

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: Chris

Last Name: Hauca

Mailing Address: W5774 North Drive

City: Elkhorn

Country: United States

State or Province: WI

ZIP/Postal Code: 53121

Email Address: hauca@hotmail.com

Organization Name: US Citizen

Comment: Dear FCC,

I am troubled at the implementation of this new proposed rule. I currently leverage multiple wifi routers for my house to provide full coverage and enjoy the ability to change the firmware to an OpenSource variant to all for additional services and functionality. Specifically I can create low cost mesh networks, VPNs, and customized firewall rules that are not possible in typical vendor provided hardware for residential customers.

This rule would be a step backwards from the freedom and flexibility I currently enjoy today. It is exceptionally short sighted to assume closing down flexibility will be an improvement for the American public.

Sincerely,
Chris Hauca

Dear FCC,

I am troubled at the implementation of this new proposed rule. I currently leverage multiple wifi routers for my house to provide full coverage and enjoy the ability to change the firmware to an OpenSource variant to all for additional services and functionality. Specifically I can create low cost mesh networks, VPNs, and customized firewall rules that are not possible in typical vendor provided hardware for residential customers.

This rule would be a step backwards from the freedom and flexibility I currently enjoy today. It is exceptionally short sighted to assume closing down flexibility will be an improvement for the American public.

Sincerely,
Chris Hauca

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: Ramsey

Mailing Address: 6000 Reynolds Drive #875

City: Rochester

Country: United States

State or Province: NY

ZIP/Postal Code: 14623

Email Address:

Organization Name:

Comment: It would be a great loss to American's freedom if this rule were to be put into place. It is important to allow users to modify the software that runs on wireless devices. Manufactururs frequently neglect to patch important sercurity holes and users often wish to have fine-grained control over their own personal devices.

This could also limit the free speech of individuals who rely on modified devices to implement mesh-networks to ensure they can report on events anomouly and without fear of repercussions.

It would also cause many upcoming children to lose opportunites to learn how devices work at a low level. If they cannot modify, break, and fixed electronics, how will we, as a country, have anyone to lead us into the next era?

It would be a great loss to American's freedom if this rule were to be put into place. It is important to allow users to modify the software that runs on wireless devices. Manufactururs frequently neglect to patch important sercurity holes and users often wish to have fine-grained control over their own personal devices.

This could also limit the free speech of individuals who rely on modified devices to implement mesh-networks to ensure they can report on events anomouly and without fear of repercussions.

It would also cause many upcoming children to lose opportunites to learn how devices work at a low level. If they cannot modify, break, and fixed electronics, how will we, as a country, have anyone to lead us into the next era?

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: Fred

Last Name: Clift

Mailing Address: 352 N 470 W

City: Lindon

Country: United States

State or Province: UT

ZIP/Postal Code: 84042

Email Address: fred@clift.org

Organization Name: -

Comment: Please don't destroy the Software-Defined-Radio (SDR) community. Rules like this, while well intentioned (I think) really just limit innovation and keep people from legally controlling and using equipment they own.

By preventing people from tinkering with technology, we will end up smothering STEM-oriented youth in our nation, and will indirectly drive technological innovation outside the US.

Please don't destroy the Software-Defined-Radio (SDR) community. Rules like this, while well intentioned (I think) really just limit innovation and keep people from legally controlling and using equipment they own.

By preventing people from tinkering with technology, we will end up smothering STEM-oriented youth in our nation, and will indirectly drive technological innovation outside the US.

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: Ben

Last Name: Greear

Mailing Address: 2417 Main Street, STE 201

City: Ferndale

Country: United States

State or Province: WA

ZIP/Postal Code: 98248

Email Address: greearb@candelatech.com

Organization Name: Candela Technologies Inc

Comment: My company, Candela Technologies, makes WiFi testing equipment. We are a small company and rely on leveraging open-source software on commercially available hardware in order to make our products.

I am afraid that if DRM is used to lock down the ability to modify software on WiFi equipment then my company will no longer be able to build test equipment for this market.

In addition to this, we have found commercial equipment with FCC stamp that fails to meet some ETSI requirements. The only way we can fix this is to modify the software on the AP. If it is no longer possible to modify software on these APs, then there would be no way to fix the equipment to actually run properly with regard to regulatory constraints.

Please do NOT further restrict the ability to run custom software on WiFi equipment.

Thanks,
Ben Greear

greearb@candelatech.com
<http://www.candelatech.com>
Phone: 360-380-1618

My company, Candela Technologies, makes WiFi testing equipment. We are a small company and rely on leveraging open-source software on commercially available hardware in order to make our products.

I am afraid that if DRM is used to lock down the ability to modify software on WiFi equipment then my company will no longer be able to build test equipment for this market.

In addition to this, we have found commercial equipment with FCC stamp that fails to meet some ETSI requirements. The only way we can fix this is to modify the software on the AP. If it is no longer possible to modify software on these APs, then there would be no way to fix the equipment to actually run properly with regard to regulatory constraints.

Please do NOT further restrict the ability to run custom software on WiFi equipment.

Thanks,
Ben Greear

greearb@candelatech.com
<http://www.candelatech.com>
Phone: 360-380-1618

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: Lloyd

Last Name: Brown

Mailing Address: 196 W Pacific Dr

City: American Fork

Country: United States

State or Province: UT

ZIP/Postal Code: 84003

Email Address:

Organization Name:

Comment: While I can see some of the reasoning that the FCC is using in this proposed set of rules, I think this will have significant unintended consequences.

A large portion of the consumer switch/router device market is driven by the wide availability of third-party firmware such as OpenWRT, DD-WRT, and (my personal favorite) TomatoUSB. These open-source projects include a number of features that are not implemented by the manufacturers. These projects are also frequently much faster than the device manufacturers, to close known security holes.

I understand that this set of rules is intended to prevent a rogue piece of software from violating the rules/provisions of a specific frequency band. It is conceivable that a third-party firmware would still respect those rules and provisions, and in practice most of them do. However, the wide diversity of firmwares available would mean that there is no practical way of verifying compliance, other than by using a PKI-based software signing mechanism, probably managed by the manufacturer. In practice this means that the manufacturer, or a designated signing agent, would only sign firmware revisions available from the device manufacturer. It simply would not be technically feasible to do otherwise. This effectively would remove the ability to load those unsigned third-party firmwares.

Many manufacturers are slow to adopt security fixes in their firmwares, and most will discontinue providing updates to their devices, long before they are generally out of circulation. Given this, and the effective elimination of third-party software, these proposed rules would encourage security holes to remain unfixed in consumer devices.

The FCC already has rules and provisions that cover the type of illicit operation that these devices are technically capable of. In short, these proposed rules take an illegal act, and make it more illegal, by making it more difficult to do. But in doing so, it severely limits customer choice, effectively removes device features, and encourages devices with known security vulnerabilities (including those no longer supported by the manufacturer) to remain unfixed.

Please let the existing rules that govern the illegal behavior stand, without adding these unnecessary additional rules, with their significant side effects.

While I can see some of the reasoning that the FCC is using in this proposed set of rules, I think this will have significant unintended consequences.

A large portion of the consumer switch/router device market is driven by the wide availability of third-party firmware such as OpenWRT, DD-WRT, and (my personal favorite) TomatoUSB. These open-source projects include a number of features that are not implemented by the manufacturers. These projects are also frequently much faster than the

device manufacturers, to close known security holes.

I understand that this set of rules is intended to prevent a rogue piece of software from violating the rules/provisions of a specific frequency band. It is conceivable that a third-party firmware would still respect those rules and provisions, and in practice most of them do. However, the wide diversity of firmwares available would mean that there is no practical way of verifying compliance, other than by using a PKI-based software signing mechanism, probably managed by the manufacturer. In practice this means that the manufacturer, or a designated signing agent, would only sign firmware revisions available from the device manufacturer. It simply would not be technically feasible to do otherwise. This effectively would remove the ability to load those unsigned third-party firmwares.

Many manufacturers are slow to adopt security fixes in their firmwares, and most will discontinue providing updates to their devices, long before they are generally out of circulation. Given this, and the effective elimination of third-party software, these proposed rules would encourage security holes to remain unfixed in consumer devices.

The FCC already has rules and provisions that cover the type of illicit operation that these devices are technically capable of. In short, these proposed rules take an illegal act, and make it more illegal, by making it more difficult to do. But in doing so, it severely limits customer choice, effectively removes device features, and encourages devices with known security vulnerabilities (including those no longer supported by the manufacturer) to remain unfixed.

Please let the existing rules that govern the illegal behavior stand, without adding these unnecessary additional rules, with their significant side effects.

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: Thompson

Mailing Address: 11121 Appletree Lane

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78726

Email Address: fcc@danielthompson.net

Organization Name:

Comment: I personally use a third-party open source firmware on my home router because it has many more features than the one provided by the manufacturer. Please do not make it more difficult to do this. As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

I personally use a third-party open source firmware on my home router because it has many more features than the one provided by the manufacturer. Please do not make it more difficult to do this. As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

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: Glen

Last Name: Stewart

Mailing Address: 733 Story Dr

City: Fairfield

Country: United States

State or Province: OH

ZIP/Postal Code: 45014

Email Address: glen_stewart@associate.com

Organization Name:

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

I use this capability today on multiple computing devices, to keep the devices current/compliant/safe for interoperability and use by thousands of people all over the world, including my family. This capability keeps my devices current and useful, reducing pollution due to otherwise useless devices that would be thrown out - or worse, left in operation with vulnerabilities.

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

I use this capability today on multiple computing devices, to keep the devices current/compliant/safe for interoperability and use by thousands of people all over the world, including my family. This capability keeps my devices current and useful, reducing pollution due to otherwise useless devices that would be thrown out - or worse, left in operation with vulnerabilities.

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: Matt

Last Name: Neilsen

Mailing Address: 10904 Schoenfeld CT

City: St. Louis

Country: United States

State or Province: MO

ZIP/Postal Code: 63123

Email Address: mwneilsen+fcc+comment@gmail.com

Organization Name:

Comment: I use OpenWRT on my PERSONAL HOME wifi equipment. I do this to get better performance and longer life out of some older equipment. The OpenWRT firmware help to make the older hardware more stable with its superior error handling and coding. I see no reason to take this option from consumers who have PURCHASED the hardware for their PERSONAL HOME use.

I use OpenWRT on my PERSONAL HOME wifi equipment. I do this to get better performance and longer life out of some older equipment. The OpenWRT firmware help to make the older hardware more stable with its superior error handling and coding. I see no reason to take this option from consumers who have PURCHASED the hardware for their PERSONAL HOME use.

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: Trevor

Last Name: Lee

Mailing Address: 19655 clubhouse drive

City: Denver

Country: United States

State or Province: CO

ZIP/Postal Code: 80138

Email Address:

Organization Name:

Comment: Due to the high level of integration of components in modern hardware, I am very concerned that this proposal will have unintended consequences for consumers who wish exercise some control over the devices they own.

Due to the high level of integration of components in modern hardware, I am very concerned that this proposal will have unintended consequences for consumers who wish exercise some control over the 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: Joshua

Last Name: Urbain

Mailing Address: 216 S Chapman St

City: Chesaning

Country: United States

State or Province: MI

ZIP/Postal Code: 48616

Email Address: null

Organization Name: null

Comment: Thank you for the opportunity to listen to the community. As a Computer Scientist, I am concerned about the ruling on software being installed in wireless hardware. Wireless networking research is what keeps our community thriving on innovation and security at their peaks. It has been proven in the past that hardware vendors do not have the security patch turnover that many of these third-parties provide. Also, this reduction of sources will provide hackers to have a much easier time to focus their attention on a single firmware source.

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

Thank you for your time, please consider the above when making your decision.

Thank you for the opportunity to listen to the community. As a Computer Scientist, I am concerned about the ruling on software being installed in wireless hardware. Wireless networking research is what keeps our community thriving on innovation and security at their peaks. It has been proven in the past that hardware vendors do not have the security patch turnover that many of these third-parties provide. Also, this reduction of sources will provide hackers to have a much easier time to focus their attention on a single firmware source.

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

Thank you for your time, please consider the above when making your decision.

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: Darren

Last Name: Jones

Mailing Address: 1022 Ringwood Road

City: Bournemouth

Country: United Kingdom

State or Province: Dorset

ZIP/Postal Code: BH11 9LA

Email Address: djaychela@gmail.com

Organization Name:

Comment: While I live outside the US, this concerns me, as there will clearly be a knock-on effect on products sold worldwide (as they increasingly are) which would be effected by this ruling. To stop modification of consumer items such as WiFi routers would mean many of the security and safety settings I take for granted every day would no longer be available to me. This isn't merely a case of "hacking", such firmware provides me with the tools I need to help keep my children safe while on the Internet - not something which a standard WiFi router does.

In addition, such an act would remove the ability for people to innovate in this field. Yes, of course, regulations need to be in place to maintain the control of the airwaves, but this regulation is merely a case of unintended consequences in terms of consumer electronic devices. Stifling innovation will hamstring everyone who is involved in this market segment, and to do so without thinking of this (which I charitably am assuming must be the case) would be foolish at best.

As I have already said, I live outside the US, but it is probably the largest market for this kind of device worldwide, and manufacturers would probably take the path of least resistance and make it impossible to alter routers sold in Europe - this is the weight of responsibility that the FCC must bear in its position as the leading global regulator on these matters.

While I live outside the US, this concerns me, as there will clearly be a knock-on effect on products sold worldwide (as they increasingly are) which would be effected by this ruling. To stop modification of consumer items such as WiFi routers would mean many of the security and safety settings I take for granted every day would no longer be available to me. This isn't merely a case of "hacking", such firmware provides me with the tools I need to help keep my children safe while on the Internet - not something which a standard WiFi router does.

In addition, such an act would remove the ability for people to innovate in this field. Yes, of course, regulations need to be in place to maintain the control of the airwaves, but this regulation is merely a case of unintended consequences in terms of consumer electronic devices. Stifling innovation will hamstring everyone who is involved in this market segment, and to do so without thinking of this (which I charitably am assuming must be the case) would be foolish at best.

As I have already said, I live outside the US, but it is probably the largest market for this kind of device worldwide, and manufacturers would probably take the path of least resistance and make it impossible to alter routers sold in Europe - this is the weight of responsibility that the FCC must bear in its position as the leading global regulator on these matters.

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: Gervais

Mailing Address: 1398, rue de l'Oural

City: Quebec City

Country: Canada

State or Province: Quebec

ZIP/Postal Code: G1C 7Y6

Email Address: jgervais@gmail.com

Organization Name:

Comment: To whom it may concern,

I highly oppose this regulation proposal, since it will impact security, liberty of choice and technology advancements. By imposing this regulation FCC will not only impact U.S. citizen but their neighbors and eventually the entire world.

Thanks

Jonathan Gervais

To whom it may concern,

I highly oppose this regulation proposal, since it will impact security, liberty of choice and technology advancements. By imposing this regulation FCC will not only impact U.S. citizen but their neighbors and eventually the entire world.

Thanks

Jonathan Gervais

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: Magnus

Last Name: Kwan

Mailing Address: 1735 Tyler Drive

City: Monterey Park

Country: United States

State or Province: CA

ZIP/Postal Code: 91755

Email Address:

Organization Name:

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

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

Please do not implement rules that take away my ability to install the software of my choosing on my 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: Jason

Last Name: Merriam

Mailing Address: 121 E 17th St

City: Pittsburg

Country: United States

State or Province: CA

ZIP/Postal Code: 94565

Email Address:

Organization Name:

Comment: There is a way to provide protection to protected frequencies without destroying the freedom to choose and modify the software running on personally owned equipment. I sincerely suggest you look for it. If nothing else, Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

There is a way to provide protection to protected frequencies without destroying the freedom to choose and modify the software running on personally owned equipment. I sincerely suggest you look for it. If nothing else, Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

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: Ron

Last Name: Light

Mailing Address: 520 W 103rd St

City: Kansas City

Country: United States

State or Province: MO

ZIP/Postal Code: 64114

Email Address: Ron@RonLight.com

Organization Name: Bright Light Investments LLC

Comment: Please do not implement this rule. Doing so will take away the ability of users to install the software of their choosing on their computing devices. As a specific example I am able to take a cheap router and install a secure, reliable firmware such as dd-wrt or tomato.

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

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

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

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

Please do not implement this rule. Doing so will take away the ability of users to install the software of their choosing on their computing devices. As a specific example I am able to take a cheap router and install a secure, reliable firmware such as dd-wrt or tomato.

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: Justin

Last Name: Rosko

Mailing Address: 7824 Hampton Forest Lane

City: Chesterfield

Country: United States

State or Province: VA

ZIP/Postal Code: 23832

Email Address: rosjustinm@yahoo.com

Organization Name:

Comment: This ruling would have an adverse impact on economically disadvantaged people.

Currently the ability to modify firmware in a multitude of cellular phones, wifi routers and other electronic devices allows individuals to optimize the behavior of these devices and thus extend their useful life significantly. I personally use 3 routers at home running open-source firmware that turned significantly outdated wireless b/g routers in to reasonably well performing network adapters and extenders at near N speeds. All without modification to the Wifi radios output strength.

I have also provided similar modified devices for friends and family to help them get more out of their once top of the line devices, without having to spend a hundred dollars or more on a new device with equivalent performance.

If the proposed rule were to go in to effect, this equipment could not be up-cycled and would not be able to meet current needs, likely resulting in it being discarded.

This ruling would have an adverse impact on economically disadvantaged people.

Currently the ability to modify firmware in a multitude of cellular phones, wifi routers and other electronic devices allows individuals to optimize the behavior of these devices and thus extend their useful life significantly. I personally use 3 routers at home running open-source firmware that turned significantly outdated wireless b/g routers in to reasonably well performing network adapters and extenders at near N speeds. All without modification to the Wifi radios output strength.

I have also provided similar modified devices for friends and family to help them get more out of their once top of the line devices, without having to spend a hundred dollars or more on a new device with equivalent performance.

If the proposed rule were to go in to effect, this equipment could not be up-cycled and would not be able to meet current needs, likely resulting in it being discarded.

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: Justin

Last Name: Cole

Mailing Address: 108 oakview ave.

City: Pittsburgh

Country: United States

State or Province: PA

ZIP/Postal Code: 15218

Email Address: justincole01@gmail.com

Organization Name:

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

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

Thank you

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

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

Thank you

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Jones

Mailing Address: 100 cashew ct

City: longwood

Country: United States

State or Province: FL

ZIP/Postal Code: 32750

Email Address: cjflow@hotmail.com

Organization Name:

Comment: I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

My reasons for this include but are not limited to:

- 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 am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

My reasons for this include but are not limited to:

- 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: Jesse

Last Name: Robinson

Mailing Address: 2343 Clover Ln

City: Janesville

Country: United States

State or Province: WI

ZIP/Postal Code: 53545

Email Address: colecago@gmail.com

Organization Name:

Comment: This isn't a good idea. Ever since the WRT54GL router line was released, custom Linux firmware has been a mainstay of those who need more configuration or power over their home network. In fact there are several routers out there whose sole purpose is running modified firmware.

My stock firmware doesn't offer bandwidth monitoring, and when ATT started limited their unlimited service, I had to put tomato on my router to have my own records to keep them honest, especially since I cannot see my usage on their website even all these years after they've implemented this rule (there has to be rules broken on that front, but whatever).

So please don't kill the open source router firmware community and force power users into crappy limited options or \$1k+ systems because of an old way of thinking.

This isn't a good idea. Ever since the WRT54GL router line was released, custom Linux firmware has been a mainstay of those who need more configuration or power over their home network. In fact there are several routers out there whose sole purpose is running modified firmware.

My stock firmware doesn't offer bandwidth monitoring, and when ATT started limited their unlimited service, I had to put tomato on my router to have my own records to keep them honest, especially since I cannot see my usage on their website even all these years after they've implemented this rule (there has to be rules broken on that front, but whatever).

So please don't kill the open source router firmware community and force power users into crappy limited options or \$1k+ systems because of an old way of thinking.

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: Jeff

Last Name: Monahan

Mailing Address: P.O. Box 192

City: Dayton

Country: United States

State or Province: OR

ZIP/Postal Code: 97114

Email Address: jeff@oregon.com

Organization Name:

Comment: To whom it may concern,

I am a user of many older routers that have been updated with open source software because the original manufacture of the device doesnt support it.

The open source software requires the firmware on that device to be flashed or upgraded in order to keep it current and to give me more control and security.

Please do not allow this restriction to be put in place.

Thank you for reading this.

To whom it may concern,

I am a user of many older routers that have been updated with open source software because the original manufacture of the device doesnt support it.

The open source software requires the firmware on that device to be flashed or upgraded in order to keep it current and to give me more control and security.

Please do not allow this restriction to be put in place.

Thank you for reading this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matt

Last Name: Poindexter

Mailing Address: 17243 E Lakeview Dr

City: Mayer

Country: United States

State or Province: AZ

ZIP/Postal Code: 86333

Email Address: mw@chiefpoints.com

Organization Name: Revolutionized Computing

Comment: I respectfully ask that the FCC not implement rules that take away the ability of users to install software of their choosing on their computing devices. While I'm sure the FCC has the best of intentions, this rule will severely limit the ability of users to secure their devices and optimize their operation.

Security researchers routinely work with device firmware to enhance protection and security for all users. This rule change will severely limit their ability to protect consumers. One only has to look at the current statistics on home and SOHO router vulnerabilities that constantly being found and corrected thanks to these researchers. End users run router firmware such as WRT to help close these gaping holes and to enable the devices to operate better in electronically polluted environments. This rule change will put an end to all of that.

The only entities that will benefit from this rule are the mobile communications providers that are trying to expand their wireless connectivity into the 5ghz spectrum in an attempt to monetize it's use. Consumers will be the definite losers here. Please do not cripple our ability to utilize hardware we privately own in the most secure and efficient manner possible.

I respectfully ask that the FCC not implement rules that take away the ability of users to install software of their choosing on their computing devices. While I'm sure the FCC has the best of intentions, this rule will severely limit the ability of users to secure their devices and optimize their operation.

Security researchers routinely work with device firmware to enhance protection and security for all users. This rule change will severely limit their ability to protect consumers. One only has to look at the current statistics on home and SOHO router vulnerabilities that constantly being found and corrected thanks to these researchers. End users run router firmware such as WRT to help close these gaping holes and to enable the devices to operate better in electronically polluted environments. This rule change will put an end to all of that.

The only entities that will benefit from this rule are the mobile communications providers that are trying to expand their wireless connectivity into the 5ghz spectrum in an attempt to monetize it's use. Consumers will be the definite losers here. Please do not cripple our ability to utilize hardware we privately own in the most secure and efficient manner 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: Brian

Last Name: Livermore

Mailing Address: 4408 W Kogel Dr

City: Sioux Falls

Country: United States

State or Province: SD

ZIP/Postal Code: 57107

Email Address: livermob@gmail.com

Organization Name:

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

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

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Hunt

Mailing Address: 107 30th Ave E

City: Tuscaloosa

Country: United States

State or Province: AL

ZIP/Postal Code: 35404

Email Address: ttg@cpan.org

Organization Name:

Comment: I would like to respectfully request that this rule be amended to maintain the ability of the private citizen to install software of their choice on computing devices. The modification of routing computer devices is a driving factor in the development of new technologies, and also has historically been a great security advantage for this country. Some of the original Internet of Things prototypes would have been impossible without modified router software. In Addition, many times, companies are sluggish about responding to security vulnerabilities. Custom firmware installation gives the power to the consumer to protect their own security. I understand the concerns of radio devices running custom software, but I would respectfully submit that the advantages in development, security, and most importantly the freedom of the American consumer, far outweigh the potential disadvantages.

I would like to respectfully request that this rule be amended to maintain the ability of the private citizen to install software of their choice on computing devices. The modification of routing computer devices is a driving factor in the development of new technologies, and also has historically been a great security advantage for this country. Some of the original Internet of Things prototypes would have been impossible without modified router software. In Addition, many times, companies are sluggish about responding to security vulnerabilities. Custom firmware installation gives the power to the consumer to protect their own security. I understand the concerns of radio devices running custom software, but I would respectfully submit that the advantages in development, security, and most importantly the freedom of the American consumer, far outweigh the potential disadvantages.

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: Mason

Mailing Address: 5123 SE 40th Ave

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97202

Email Address: cmason@cmason.com

Organization Name:

Comment: I respectfully request that you not implement rules that prevent end users from modifying the software or firmware on wireless computing devices.

Choice and innovation are crucial to the safety and utility of the open internet. By allowing users a choice of both proprietary and open source software and firmware on the critical components that back the internet, you enable innovation and protect this valuable infrastructure.

This ability to choose and modify software/firmware allows researchers to innovate via research into:

- * advanced networking mesh topologies that extend the reach of the internet to every device,
- * flexible, reconfigurable devices that make best use of limited battery power,
- * security techniques and investigations that interact directly with wireless hardware.

By allowing a choice of open source drivers and firmware for wireless devices such as routers, you enable many more "eyes" to protect critical e-commerce infrastructure. Open source developers can and do find and fix critical vulnerabilities in proprietary wireless drivers and firmware. Moreover, open source firmware such as DD-WRT for wireless routers innovate faster than proprietary vendors and provide dramatically more features and security. By prohibiting users such as me from installing such firmware, you limit the choice I have in maintaining my network and fine tuning my access to the internet.

It's true that, by allowing modification to software and firmware on wireless devices, it's possible that users may exceed certification limits or generate undesirable interference. However, there are already existing enforcement regimes available for protecting against such eventualities. Moreover, it is possible to design hardware that, for instance, separately limits maximum transmit power, without a blanket prohibition against any firmware modifications.

In summary, while it's important that the FCC protect the open airwaves, it should not remove critical choice that exists today to the expense of future innovation.

Thank you for listening.

I respectfully request that you not implement rules that prevent end users from modifying the software or firmware on wireless computing devices.

Choice and innovation are crucial to the safety and utility of the open internet. By allowing users a choice of both

proprietary and open source software and firmware on the critical components that back the internet, you enable innovation and protect this valuable infrastructure.

This ability to choose and modify software/firmware allows researchers to innovate via research into:

- * advanced networking mesh topologies that extend the reach of the internet to every device,
- * flexible, reconfigurable devices that make best use of limited battery power,
- * security techniques and investigations that interact directly with wireless hardware.

By allowing a choice of open source drivers and firmware for wireless devices such as routers, you enable many more "eyes" to protect critical e-commerce infrastructure. Open source developers can and do find and fix critical vulnerabilities in proprietary wireless drivers and firmware. Moreover, open source firmware such as DD-WRT for wireless routers innovate faster than proprietary vendors and provide dramatically more features and security. By prohibiting users such as me from installing such firmware, you limit the choice I have in maintaining my network and fine tuning my access to the internet.

It's true that, by allowing modification to software and firmware on wireless devices, it's possible that users may exceed certification limits or generate undesirable interference. However, there are already existing enforcement regimes available for protecting against such eventualities. Moreover, it is possible to design hardware that, for instance, separately limits maximum transmit power, without a blanket prohibition against any firmware modifications.

In summary, while it's important that the FCC protect the open airwaves, it should not remove critical choice that exists today to the expense of future innovation.

Thank you for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: George

Last Name: Cash

Mailing Address: 8726 Bexar Dr

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77064

Email Address: hextejas@fastmail.com

Organization Name: None

Comment: I respectfully ask the FCC to not implement rules that take away my ability to install software of my choosing on my computing devices. Wireless networking research is of great interest to me and I need to be able to investigate and modify my devices.- I have found a need to override the default settings in my devices when the manufacturer chooses to not do so.

I respectfully ask the FCC to not implement rules that take away my ability to install software of my choosing on my computing devices. Wireless networking research is of great interest to me and I need to be able to investigate and modify my devices.- I have found a need to override the default settings in my devices when the manufacturer chooses to not do so.

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: Nadeau

Mailing Address: 29 Short St Apt 1

City: Vergennes

Country: United States

State or Province: VT

ZIP/Postal Code: 05491

Email Address:

Organization Name:

Comment: Do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I own the hardware, I should be able to run whatever software on it that I want. If I own something, I should be able to do what I want with it. You've ruled similarly on cell phones...

I'm a computer programmer and removing this ability would be the same as not allowing home mechanics to change their own oil or fix their own car.

This regulation will not be effective and will not result in any improvement to consumers.

Do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I own the hardware, I should be able to run whatever software on it that I want. If I own something, I should be able to do what I want with it. You've ruled similarly on cell phones...

I'm a computer programmer and removing this ability would be the same as not allowing home mechanics to change their own oil or fix their own car.

This regulation will not be effective and will not result in any improvement to consumers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Radu

Last Name: Motisan

Mailing Address: Timisoara

City: Timisoara

Country: Romania

State or Province: Timis

ZIP/Postal Code: 300414

Email Address: radhoo.tech@gmail.com

Organization Name: n/a

Comment: Rules can help to keep society organised, but there are cases when the very same rules become obstacles to new things that just can't follow the strict guidelines.

Innovation is a black box, we never know on what path the progress gets out, so we need to keep a balance on what we say no to.

Connectivity has this type of potential and the late progress on WLAN modules has boosted the community of makers including the small companies creating innovative products. All these sector rely on getting to the bottom levels of hardware and software to find new ideas and create new value, and this sometimes may include using a WLAN module for completely other things then it was designed for. Just to enumerate a few applications, there are indoor position systems or parallel data transmission links for increased speed.

I don't think it is right to put an end to this direction, by banning custom firmware/radio firmware on WLAN modules. Hardware and software are tools, and we should be free to exploit them to the very last bit, if it is to help creativity move forward even a small step.

Rules can help to keep society organised, but there are cases when the very same rules become obstacles to new things that just can't follow the strict guidelines.

Innovation is a black box, we never know on what path the progress gets out, so we need to keep a balance on what we say no to.

Connectivity has this type of potential and the late progress on WLAN modules has boosted the community of makers including the small companies creating innovative products. All these sector rely on getting to the bottom levels of hardware and software to find new ideas and create new value, and this sometimes may include using a WLAN module for completely other things then it was designed for. Just to enumerate a few applications, there are indoor position systems or parallel data transmission links for increased speed.

I don't think it is right to put an end to this direction, by banning custom firmware/radio firmware on WLAN modules. Hardware and software are tools, and we should be free to exploit them to the very last bit, if it is to help creativity move forward even a small step.

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: Ethan

Last Name: Joyce

Mailing Address: Erhan Joyce, 24 Dumbarton Place, St. John's Newfoundland A1A5X6, Canada

City: St. John's

Country: Canada

State or Province: Newfoundland

ZIP/Postal Code: A1A5X6

Email Address:

Organization Name:

Comment: I believe that it's important to give users control over their tools, not vise-versa. Please don't lock down RF electronics.

Removing the right to control how our electronics perform wireless networking tasks has many ramifications:

First off, we will face security problems. Many people choose to use Free (as in free speech) drivers for ethical and security reasons. These are drivers that anyone can run, study, modify, and redistribute verbatim or modified. Free drivers are inherently more secure than the non-Free/proprietary, locked down drivers that vendors distribute. Since anyone can study how a Free driver works and make changes to it, people ranging from hobbieists to security professionals are all able to fix security bugs before they're discovered by malicious crackers. Many vendors ignore bugs, which leads to a higher risk of being compromised, and users are unable to legally fix them themselves, despite the fact that it would be a very difficult task. Forcing vendors to lock down their RF devices hurts the security of computer users.

Secondly, both students and researchers will be set back. Researchers need to be able to control how their RF devices work in order to do what they do. Likewise, students will have yet another obstacle in their studies about RF devices. We want to foster interest, and thus development of RF devices, not obstruct it. By locking down these devices people will no longer be able to learn about how they work. Forcing vendors to lock down their RF devices hurts the development of RF technologies.

Thirdly, it's unethical. Computers are tools, and tools should help their users, not fight them. What would the carpentry situation be if hammers prevented their users from nailing in nails that a company doesn't like? The user should have the final say over how their computer works, not a company. People will still find ways to do illegal things, so it's better to protect the good than to destroy it all along with a small bit of bad. For the loss compared to gain, it's definitely not worth it. Forcing vendors to lock down their RF devices isn't worth the loss.

Those were three reasons why this would be wrong. Of course, there are plenty of other problems with locking down RF devices as well. Please do not destroy the control that we have over our RF devices.

I believe that it's important to give users control over their tools, not vise-versa. Please don't lock down RF electronics.

Removing the right to control how our electronics perform wireless networking tasks has many ramifications:

First off, we will face security problems. Many people choose to use Free (as in free speech) drivers for ethical and

security reasons. These are drivers that anyone can run, study, modify, and redistribute verbatim or modified. Free drivers are inherently more secure than the non-Free/proprietary, locked down drivers that vendors distribute. Since anyone can study how a Free driver works and make changes to it, people ranging from hobbyists to security professionals are all able to fix security bugs before they're discovered by malicious crackers. Many vendors ignore bugs, which leads to a higher risk of being compromised, and users are unable to legally fix them themselves, despite the fact that it would be a very difficult task. Forcing vendors to lock down their RF devices hurts the security of computer users.

Secondly, both students and researchers will be set back. Researchers need to be able to control how their RF devices work in order to do what they do. Likewise, students will have yet another obstacle in their studies about RF devices. We want to foster interest, and thus development of RF devices, not obstruct it. By locking down these devices people will no longer be able to learn about how they work. Forcing vendors to lock down their RF devices hurts the development of RF technologies.

Thirdly, it's unethical. Computers are tools, and tools should help their users, not fight them. What would the carpentry situation be if hammers prevented their users from nailing in nails that a company doesn't like? The user should have the final say over how their computer works, not a company. People will still find ways to do illegal things, so it's better to protect the good than to destroy it all along with a small bit of bad. For the loss compared to gain, it's definitely not worth it. Forcing vendors to lock down their RF devices isn't worth the loss.

Those were three reasons why this would be wrong. Of course, there are plenty of other problems with locking down RF devices as well. Please do not destroy the control that we have over our RF devices.

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: Jeff

Last Name: Whitney

Mailing Address: 4850s 4900w

City: Slc

Country: United States

State or Province: UT

ZIP/Postal Code: 84118

Email Address:

Organization Name:

Comment: People need to be able to modify any aspect of any hardware or software they rightfully purchased. Enough restrictions.

People need to be able to modify any aspect of any hardware or software they rightfully purchased. Enough restrictions.

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: Aled

Last Name: Cuda

Mailing Address: 7653 hillrose st

City: Tujunga

Country: United States

State or Province: CA

ZIP/Postal Code: 91042

Email Address: aledvirgil@gmail.com

Organization Name:

Comment: In modern times nearly every device we have is connected with every other through the internet, and most of that happens over wifi, and mobile networks. Along with this trend there has also been one to move towards more integrated systems, often storing firmware and software inseparably in one package for one specific embedded device. This presents an issue because the people who design the devices, and write software for them are generally incompetent or just don't care. This has led to many security issues especially in routers, that are simple to exploit and often never get fixed. If a router is breached then anyone anywhere with the right knowledge can listen to your webtraffic, capture it and change it potentially releasing a hoard of private data like credit card numbers, passwords, and emails. This however is not the worst of it, because beyond that it leaves the computer that is normally protected by NAT wide open to attack. The small, but incredibly talented community that has built up around these devices routinely finds these issues and fixes them, and many among them develop their own more capable, and more secure pieces of firmware that are used by private individuals and small businesses alike to secure and improve their networks. Unfortunately none of this would be possible without the right to modify the firmware of these devices. This however does not completely cover the issue, because embedded devices are not the only places where custom wireless firmware is common, because many operating systems load their own firmware at boot time so that they can communicate so the issue with wireless firmware is not limited to embedded devices it extends to laptops and desktops alike. The most common example of this aftermarket firmware is the operating system Linux, this operating system drives everything from the ISS (by the way all the laptops on the ISS use Linux and have wifi which means they use custom firmware and this frames the issue of security in standard, because when they used Windows they got a worm) to the LHC to our tanks and ships over seas. This is an operating system that was created by a hobiist who instead of being content with what he had, decided to turn it into something more and in an atmosphere like the one this bill proposes, that kind of innovation would be illegal because to create a successful operating system he would have to create his own third party wireless firmware. A large portion of the technological innovation that happens in this country happens because of hobiists who experiment and by passing this regulation you make that innovation illegal. Finally this could easily infringe on the Title 47, Section 19 rights of ham radio operators because most of these devices operate secondarily on the ISM bands on which Hams are usually primary, and under section 19 Ham radio operators are allowed to modify radios for their use as long as they comply with the restrictions on bandwidth, frequency, and transmit power (among others) that the FCC puts in place. This legislation effectively violates that right by removing their ability to modify radios which they routinely do.

In modern times nearly every device we have is connected with every other through the internet, and most of that happens over wifi, and mobile networks. Along with this trend there has also been one to move towards more integrated systems, often storing firmware and software inseparably in one package for one specific embedded device. This presents an issue because the people who design the devices, and write software for them are generally incompetent or just don't care. This has led to many security issues especially in routers, that are simple to exploit and often never get fixed. If a router is breached then anyone anywhere with the right knowledge can listen to your webtraffic, capture it and change it

potentially releasing a hord of private data like credit card numbers, passwords, and emails. This however is not the worst of it, because beyond that it leaves the computer that is normally protected by NAT wide open to attack. The small, but incredibly talented community that has built up around these devices routinely finds these issues and fixes them, and many among them develop their own more capable, and more secure pieces of firmware that are used by private individuals and small businesses alike to secure and improve their networks. Unfortunately none of this would be possible without the right to modify the firmware of these devices. This however does not completely cover the issue, because embedded devices are not the only places where custom wireless firmware is common, because many operating systems load their own firmware at boot time so that they can communicate so the issue with wireless firmware is not limited to embedded devices it extends to laptops and desktops alike. The most common example of this aftermarket firmware is the operating system Linux, this operating system drives everything from the ISS (by the way all the laptops on the ISS use Linux and have wifi which means they use custom firmware and this frames the issue of security in standard, because when they used Windows they got a worm) to the LHC to our tanks and ships over seas. This is an operating system that was created by a hobiist who instead of being content with what he had, decided to turn it into something more and in an atmosphere like the one this bill proposes, that kind of innovation would be illegal because to create a successful operating system he would have to create his own third party wireless firmware. A large portion of the technological innovation that happens in this country happens because of hobiests who experiment and by passing this regulation you make that innovation illegal. Finally this could easilly infringe on the Title 47, Section 19 rights of ham radio operators because most of these devices operate secondarily on the ISM bands on which Hams are usually primary, and under section 19 Ham radio operators are allowed to modify radios for their use as long as they comply with the restrictions on bandwidth, frequency, and transmit power (among others) that the Fcc puts in place. This legislation effectively violates that right by removing their ability to modify radios which they routinely do.

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: Allshouse

Mailing Address: 201 Fiddlers Elbow Rd.

City: Middletown

Country: United States

State or Province: PA

ZIP/Postal Code: 17057-2912

Email Address: m.allshouse@gmail.com

Organization Name:

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

There is simply no god reason for implementing these unnecessarily restrictive regulations. Please reconsider. Thank you.

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

There is simply no god reason for implementing these unnecessarily restrictive regulations. Please reconsider. Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd apt 10c

City: Miami Springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Collette

Mailing Address: 36 Windswept Way

City: Coventry

Country: United States

State or Province: CT

ZIP/Postal Code: 06488

Email Address: rcollette@yahoo.com

Organization Name:

Comment: I respectfully request that the FCC does not pass this rule. For years amateur radio operators have been providing useful, free, disaster services using modified wifi routers, such as in Haiti. This rule bans this use case, stifles innovation and prevents amateur radio operators from operating legally on channels they are authorized to use.

I respectfully request that the FCC does not pass this rule. For years amateur radio operators have been providing useful, free, disaster services using modified wifi routers, such as in Haiti. This rule bans this use case, stifles innovation and prevents amateur radio operators from operating legally on channels they are authorized to use.

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: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd

City: miami springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd

City: miami springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Jose

Last Name: Mendoza

Mailing Address: 375 south royal poinciana blvd

City: miami springs

Country: United States

State or Province: FL

ZIP/Postal Code: 33166

Email Address: joedoe47@gmail.com

Organization Name: null

Comment: the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

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

I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

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

We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

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

As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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.

personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

the FCC should allow WIFI standards to remain as open as possible. You are requiring manufactures to "lock down" devices however there is a much impact that will have as follows.

*Wireless networking research depends on the ability of researchers to investigate and modify their devices. I am not very familiar with R&D; however, we all know the scientific process. People who are doing R&D need to be able to debug and change parameters that would allow them to do their jobs. Having binaries that they can not edit, audit, or replace with their own, would prevent them from doing their job and perhaps bettering wifi.

*Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. We all know manufactures like to keep things at cost, as such things like security updates are sometimes held back, due to distributing patches and cost required to actually find and fix these critical bugs. As such we as individuals and as employees that support critical company infrastructure may need to be able to put in our own firmware and patches to ensure the security of our networks. Having manufactures take care of security will only make it difficult for individuals and enterprises to pick up the slack, so to speak.

*Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. As you may or not be aware, individuals in the FOSS community have solved very big problems when they have actually been allowed access to audit and contribute to code for wifi drivers, graphic drivers, etc. By leaving up to the manufacture, you are doing to make it possibly difficult for passionate users that want to contribute to your technology and thus, you will lose these resources.

*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. personally, I like to use hardware where I can load DDWRT on the router. I can also think of two companies that are using their own software to provide service to their users. We would likely have to either find alternatives or see how much we would have to pay, just to have the feature to adapt our own binaries/firmware. Personally I would be willing to pay a little extra to have the ability to have my own binaries; although I am not sure of these two companies, I don't represent them in anyway.

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: Larry

Last Name: Boles

Mailing Address: 100 NE 6TH AVE 223

City: HOMESTEAD

Country: United States

State or Province: FL

ZIP/Postal Code: 33030

Email Address: GIVEROFDOOM@COMCAST.NET

Organization Name:

Comment: I am totally against this new rule. We have enough government regulations controlling Armature Radio, and digital based communications. There is no benefit to anyone with these new rules other then to regulate the people.

I do understand as members of a commission your jobs are to create rules and regulations. Every once in a while the rules and regulations are a benefit to us all. All to often like these new proposed rules the only benefit is to the government and more control over the people.

How about you guys leave this one alone and spend a good day on the golf course?

Sincerely,

Larry A Boles

KM4KPU

I am totally against this new rule. We have enough government regulations controlling Armature Radio, and digital based communications. There is no benefit to anyone with these new rules other then to regulate the people.

I do understand as members of a commission your jobs are to create rules and regulations. Every once in a while the rules and regulations are a benefit to us all. All to often like these new proposed rules the only benefit is to the government and more control over the people.

How about you guys leave this one alone and spend a good day on the golf course?

Sincerely,

Larry A Boles

KM4KPU

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: Phil

Last Name: Heid

Mailing Address: 227 Main Street

City: North Creek

Country: United States

State or Province: NY

ZIP/Postal Code: 12853

Email Address: philphun@gmail.com

Organization Name: null

Comment: This bad for people and slows innovation and advance of technology. People bought and own these devices. They should be free to do anything they want with them that doesn't harm or interfere with other people.

This bad for people and slows innovation and advance of technology. People bought and own these devices. They should be free to do anything they want with them that doesn't harm or interfere with other 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: Moon

Last Name: Quddus

Mailing Address: 16 Pomeroy Street

City: Cardiff

Country: United Kingdom

State or Province: South Glamorgan

ZIP/Postal Code: CF10 5GS

Email Address: moonquddus@gmail.com

Organization Name: null

Comment: This is the worst idea I've ever heard. I have a WiFi adapter on my PC, and I would hate to have it locked down; unable to install any other OS. Aren't regulations meant to prevent things like monopolies? Why are you handing one to Microsoft on a silver platter?

This is the worst idea I've ever heard. I have a WiFi adapter on my PC, and I would hate to have it locked down; unable to install any other OS. Aren't regulations meant to prevent things like monopolies? Why are you handing one to Microsoft on a silver platter?

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: Shaun

Last Name: Reich

Mailing Address: 459 Bernhardt Dr

City: Buffalo

Country: United States

State or Province: NY

ZIP/Postal Code: 14226

Email Address: Sreich02@gmail.com

Organization Name: null

Comment: This is an absolutely terrible step backwards. When I buy hardware , I deserve to be able to modify it as I see fit. Locking these systems down just results in a worse experience for everyone. It also stifles competition. Eg openwrt and dd-wrt, two of the most common roms for routers, have had a feature set such that it has forced routers from large companies to incorporate such necessary features.

I'm allowed to work on my car, I should always be allowed to work on my electronics.

Additionally, this is even worse of an idea these r recent years and onto the future, where routers and software all over the world are getting exploits weekly.. We need to be able to patch these ourselves.

This is an absolutely terrible step backwards. When I buy hardware , I deserve to be able to modify it as I see fit. Locking these systems down just results in a worse experience for everyone. It also stifles competition. Eg openwrt and dd-wrt, two of the most common roms for routers, have had a feature set such that it has forced routers from large companies to incorporate such necessary features.

I'm allowed to work on my car, I should always be allowed to work on my electronics.

Additionally, this is even worse of an idea these r recent years and onto the future, where routers and software all over the world are getting exploits weekly.. We need to be able to patch these ourselves.

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: M

Last Name: Corish

Mailing Address: 1 Queen street

City: Charlottetown

Country: Canada

State or Province: Prince Edward Island

ZIP/Postal Code: C1a4h4

Email Address: null

Organization Name: null

Comment: Regulations lime this will be of no help, other than to hinder the ability for people to be able to innovate, explore and improve devices. Having no ability to flash a custom ROM for an android phone, or being able to install a UNIX/Linux operating system also hinders work in areas such as computer science, and development of applications in general.

Please understand the ramifications of doing something like this affects no one else other than those with the ability to help innovate.

Regulations lime this will be of no help, other than to hinder the ability for people to be able to innovate, explore and improve devices. Having no ability to flash a custom ROM for an android phone, or being able to install a UNIX/Linux operating system also hinders work in areas such as computer science, and development of applications in general.

Please understand the ramifications of doing something like this affects no one else other than those with the ability to help innovate.