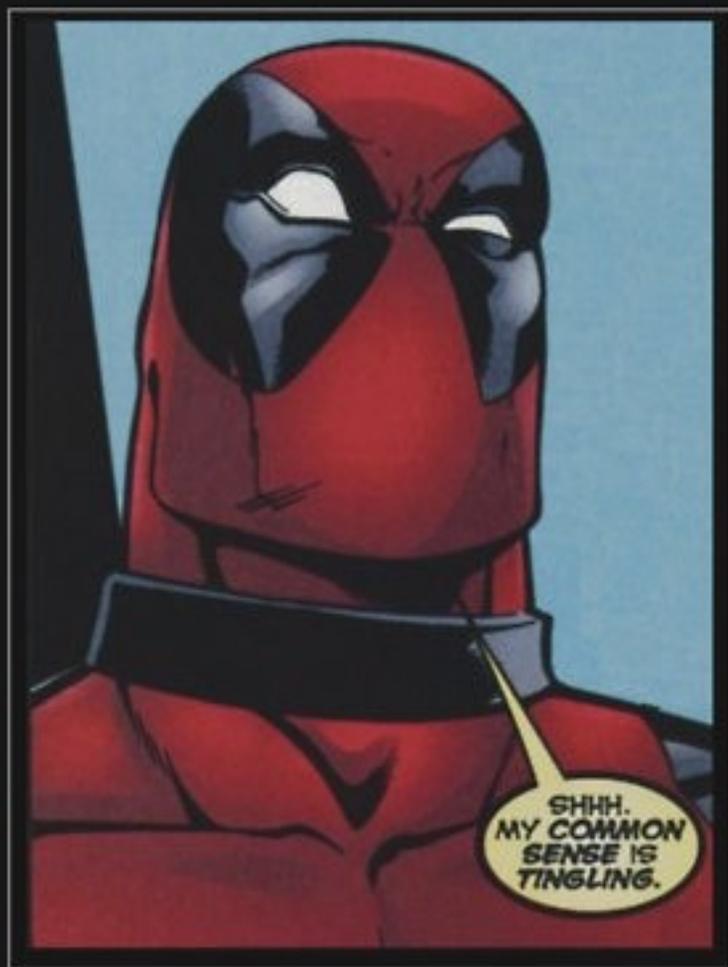
My one question, how many complaints have you received as a result of the option to install a custom firmware to a router and from whom?

This proposed regulation is bad and you should feel bad.

The decision to update/change the firmware on a router should remain with the consumer. To make it illegal to update firmware will open holes in unpatched routers as anytime a bug is found it would be up to the device manufacturer to release a patch. On devices as young as a year or two the manufacturer may not release a patch for the issue therefore keeping a known bug 'in the wild'.

They may not update the firmware on older routers anyway, but the user has then option to upload an Open Source firmware that doesn't have that vulnerability.

My one question, how many complaints have you received as a result of the option to install a custom firmware to a router and from whom?



# Common Sense

---

So rare it's a god damn super power.

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: Gary

Mailing Address: 1610 Cornfield Circle

City: Farmington

Country: United States

State or Province: NY

ZIP/Postal Code: 14425-9318

Email Address: flake@frontiernet.net

Organization Name: NA

Comment: I think making it so that open source software is effectively impossible to get certified is wrong. Many times the open source software is more responsive than manufacturers and blocking them from the hardware that I prefer to use is nonsense. Manufacturers in many cases stop releasing fixes to their firmware because they have newer products and don't want to be bothered spending money on something that they aren't making money on any longer. Free and open source software tends to give older equipment a longer lifespan because many of the people working on it don't care about the fact that the product isn't making money they care about it working properly. Plus shutting off this avenue to keeping older hardware and in some cases newer hardware relevant means that the hardware will just be thrown away instead of being used until it has died the permanent death so it goes to fill trash heaps much sooner than it would otherwise. Even if recycled, not all parts are recycled so this will add to the waste that our society is already generating making the world a worse place instead of a better place.

I think making it so that open source software is effectively impossible to get certified is wrong. Many times the open source software is more responsive than manufacturers and blocking them from the hardware that I prefer to use is nonsense. Manufacturers in many cases stop releasing fixes to their firmware because they have newer products and don't want to be bothered spending money on something that they aren't making money on any longer. Free and open source software tends to give older equipment a longer lifespan because many of the people working on it don't care about the fact that the product isn't making money they care about it working properly. Plus shutting off this avenue to keeping older hardware and in some cases newer hardware relevant means that the hardware will just be thrown away instead of being used until it has died the permanent death so it goes to fill trash heaps much sooner than it would otherwise. Even if recycled, not all parts are recycled so this will add to the waste that our society is already generating making the world a worse place instead of a better 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: David

Last Name: Marsh

Mailing Address: 39317 Fallbrook Circle

City: Palmdale

Country: United States

State or Province: CA

ZIP/Postal Code: 93551

Email Address:

Organization Name:

Comment: Please reconsider the portion of these proposed rules that will effectively ban third-party firmware development and installation on wireless networking devices.

If the rule goes into effect as-is, it will make illegal a common practice of changing device firmware to add features and increase security. The security issues in particular are troubling, as many manufacturers fail to support their equipment with security updates after new models are on the market, typically on a 6-12 month cycle.

I personally have fixed security flaws in several consumer-grade WiFi routers after the manufacturers failed to support them. If the rule were in effect at the time, I would have had no choice but to discard these otherwise good devices.

There are many other reasons to change device firmware that do not cause the affected device to operate the radio elements in ways the violate the proposed or existing rules. In the case of consumer-grade WiFi routers, it is possible to add networking features that make them far more functional, but leave radio operation untouched. The proposed rule will, perhaps unintentionally, effectively destroy the ability to do this. Please reconsider.

Please reconsider the portion of these proposed rules that will effectively ban third-party firmware development and installation on wireless networking devices.

If the rule goes into effect as-is, it will make illegal a common practice of changing device firmware to add features and increase security. The security issues in particular are troubling, as many manufacturers fail to support their equipment with security updates after new models are on the market, typically on a 6-12 month cycle.

I personally have fixed security flaws in several consumer-grade WiFi routers after the manufacturers failed to support them. If the rule were in effect at the time, I would have had no choice but to discard these otherwise good devices.

There are many other reasons to change device firmware that do not cause the affected device to operate the radio elements in ways the violate the proposed or existing rules. In the case of consumer-grade WiFi routers, it is possible to add networking features that make them far more functional, but leave radio operation untouched. The proposed rule will, perhaps unintentionally, effectively destroy the ability to do this. 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: John

Last Name: Chamberlain

Mailing Address: PO Box 747

City: Natick

Country: United States

State or Province: MA

ZIP/Postal Code: 01760

Email Address: null

Organization Name: null

Comment: Concerning the aspect of the proposed rule "Equipment Authorization and Electronic Labeling for Wireless Devices" that would make it illegal for third parties to modify router ("certified equipment") firmware, I am submitting this comment opposing the proposed rule.

(First of all I find it obnoxious that your comment web site requires both Javascript (a security risk) and cookies (a privacy violation). I suggest you program your web site to use IP address rather than cookies and not use Javascript in the future.)

Secondly, let me just say for the record that I am opposed to non-elected persons and organizations making laws and I consider it unconstitutional and undemocratic for non-legislative bodies to be generating new legal statutes. I do not believe it is either proper nor the right of Congress to delegate to you or anyone else their law-making authority and it is wrong for you to be making federal laws without a vote in Congress.

Concerning the so-called "rule" itself:

Making it illegal for people to modify their own radio transmission equipment, including wireless routers, is an arrogant, oppressive and un-American idea which harkens back to the worst excesses of totalitarian regimes such as those of the Soviet Union and the so-called Deutsche Demokratische Republik who had many such "regulations" in their toolkit of oppression.

Choking off millions of people from using radio equipment in the ways they see fit, in a supposed effort to prevent radio interference, would be highly damaging to both the economy and technological progress. I say "supposed effort" because this rule will do nothing to hinder those small numbers people who for whatever reason are generating interference. This rule will only succeed in crushing the aspirations of millions of legitimate router users, while doing nothing to affect the tiny handful of interferers who will simply ignore your regulation. There are already "rules" in place concerning the generation of radio interference. Criminalizing modification of radio equipment adds nothing to these existing rules and will do nothing additional to prevent interference.

Concerning the aspect of the proposed rule "Equipment Authorization and Electronic Labeling for Wireless Devices" that would make it illegal for third parties to modify router ("certified equipment") firmware, I am submitting this comment opposing the proposed rule.

(First of all I find it obnoxious that your comment web site requires both Javascript (a security risk) and cookies (a privacy violation). I suggest you program your web site to use IP address rather than cookies and not use Javascript in

the future.)

Secondly, let me just say for the record that I am opposed to non-elected persons and organizations making laws and I consider it unconstitutional and undemocratic for non-legislative bodies to be generating new legal statutes. I do not believe it is either proper nor the right of Congress to delegate to you or anyone else their law-making authority and it is wrong for you to be making federal laws without a vote in Congress.

Concerning the so-called "rule" itself:

Making it illegal for people to modify their own radio transmission equipment, including wireless routers, is an arrogant, oppressive and un-American idea which harkens back to the worst excesses of totalitarian regimes such as those of the Soviet Union and the so-called Deutsche Demokratische Republik who had many such "regulations" in their toolkit of oppression.

Choking off millions of people from using radio equipment in the ways they see fit, in a supposed effort to prevent radio interference, would be highly damaging to both the economy and technological progress. I say "supposed effort" because this rule will do nothing to hinder those small numbers people who for whatever reason are generating interference. This rule will only succeed in crushing the aspirations of millions of legitimate router users, while doing nothing to affect the tiny handful of interferers who will simply ignore your regulation. There are already "rules" in place concerning the generation of radio interference. Criminalizing modification of radio equipment adds nothing to these existing rules and will do nothing additional to prevent interference.

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: Mark

Last Name: Craig

Mailing Address: 60 Creeks Edge Way

City: Sacramento

Country: United States

State or Province: CA

ZIP/Postal Code: 95823

Email Address: null

Organization Name: null

Comment: Isn't this delicious irony? The FCC's own "SamKnows" broadband survey project uses Netgear routers with modified firmware that enables the routers to phone home the broadband benchmark data collected. This rule would apparently invalidate the FCC's own survey project unless it hypocritically excludes these routers from the rule.

(I know about this modified firmware because I'm a project participant and have one of the modified routers.)

Isn't this delicious irony? The FCC's own "SamKnows" broadband survey project uses Netgear routers with modified firmware that enables the routers to phone home the broadband benchmark data collected. This rule would apparently invalidate the FCC's own survey project unless it hypocritically excludes these routers from the rule.

(I know about this modified firmware because I'm a project participant and have one of the modified routers.)

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: McMahon

Mailing Address: 696 West Timothy Dr

City: La Porte

Country: United States

State or Province: IN

ZIP/Postal Code: 46350

Email Address:

Organization Name:

Comment: I wish to express my disagreement with this proposed FCC Regulation. I comprehend the desire to restrict malicious (unintentional or not) disruption to existing Wi-Fi networking by utilizing a base level DRM to prevent modifications of firmware code, however this proposed regulation goes too far. Allowing end users the opportunity to enhance the utility of their purchased physical devices through modifications in software are the essence of our modern computing platforms. I personally utilize DD-WRT on my home router as it allows me more flexibility in my system than the original firmware would ever do. I fear that implementation of this regulation would affect hundreds of thousands of end users like myself from being able to utilize a third party firmware to enhance and expand my ability to maintain and control my networking connections. Please revise this proposed regulation to expressly exempt the installation of third party firmware into electronic devices by the owners of those devices.

Sincerely Yours,

I wish to express my disagreement with this proposed FCC Regulation. I comprehend the desire to restrict malicious (unintentional or not) disruption to existing Wi-Fi networking by utilizing a base level DRM to prevent modifications of firmware code, however this proposed regulation goes too far. Allowing end users the opportunity to enhance the utility of their purchased physical devices through modifications in software are the essence of our modern computing platforms. I personally utilize DD-WRT on my home router as it allows me more flexibility in my system than the original firmware would ever do. I fear that implementation of this regulation would affect hundreds of thousands of end users like myself from being able to utilize a third party firmware to enhance and expand my ability to maintain and control my networking connections. Please revise this proposed regulation to expressly exempt the installation of third party firmware into electronic devices by the owners of those devices.

Sincerely Yours,