

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: Afonso

Last Name: Garcia

Mailing Address: Jmerntaival 11 G 160

City: Espoo

Country: Finland

State or Province: Uusimaa

ZIP/Postal Code: 02150

Email Address:

Organization Name:

Comment: To whom it may concern,

It has come to my attention that this proposal will stop users and resellers from modifying the software installed on their devices. It is my opinion that this will harm our ability to study and develop new technologies using RF products.

As an example of that, I would like you to know what I've been doing for my master thesis. I am developing a system that will enable the uploads to cloud services to be faster and consume less energy. In order to test it, I am using an Android device as a client and a computer as a server.

The computer I'm using originally had Windows installed but I am using Ubuntu, a variant of the GNU/Linux OS, to run my software, since it is only compatible with GNU/Linux. Under the proposed rule, I would not be able to do this.

I also need access to lower level functions of the Android OS to gather data. To do this, I had to install a custom firmware on the device. Under the proposed rule, I would not be able to do this.

To connect all devices together, I am using a wifi router . However, for my measurements I need to limit the connection speed of the Android device. To do so, I had to install DD-WRT, a free alternative firmware for my router. Under the proposed rule, I would not be able to do this.

Concluding my example, if this rule was in effect, I wouldn't be able to develop the system I'm developing and, as a result, I wouldn't be able to do my master thesis.

More so, limiting access to the OS and firmware of devices will make people unable to search for flaws on their designs that may have security implications for the user or even for the national security of the USA and its allies.

As such, I urge you to not approve this proposed rule, as it will stop scientific advance and will cause security issues in the long term.

Best regards,

Afonso Garcia

To whom it may concern,

It has come to my attention that this proposal will stop users and resellers from modifying the software installed on their devices. It is my opinion that this will harm our ability to study and develop new technologies using RF products.

As an example of that, I would like you to know what I've been doing for my master thesis. I am developing a system that will enable the uploads to cloud services to be faster and consume less energy. In order to test it, I am using an Android device as a client and a computer as a server.

The computer I'm using originally had Windows installed but I am using Ubuntu, a variant of the GNU/Linux OS, to run my software, since it is only compatible with GNU/Linux. Under the proposed rule, I would not be able to do this.

I also need access to lower level functions of the Android OS to gather data. To do this, I had to install a custom firmware on the device. Under the proposed rule, I would not be able to do this.

To connect all devices together, I am using a wifi router . However, for my measurements I need to limit the connection speed of the Android device. To do so, I had to install DD-WRT, a free alternative firmware for my router. Under the proposed rule, I would not be able to do this.

Concluding my example, if this rule was in effect, I wouldn't be able to develop the system I'm developing and, as a result, I wouldn't be able to do my master thesis.

More so, limiting access to the OS and firmware of devices will make people unable to search for flaws on their designs that may have security implications for the user or even for the national security of the USA and its allies.

As such, I urge you to not approve this proposed rule, as it will stop scientific advance and will cause security issues in the long term.

Best regards,

Afonso Garcia

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: Adriano

Last Name: Peluso

Mailing Address: via di palma 129

City: Taranto

Country: Italy

State or Province: TA

ZIP/Postal Code: 74123

Email Address: catonano@gmail.com

Organization Name:

Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *still* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks for listening.

I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more

lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *still* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks 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: Dietmar

Last Name: Gombotz

Mailing Address: Spengergasse 37-39/3. Stock

City: Vienna

Country: Austria

State or Province: Vienna

ZIP/Postal Code: 1050

Email Address: d.gombotz@gmx.at

Organization Name: Sphares GmbH

Comment: I have read through the proposal and cannot but shake my head at the proposed regulation of the software part of wireless devices.

As you might, or might not know "Software is eating the world", much of today's progress and innovation comes from the way to integrate software and hardware systems. software allows fast upgrading, longer lifetime of hardware (as security fixes and modern protocols can be added on later) and more innovation on the whole sector. Therefore trying to splitting into a defined "secure" firmware and an flexible software part is clueless. the more i can do in the software part the better for the usage scenarios and the competition within the sector.

This only helps the producers of hardware, because they believe that they can sell more products when theirs have some kind of "planned obsolescence", but this will be bad for consumers and business using those devices because it will hinder them in their advancements and bind unnecessary capital.

Allow the market to decide what is a good product and what is a bad product. if a product does not work properly people will stop using it.

i am strongly against this proposal

I have read through the proposal and cannot but shake my head at the proposed regulation of the software part of wireless devices.

As you might, or might not know "Software is eating the world", much of today's progress and innovation comes from the way to integrate software and hardware systems. software allows fast upgrading, longer lifetime of hardware (as security fixes and modern protocols can be added on later) and more innovation on the whole sector. Therefore trying to splitting into a defined "secure" firmware and an flexible software part is clueless. the more i can do in the software part the better for the usage scenarios and the competition within the sector.

This only helps the producers of hardware, because they believe that they can sell more products when theirs have some kind of "planned obsolescence", but this will be bad for consumers and business using those devices because it will hinder them in their advancements and bind unnecessary capital.

Allow the market to decide what is a good product and what is a bad product. if a product does not work properly people will stop using it.

i am strongly against this proposal

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: Bimmler

Mailing Address: Zrichstrasse 119

City: Ksnacht

Country: Switzerland

State or Province: Zrich

ZIP/Postal Code: 8700

Email Address:

Organization Name:

Comment: Please do not implement the rules which disallow users to install software of their choosing on their computing devices. Locking down so many devices (basically everything has a wireless module by now, or will soon) is going to be devastating for research, security and even commerce.

Researchers need to be able to tinker with their devices, progress would come to a sudden halt if that is not possible anymore.

It is all too obvious that security holes would be ignored by OEMs, be that for old devices or for new ones, and leaving everybody else unable to modify the software on these devices is great for exploiting these vulnerabilities, but terrible for everyone else.

Finally, quite a bit of commerce also depends on users being able to install software on their devices: secure wifi vendors, retail hotspot vendors etc.

Don't do it.

Please do not implement the rules which disallow users to install software of their choosing on their computing devices. Locking down so many devices (basically everything has a wireless module by now, or will soon) is going to be devastating for research, security and even commerce.

Researchers need to be able to tinker with their devices, progress would come to a sudden halt if that is not possible anymore.

It is all too obvious that security holes would be ignored by OEMs, be that for old devices or for new ones, and leaving everybody else unable to modify the software on these devices is great for exploiting these vulnerabilities, but terrible for everyone else.

Finally, quite a bit of commerce also depends on users being able to install software on their devices: secure wifi vendors, retail hotspot vendors etc.

Don't do it.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Valentino

Last Name: Stampone

Mailing Address: valentino.stampone@gmail.com

City: Quiliano (Savona)

Country: Italy

State or Province: Italia

ZIP/Postal Code: 17047

Email Address:

Organization Name:

Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *still* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks for listening.

I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however **still** possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks 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: Anonymous

Last Name: Anonymous

Mailing Address: Arroyo Drive 1000

City: Irvine

Country: Germany

State or Province: CA

ZIP/Postal Code: 92614

Email Address: null

Organization Name: null

Comment: Planned legislation to restrict the freedom to install alternative software on wireless communication devices is extremely harmful.

Running alternative software that is free and open - as in available to be independently reviewed, studied, modified and distributed - is essential to having control over the setup of ones network environment. Since much of peoples' political and social life happens via this network, freedom to control it is of emminent importance.

Further, being able to deploy alternative software on wireless devices is required to construct decentralised and accessible networks, which can be part of very important social infrastructure.

It is possible to deploy such networks without interffering with other networks and public service infrastructure.

Prohibition of deploying alternative software is not an effective and proportional measure to ensure compatibility and non-interference.

Planned legislation to restrict the freedom to install alternative software on wireless communication devices is extremely harmful.

Running alternative software that is free and open - as in available to be independently reviewed, studied, modified and distributed - is essential to having control over the setup of ones network environment. Since much of peoples' political and social life happens via this network, freedom to control it is of emminent importance.

Further, being able to deploy alternative software on wireless devices is required to construct decentralised and accessible networks, which can be part of very important social infrastructure.

It is possible to deploy such networks without interffering with other networks and public service infrastructure.

Prohibition of deploying alternative software is not an effective and proportional measure to ensure compatibility and non-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: Jeremiah

Last Name: Nichols

Mailing Address: 3851 Banyan Dr Apt B

City: Bowling Green

Country: United States

State or Province: KY

ZIP/Postal Code: 42104

Email Address: Dirtysouthboy91@gamil.com

Organization Name: null

Comment: I ask that you not implement these rules not allowing people to customize their routers with software like DD-WRT of Pfsense. These router OS's are usually more secure and stable then what manufacturers choose to release in updates. Using these other operating systems allow you to expand greatly on the options available let to consumers, such as features and security. These different router operating systems have fixed bugs and security holes which big manufacturers have ignored. We all know how security is especially when it comes to people finances and lives. This also is a business for me. If I can no longer perfor these services I will loose money in my personal life, since I do this as a second job. I build, sell, and reprogram routers with this software for people to enhance their security and give them better experiences then what some manufacturers give their customers. People also rely on modifying software as well for setting up hot spots. This is crucial for Hotspot software to be to be installed. If it's taken away that will cut a individual company or a businesses cash flow. This will hurt software developers, people trying to get better security and better user experience, and lots of money would be lost to people that rely on this as part of their lively hoods and businesses.

I ask that you not implement these rules not allowing people to customize their routers with software like DD-WRT of Pfsense. These router OS's are usually more secure and stable then what manufacturers choose to release in updates. Using these other operating systems allow you to expand greatly on the options available let to consumers, such as features and security. These different router operating systems have fixed bugs and security holes which big manufacturers have ignored. We all know how security is especially when it comes to people finances and lives. This also is a business for me. If I can no longer perfor these services I will loose money in my personal life, since I do this as a second job. I build, sell, and reprogram routers with this software for people to enhance their security and give them better experiences then what some manufacturers give their customers. People also rely on modifying software as well for setting up hot spots. This is crucial for Hotspot software to be to be installed. If it's taken away that will cut a individual company or a businesses cash flow. This will hurt software developers, people trying to get better security and better user experience, and lots of money would be lost to people that rely on this as part of their lively hoods and businesses.

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: Fabio

Last Name: Muzzi Frabetti

Mailing Address: Vicolo Viazzolo 3

City: Bologna

Country: Italy

State or Province: BO

ZIP/Postal Code: 40124

Email Address: fabio@muzzi.net

Organization Name:

Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *still* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

* Ham radio operators like myself will be unable to use commercial devices for their lawful hobby and experiments.

* This ruling will impact also nations that are not ruled by the FCC, because manufacturers will standardize on one product design only (that is going to be FCC approved) and not bother to design an FCC-approved version and an unlocked version for the rest of the world.

Best regards.

I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *still* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

* Ham radio operators like myself will be unable to use commercial devices for their lawful hobby and experiments.

* This ruling will impact also nations that are not ruled by the FCC, because manufacturers will standardize on one product design only (that is going to be FCC approved) and not bother to design an FCC-approved version and an unlocked version for the rest of the world.

Best regards.

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: painter

Mailing Address: 7234 antelope meadows cir

City: falcon

Country: United States

State or Province: CO

ZIP/Postal Code: 80831

Email Address: painterengr@gmail.com

Organization Name: painter engineering inc

Comment: I am writing to oppose this proposed rule to the extent that it would prevent or restrict the use of open-source operating software for many WiFi Routers and experimentation by licensed Amateurs.

My comments below refer to the reference numbers in the SUPPLEMENTARY INFORMATION Section of the proposed rule.

Please see attached text file.

I am writing to oppose this proposed rule to the extent that it would prevent or restrict the use of open-source operating software for many WiFi Routers and experimentation by licensed Amateurs.

My comments below refer to the reference numbers in the SUPPLEMENTARY INFORMATION Section of the proposed rule.

Please see attached text file.

I am writing to oppose this proposed rule to the extent that it would prevent or restrict the use of open-source operating software for many WiFi Routers and experimentation by licensed Amateurs.

My comments below refer to the reference numbers in the SUPPLEMENTARY INFORMATION Section of the proposed rule.

Ref 13: Additionally, manufacturers are increasingly designing transmitters that use software to set the operating parameters. Such RF-controlling software can allow adjustment of individual parameters or enable a device to operate in different modes, and the manufacturer may provide software upgrades in the field to enable new capabilities.

The above would include the open-source software commonly used in WiFi Routers. Yet these software, such as openwrt, dd-wrt and tomato to name a few, are well designed, stable and widely supported by the open-source community. In contrast, I know of only ONE router vendor, Buffalo (buffalotech.com), who supports and delivers an open-source option.

Ref 20: ... grantees would have to implement well-defined measures to ensure that certified equipment is not capable of operating with RF-controlling software for which it has not been approved. All manufacturers of devices that have software-based control of RF parameters would have to provide specific information about the software capabilities of their devices. The Commission proposed to require that an applicant for certification explicitly describe the RF device's capabilities for software configuration and upgradeability in the application for certification. This description would include all frequency bands, power levels, modulation types, or other modes of operation for which the device is designed to operate, including modes not enabled in the device as initially marketed. Also, an applicant for certification would have to specify which parties will be authorized to make software changes (e.g., the grantee, wireless service provider, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation.

The above clearly states that router vendors must prevent non-vendor software (I read as open-source) from being used. This clearly would prevent end users from running all open-source software. This is unacceptable. One of the reasons open-source router software was created and flourished is the router vendors have offered limited, often hobbled, features when even the embedded chip has vastly more features. Often too router vendors are slow or even never correct flaws. In contrast, open-source development is much more responsive in addition to feature rich.

Ref 29: The grantee of certification is responsible for the compliance of the certified equipment. When another party modifies a device through either hardware or software changes without the authority of the original grantee, or incorporates a certified device into another host device, that party becomes responsible for the modified device's compliance and must obtain a new FCC ID for its product.

The above would also prevent open-source software on WiFi routers because end users would not be able for a host of reasons to certify. Since only one vendor currently offers open-source all of the other brands and models would not be viable for use. This is potentially millions of devices that currently run the open-source software.

Ref 38: It proposed to revise Â§ 2.909(d), which allows a new party that performs device modifications without the consent of the original grantee to become responsible for the compliance by labeling the device with a statement indicating it was modified, with the requirement that the party obtain a new grant of certification. It would have to specify a new FCC ID unless the consent of the original is obtained.

The above would also prevent the use of open-source software on these routers. Clearly the vast majority of router vendors do not want end users to use open-source software which is seen as competition and thus would "not give consent".

Ref 41: The Commission also proposed to permit third-party RF-controlling software modifications to previously certified devices under the same procedures that currently apply to grantee modifications of SDRs.

Amateur radio has more than a century of experimentation and innovation. SDR, not unlike the open-source revolution with WiFi routers, currently enjoys the benefits of experimentation and innovation. Implementing this proposed rule would prevent what has long been supported by the FCC for Amateur Radio experimentation. This too is unacceptable.

Ref 88: The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.

This reference (and a number of others I don't list) does not account for the inclusion of individuals and end users that would be subjected to the rule if adopted. Open source WiFi Router software is installed by the end user typically. Based on Ref 88 none of these individuals would be counted and are likely to be very large numbers. Likewise in relation to Amateur Radio licensees for SDR and WiFi experimentation you have grossly under estimated the number of entities impacted. You cannot simply count large and small businesses and leave out individuals who already practice and in many cases are licensed in this area.

This same criticism applies to Ref 90.

Ref 97 claims that these changes in part are to reduce the burden of compliance. However, vast numbers of end users who install open source software into WiFi Routers would be required to to certify compliance. This would not reduce compliance burden.

Ref 99 completely fails to mention the end users who would be burdened by this rule and thus a large economic impact has been overlooked.

This proposed rule must NOT be adopted as written. It must be reworked to accommodate open-source software and Amateur experimentation and development.

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: Martin

Last Name: Ackermann

Mailing Address: Am Prinzenweg 5

City: Leopoldshhe

Country: Germany

State or Province: NRW

ZIP/Postal Code: 33818

Email Address: randycole42-wireless@mailinator.com

Organization Name:

Comment: Hi,

I recently updated my wifes and my own phone with an alternative firmware (cyanogen). Being able to do this is vital since the manufacturer seems not capable of providing security updates for a 2 year old smartphone in a reasonable short period. Using an alternative firmware protected us in this case from exploits for the stagefright security issue.

From my experience vendors of DSL routers and smartphones will stop issuing firmware updates way before their end-of-life. My DSL router works fine. Its fast enough for my slow landline, but its software is nearly 10 years old. Does it have security issues? Certainly! Can I update its firmware? Unfortunately not since its not a popular device any of the free software developers cares for.

If the proposed rule will result in me not being able to change the firmware of wireless devices I own, please make sure that the manufacturer is liable for all damage which was caused by out of maintenance products which could have been prevented by a firmware update.

Best regards,
Martin

: And yes, I think the US market is important enough that this'll affect me in Germany.

Hi,

I recently updated my wifes and my own phone with an alternative firmware (cyanogen). Being able to do this is vital since the manufacturer seems not capable of providing security updates for a 2 year old smartphone in a reasonable short period. Using an alternative firmware protected us in this case from exploits for the stagefright security issue.

From my experience vendors of DSL routers and smartphones will stop issuing firmware updates way before their end-of-life. My DSL router works fine. Its fast enough for my slow landline, but its software is nearly 10 years old. Does it have security issues? Certainly! Can I update its firmware? Unfortunately not since its not a popular device any of the free software developers cares for.

If the proposed rule will result in me not being able to change the firmware of wireless devices I own, please make sure that the manufacturer is liable for all damage which was caused by out of maintenance products which could have been

prevented by a firmware update.

Best regards,
Martin

: And yes, I think the US market is important enough that this'll affect me in Germany.

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: Krattiger

Mailing Address: 19353 Clymer St.

City: Porter Ranch

Country: United States

State or Province: CA

ZIP/Postal Code: 91326

Email Address: mr.music25@gmail.com

Organization Name: Xirrus, Inc.

Comment: As an avid user of Open Source Software, I believe the implementation of these rules is not justified. By "locking down" the firmware of devices it leaves a loophole available to possibly stop innovation and the freedom of choice. The point of this is to make it so that radio power settings can NOT be set over a certain amount, which is a good idea, but sacrificing one of the most important sectors in the computing industry is not the way to do it. Many people rely on open source routing software, such as DD-WRT, as the manufacturers stop updating it as soon as their latest product hits the shelves, and the devices get old and lack in features. While trying to just stop a problem that is relatively unheard of, you might inadvertently hurt the entire IT industry.

I hope that you change your minds about passing this rule, as it will harm everyone whether they know it or not.

As an avid user of Open Source Software, I believe the implementation of these rules is not justified. By "locking down" the firmware of devices it leaves a loophole available to possibly stop innovation and the freedom of choice. The point of this is to make it so that radio power settings can NOT be set over a certain amount, which is a good idea, but sacrificing one of the most important sectors in the computing industry is not the way to do it. Many people rely on open source routing software, such as DD-WRT, as the manufacturers stop updating it as soon as their latest product hits the shelves, and the devices get old and lack in features. While trying to just stop a problem that is relatively unheard of, you might inadvertently hurt the entire IT industry.

I hope that you change your minds about passing this rule, as it will harm everyone whether they know it or 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: Dan

Last Name: Mossor

Mailing Address: 8626 Barn Owl

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78255

Email Address: dan.mossor@gmail.com

Organization Name:

Comment: I strongly urge the FCC to reconsider the proposed rules for Software Defined Radios. The proposed rules will do more to hurt innovation and the economy than it will to serve whatever interest the FCC is attempting to placate.

I strongly urge the FCC to reconsider the proposed rules for Software Defined Radios. The proposed rules will do more to hurt innovation and the economy than it will to serve whatever interest the FCC is attempting to placate.

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 user's 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.

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 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.

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.

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

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: Martin

Last Name: Reinke

Mailing Address: 931 Sherman Ave

City: Evanston

Country: United States

State or Province: IL

ZIP/Postal Code: 60202

Email Address: rfdevices@martin-reinke.de

Organization Name:

Comment: Please see the attached file for comments.

Please see the attached file for comments.

This comment is mainly about part b, 18, 19, 20;

User Freedom

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 user's 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.

Innovation

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 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.

Economic Impact

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.

Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

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: Brian

Last Name: Busk

Mailing Address: 1401 Oregon St

City: Ashland

Country: United States

State or Province: OR

ZIP/Postal Code: 97520

Email Address: brian.busk@gmail.com

Organization Name:

Comment: Many times there is very little stability in the native firmware, being able to flash a different firmware has given me stability in a wireless world.

Many times there is very little stability in the native firmware, being able to flash a different firmware has given me stability in a wireless world.

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: Harrison

Last Name: Prevor

Mailing Address: 3700 Spruce St

City: Philadelphia

Country: United States

State or Province: PA

ZIP/Postal Code: 19104-6025

Email Address:

Organization Name:

Comment: Please don't restrict people's ability to install the operating system and firmware of their choice on hardware they own.

Please don't restrict people's ability to install the operating system and firmware of their choice on hardware 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: Tim

Last Name: Brackbill

Mailing Address: 211 E 15th

City: Larned

Country: United States

State or Province: KS

ZIP/Postal Code: 67550

Email Address: tbrackbill@cox.net

Organization Name:

Comment: Please don't be so foolhardy nor willingly captured by those you are supposed to regulate. You must be actively ignoring both historical and even current events of proprietary, closed-source firmware for both residential and even commercial grade routers being chocked-full of bugs and both intentional and unintentional backdoors, leaving all those who use them exposed and at the mercy of corporations that only value profit margins and thus slow-playing fixes or not even bothering to support the hardware they've already pocketed the money from.

The only thing that has fully protected US citizens, and MUST continue to be available is the ability to install OPEN SOURCE firmware and software on the routers and all communications equipment they already OWN. No human endeavor is perfect, nor is F/OSS software, BUT if vulnerabilities are found, there are literally thousands of dedicated, honest, passionate professionals there to pitch-in, contribute, and fix them FOR FREE, for their own security and privacy is on the line as well as ours. There have even been instances where the fix has occurred even as news of the bug was released. Don't take this away from us.

Ask your own tech folks for once, not the endless stream of corporate lobbyists spinning BS tales about 'security through obscurity' and no doubt promising future lucrative 'consultancy' gigs after your terms expire, in return for 'services rendered'.

Try to remember your oath of office for once and act like your promises to the American people weren't just empty lies.

I'll thank you when you do the right thing.

Please don't be so foolhardy nor willingly captured by those you are supposed to regulate. You must be actively ignoring both historical and even current events of proprietary, closed-source firmware for both residential and even commercial grade routers being chocked-full of bugs and both intentional and unintentional backdoors, leaving all those who use them exposed and at the mercy of corporations that only value profit margins and thus slow-playing fixes or not even bothering to support the hardware they've already pocketed the money from.

The only thing that has fully protected US citizens, and MUST continue to be available is the ability to install OPEN SOURCE firmware and software on the routers and all communications equipment they already OWN. No human endeavor is perfect, nor is F/OSS software, BUT if vulnerabilities are found, there are literally thousands of dedicated, honest, passionate professionals there to pitch-in, contribute, and fix them FOR FREE, for their own security and privacy is on the line as well as ours. There have even been instances where the fix has occurred even as news of the bug was released. Don't take this away from us.

Ask your own tech folks for once, not the endless stream of corporate lobbyists spinning BS tales about 'security thru obscurity' and no doubt promising future lucrative 'consultancy' gigs after your terms expire, in return for 'services rendered'.

Try to remember your oath of office for once and act like your promises to the American people weren't just empty lies.

I'll thank you when you do the right thing.

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: Michael

Last Name: Walker

Mailing Address: 4201 California Ave. #7

City: Bakersfield

Country: United Kingdom

State or Province: CA

ZIP/Postal Code: 93309

Email Address: mwalkerx45@gmail.com

Organization Name: none

Comment: This entire concept is based on the idea that people should not be allowed to modify their own equipment. There should be punishments for modifying the equipment in such a way that breaks other laws, but there should be no law, rule, or regulation of any sort banning or attempting to stop any modification as a whole. Modification is the basis for innovation. You can't innovate if you can't fiddle with it. I am against any rules that would hinder modifications in any way shape or form. I am in full support of banning modifications that break others.

This entire concept is based on the idea that people should not be allowed to modify their own equipment. There should be punishments for modifying the equipment in such a way that breaks other laws, but there should be no law, rule, or regulation of any sort banning or attempting to stop any modification as a whole. Modification is the basis for innovation. You can't innovate if you can't fiddle with it. I am against any rules that would hinder modifications in any way shape or form. I am in full support of banning modifications that break others.

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: Lyles

Mailing Address: 131 Jenna Dr Apt 210

City: Verona

Country: United States

State or Province: WI

ZIP/Postal Code: 53593

Email Address:

Organization Name:

Comment: The proposed solution is analogous to taking a sledgehammer to a colony of termites (and the walls of the house they've infested) to prevent them from destroying the house. Most or all violations of FCC regulations have not been a result of custom firmware, and this change would still not prevent the stock firmware from breaking the rules.

Furthermore, custom firmware allows for a lot of innovation. If individuals cannot install their own firmware, advances such as the fq_codel algorithm, which addresses the buffer bloat problem affecting everyone's network speeds. This is just one example; locking things down would prevent many more advances.

Please try enforcing the current regulations for stock firmware before creating new laws to try to solve the problem.

The proposed solution is analogous to taking a sledgehammer to a colony of termites (and the walls of the house they've infested) to prevent them from destroying the house. Most or all violations of FCC regulations have not been a result of custom firmware, and this change would still not prevent the stock firmware from breaking the rules.

Furthermore, custom firmware allows for a lot of innovation. If individuals cannot install their own firmware, advances such as the fq_codel algorithm, which addresses the buffer bloat problem affecting everyone's network speeds. This is just one example; locking things down would prevent many more advances.

Please try enforcing the current regulations for stock firmware before creating new laws to try to solve the problem.

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: Allen

Last Name: Biehle

Mailing Address: 22001 Latrobe Rd.

City: Plymouth

Country: United States

State or Province: CA

ZIP/Postal Code: 95669

Email Address: Allen.Biehle@gmail.com

Organization Name:

Comment: Placing limitations on modifying the firmware of a wireless device will do the following things:

1. Significantly hamper innovation. For example, many new techniques in networking came from the ability to innovate on routers, access points. One very real example are "captive portals." A captive portal is a landing page provided at nearly every coffee shop or hotel but the innovation behind it came not from a big company but from the tinkering of a handful of individuals working together on an open source project.
2. Reduce Americans competitiveness. Other countries won't put in place the same kinds of restrictions, meaning that more and more hardware purchased from those companies will be preferred. One example of huge success found from open source firmware is the wrt54g series. https://en.wikipedia.org/wiki/Linksys_WRT54G_series
3. Reduced opportunities to learn. I now work in an IT field and frequently have to refer back to knowledge I gained when tinkering with my own 20-30\$ network equipment. Forcing a change to this rule will mean that education on such kinds of technologies will have increased costs, significantly hampering the ability of self-taught engineers to compete for jobs.
4. Doing so is a slippery slope. Placing limitations on modifying the firmware of wireless devices will serve to create a slippery slope as devices converge in functionality. Already there are clocks, photo frames, and "Internet of Things" devices that provide similar functionality. By placing limits on wireless devices, we may find that somehow these rules will eventually be used to prevent everyday Americans from changing minor things about IOT devices.
5. Such kinds of limitations will be unenforceable. As America is but one of many countries, and as such kinds of devices already exist on the market, it will be impossible to "turn back the clock" on those already modified devices. Additionally, by putting such limitations on devices, only American companies selling products to America will be compelled.

My final point is that putting such kinds of limitations in place are bad policy. It will damage American competitiveness, innovation, educational opportunities, and serve as a slippery slope for misuse against the modification of other devices (watches, refrigerators, anything that will in the future have a wireless radio). The best case scenario is that this limitation will be used by manufacturers to price gauge customers with artificial software limitations to differentiate their products.

Placing limitations on modifying the firmware of a wireless device will do the following things:

1. Significantly hamper innovation. For example, many new techniques in networking came from the ability to innovate on routers, access points. One very real example are "captive portals." A captive portal is a landing page provided at nearly every coffee shop or hotel but the innovation behind it came not from a big company but from the tinkering of a

handful of individuals working together on an open source project.

2. Reduce Americans competitiveness. Other countries won't put in place the same kinds of restrictions, meaning that more and more hardware purchased from those companies will be preferred. One example of huge success found from open source firmware is the wrt54g series. https://en.wikipedia.org/wiki/Linksys_WRT54G_series

3. Reduced opportunities to learn. I now work in an IT field and frequently have to refer back to knowledge I gained when tinkering with my own 20-30\$ network equipment. Forcing a change to this rule will mean that education on such kinds of technologies will have increased costs, significantly hampering the ability of self-taught engineers to compete for jobs.

4. Doing so is a slippery slope. Placing limitations on modifying the firmware of wireless devices will serve to create a slippery slope as devices converge in functionality. Already there are clocks, photo frames, and "Internet of Things" devices that provide similar functionality. By placing limits on wireless devices, we may find that somehow these rules will eventually be used to prevent everyday Americans from changing minor things about IOT devices.

5. Such kinds of limitations will be unenforceable. As America is but one of many countries, and as such kinds of devices already exist on the market, it will be impossible to "turn back the clock" on those already modified devices. Additionally, by putting such limitations on devices, only American companies selling products to America will be compelled.

My final point is that putting such kinds of limitations in place are bad policy. It will damage American competitiveness, innovation, educational opportunities, and serve as a slippery slope for misuse against the modification of other devices (watches, refrigerators, anything that will in the future have a wireless radio). The best case scenario is that this limitation will be used by manufacturers to price gauge customers with artificial software limitations to differentiate their products.

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: Olle

Last Name: Gladso

Mailing Address: 412 High St.

City: Albert Lea

Country: United States

State or Province: MN

ZIP/Postal Code: 56007

Email Address:

Organization Name:

Comment: As a person that strongly believes in personal freedom, along with personal responsibility, I strongly object to the rules in their proposed form.

For example, if a manufacturer were to cease operation for whatever reason, should I not be allowed to update the device firmware with third-party code?

If not, the device that I own, will be rendered obsolete and unusable, due to an arbitrary rule, not due to a technical reason.

As a person that strongly believes in personal freedom, along with personal responsibility, I strongly object to the rules in their proposed form.

For example, if a manufacturer were to cease operation for whatever reason, should I not be allowed to update the device firmware with third-party code?

If not, the device that I own, will be rendered obsolete and unusable, due to an arbitrary rule, not due to a technical reason.

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: Otis

Last Name: Lewis

Mailing Address: 5141 W. Bloomingdale

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60639-4424

Email Address:

Organization Name:

Comment: I would ask that the FCC not pass a rule which prevent users from installing the software of their choosing on their own devices. I believe the freedom to tinker is important and this proposes ruling would curtail that freedom. Please do not pass this rule.

I would ask that the FCC not pass a rule which prevent users from installing the software of their choosing on their own devices. I believe the freedom to tinker is important and this proposes ruling would curtail that freedom. Please do not pass 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: James

Last Name: Donley

Mailing Address: 2504 Willow Creek

City: Jenison

Country: United States

State or Province: MI

ZIP/Postal Code: 49428

Email Address: twocows360@gmail.com

Organization Name:

Comment: This is utterly ridiculous. The only positive point is that it's nigh-unenforceable and completely ineffectual, which also means it won't solve the problem it's meant to fix (something which could be handled in other ways that I'm sure other people have already pointed out). The downshot is that it will ban many, many positive use-cases, both for hobbyists and for professionals and businesses and could cause permanent harm to the open source firmware community, which does some really great work that benefits a lot of people. I work in technology for a living and I've asked every single professional I know to weigh in, as well, as this is just patently absurd.

Speaking for me personally, I use the Tomato firmware on my home router because the official firmware hasn't been updated in somewhere around a decade (making it full of security holes) and because Tomato has additional features that I make frequent use of. I need to use Tomato to get what I want out of my device.

For instance, Tomato has a built-in SSH server that allows me to perform SSH tunneling. Without a third party firmware solution like Tomato or DD-WRT, I would either have to set up a dedicated server to handle SSH tunneling or get a high-grade commercial router with that functionality built in.

Tomato has let me make great use of a ten year old piece of hardware to do some really neat and highly useful things and many others make great use of projects like this. The proposed rule has too many negative side effects to hobbyists alone, and I'm sure businesses would also be significant harmed by the proposed rule. Come up with a better solution.

For reference, this is the specific "distribution" of Tomato that I use:

<http://toastmanfirmware.yolasite.com/>

This is utterly ridiculous. The only positive point is that it's nigh-unenforceable and completely ineffectual, which also means it won't solve the problem it's meant to fix (something which could be handled in other ways that I'm sure other people have already pointed out). The downshot is that it will ban many, many positive use-cases, both for hobbyists and for professionals and businesses and could cause permanent harm to the open source firmware community, which does some really great work that benefits a lot of people. I work in technology for a living and I've asked every single professional I know to weigh in, as well, as this is just patently absurd.

Speaking for me personally, I use the Tomato firmware on my home router because the official firmware hasn't been updated in somewhere around a decade (making it full of security holes) and because Tomato has additional features that I make frequent use of. I need to use Tomato to get what I want out of my device.

For instance, Tomato has a built-in SSH server that allows me to perform SSH tunneling. Without a third party firmware

solution like Tomato or DD-WRT, I would either have to set up a dedicated server to handle SSH tunneling or get a high-grade commercial router with that functionality built in.

Tomato has let me make great use of a ten year old piece of hardware to do some really neat and highly useful things and many others make great use of projects like this. The proposed rule has too many negative side effects to hobbyists alone, and I'm sure businesses would also be significant harmed by the proposed rule. Come up with a better solution.

For reference, this is the specific "distribution" of Tomato that I use:

<http://toastmanfirmware.yolasite.com/>

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: Dark

Last Name: Empire

Mailing Address: nevofo@postonline.me

City: Perm

Country: Russia

State or Province: Perm

ZIP/Postal Code: 614111

Email Address:

Organization Name:

Comment: I bought the device, and I will do with it what I want

I bought the device, and I will do with it what I want

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: Fabio

Last Name: Pucci

Mailing Address: fabick@cheapnet.it

City: Cosenza

Country: Italy

State or Province: Cosenza

ZIP/Postal Code: 87100

Email Address:

Organization Name:

Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *still* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks for listening.

I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

* manufacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more

lucrative use cases addressed by the manufacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however **still** possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manufactures.

Thanks 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: Andrew

Last Name: Patterson

Mailing Address: 163 Shadow Wood Court

City: Waterloo

Country: Canada

State or Province: Ontario

ZIP/Postal Code: N2K3W4

Email Address:

Organization Name:

Comment: If I understand correctly, it appears you want manufacturers to lock the software on any device containing a modular radio.

This is a terrible attempt to fix whatever issue you are trying to resolve (terrorist catching I presume?).

If these changes are put in place and enforced, a whole suite of hobbyist computing activities will be made more difficult. I say "more difficult" rather than impossible, because if these locks are enforced in the U.S. manufacture of devices, people will certainly turn to black markets where unlocked devices will be readily available. These unlocked devices will have been hacked, or simply manufactured by foreign nations.

Ultimately requiring digital locks on any device with a radio is going to be a costly endeavour with ZERO real world benefits. Please be sensible and drop this action.

If I understand correctly, it appears you want manufacturers to lock the software on any device containing a modular radio.

This is a terrible attempt to fix whatever issue you are trying to resolve (terrorist catching I presume?).

If these changes are put in place and enforced, a whole suite of hobbyist computing activities will be made more difficult. I say "more difficult" rather than impossible, because if these locks are enforced in the U.S. manufacture of devices, people will certainly turn to black markets where unlocked devices will be readily available. These unlocked devices will have been hacked, or simply manufactured by foreign nations.

Ultimately requiring digital locks on any device with a radio is going to be a costly endeavour with ZERO real world benefits. Please be sensible and drop this action.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Greg

Last Name: Smela

Mailing Address: 4740 Rt 30

City: Cornwall

Country: United States

State or Province: VT

ZIP/Postal Code: 05753

Email Address: gsmela@shoreham.net

Organization Name:

Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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

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

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

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

I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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: Kirill

Last Name: Guz

Mailing Address: Kirov str

City: Shostka

Country: Ukraine

State or Province: Sumy distr

ZIP/Postal Code: 05449

Email Address: kirgiz2465@gmail.com

Organization Name:

Comment: It's ridiculous!

It's ridiculous!

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: Staub

Mailing Address: 32 Karen Circle

City: Holliston

Country: United States

State or Province: MA

ZIP/Postal Code: 01746

Email Address:

Organization Name:

Comment: The proposed regulations regarding wireless radios are overly broad and cripplingly restrictive. In addition to preventing the development of advanced wireless technologies (eg. mesh networks) and open-source WiFi firmware (eg. OpenWrt), these regulations could be used to restrict modifications that are entirely unrelated to radio technology. Many consumer computers contain built-in WiFi chips, and therefore, are subject to these restrictions. Installing an alternate operating system on a computer with a built-in wireless chip, for example, would be illegal under this regulatory framework.

The proposed regulations regarding wireless radios are overly broad and cripplingly restrictive. In addition to preventing the development of advanced wireless technologies (eg. mesh networks) and open-source WiFi firmware (eg. OpenWrt), these regulations could be used to restrict modifications that are entirely unrelated to radio technology. Many consumer computers contain built-in WiFi chips, and therefore, are subject to these restrictions. Installing an alternate operating system on a computer with a built-in wireless chip, for example, would be illegal under this regulatory framework.

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: Woodard

Mailing Address: 2378 Woodhill Dr

City: Pittsburg

Country: United States

State or Province: CA

ZIP/Postal Code: 94565-7332

Email Address: gtfoomw@hotmail.com

Organization Name:

Comment: This rule is, almost certainly unintentionally, going to ban the updating of firmware on wireless routers. This is an obvious security issue, forcing people to remain vulnerable to known issues, and is also unnecessarily restrictive of networking power users, include most business IT administrators. You need a rewrite to make sure this normal usage is not restricted.

This rule is, almost certainly unintentionally, going to ban the updating of firmware on wireless routers. This is an obvious security issue, forcing people to remain vulnerable to known issues, and is also unnecessarily restrictive of networking power users, include most business IT administrators. You need a rewrite to make sure this normal usage is not restricted.

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: Brown

Mailing Address: 176 Palladium Ln

City: Shreveport

Country: United States

State or Province: LA

ZIP/Postal Code: 71115

Email Address:

Organization Name:

Comment: Please do not require modifications to WiFi enabled devices to lock down firmware. This will affect many devices from routers, access points, televisions, cell phones and prevent people from actually owning the products they purchase and not be able to modify them.

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.

Thank you.

Please do not require modifications to WiFi enabled devices to lock down firmware. This will affect many devices from routers, access points, televisions, cell phones and prevent people from actually owning the products they purchase and not be able to modify them.

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.

Thank you.