

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: PAul

Last Name: Gupta

Mailing Address: 14081 big crest ln #004

City: woodbridge

Country: United States

State or Province: VA

ZIP/Postal Code: 22191

Email Address: paul.n.gupta@gmail.com

Organization Name:

Comment: Do not restrict the hardware that I purchase from being used as I see fit as a law abiding radio operator!

Do not restrict the hardware that I purchase from being used as I see fit as a law abiding radio operator!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Griffin

Mailing Address: 5773 Oatfield

City: Farmington

Country: United States

State or Province: NY

ZIP/Postal Code: 14425

Email Address: hexatron@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: Michael

Last Name: Zimmermann

Mailing Address: 931 Apache Mountain Ln

City: Georgetown

Country: United States

State or Province: TX

ZIP/Postal Code: 78633

Email Address: michael@zimm3rmann.com

Organization Name:

Comment: Lacking evidence that open-source firmware has caused any more wireless interference than closed-source firmware, I would urge the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I have installed open-source firmware on a number of my devices to expand their functionality and feel the freedom to modify software is important.

Lacking evidence that open-source firmware has caused any more wireless interference than closed-source firmware, I would urge the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I have installed open-source firmware on a number of my devices to expand their functionality and feel the freedom to modify software is important.

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: Sascha

Last Name: Winter

Mailing Address: 123 Public Record Lane

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94110

Email Address:

Organization Name:

Comment: I would like to ask the FCC not implement rules that take away the ability of users to install the software of their choosing on their computing devices

In learning how to install linux on my router was one of the things that got me interested in computers in the first place. Adding restrictions to what software can be installed on WiFi access points is like adding a bandaid to a overflowing dam.

I understand the motivation in trying to stop people from using unauthorized frequencies. I just don't think it will help and will be destructive to the fabric of our society freedom of expression and the entrepreneuring spirit. Here are some additional reasons I have plagiarized:

- 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 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 no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Thanks for your consideration.

Sascha

I would like to ask the FCC not implement rules that take away the ability of users to install the software of their choosing on their computing devices

In learning how to install linux on my router was one of the things that got me interested in computers in the first place. Adding restrictions to what software can be installed on WiFi access points is like adding a bandaid to a overflowing dam.

I understand the motivation in trying to stop people from using unauthorized frequencies. I just don't think it will help and will be destructive to the fabric of our society freedom of expression and the entrepreneuring spirit. Here are some additional reasons I have plagiarized:

- 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 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 no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Thanks for your consideration.

Sascha

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: Klaus-M.

Last Name: Schremser

Mailing Address: Gonzagagasse 11/25

City: Vienna

Country: Austria

State or Province: Vienna

ZIP/Postal Code: 1010

Email Address: email@schremser.com

Organization Name:

Comment: Please do not implement your 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.

People 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.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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 no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Please do not implement your 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.

People 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.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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 no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Saunders

Mailing Address: 1360 Apple Creek Rd.

City: Waynesville

Country: United States

State or Province: NC

ZIP/Postal Code: 28786

Email Address: john.saunders@gmail.com

Organization Name:

Comment: The proposed rules prohibiting new device firmware will have dire economic impact, the security implications would be extreme, and emergency preparedness would be greatly hindered by the proposed restrictions on router firmware.

The federal government, with its best intentions, is not prepared to govern this effectively. Please remember that "We the people" should empower the individual innovative abilities to strengthen our country rather than hindering unintentionally with arbitrary regulation forcing more vulnerabilities to be exposed as workarounds to enable basic safety and opportunity.

The proposed rules prohibiting new device firmware will have dire economic impact, the security implications would be extreme, and emergency preparedness would be greatly hindered by the proposed restrictions on router firmware.

The federal government, with its best intentions, is not prepared to govern this effectively. Please remember that "We the people" should empower the individual innovative abilities to strengthen our country rather than hindering unintentionally with arbitrary regulation forcing more vulnerabilities to be exposed as workarounds to enable basic safety and opportunity.

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: Brie

Mailing Address: 3497 Sunset Blvd

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 32347

Email Address:

Organization Name:

Comment: Please don't make OpenWRT/DD WRT illegal!

Please don't make OpenWRT/DD WRT illegal!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: William

Last Name: Warren

Mailing Address: 324 West Postomac Street

City: Brunswick

Country: United States

State or Province: MD

ZIP/Postal Code: 21716

Email Address:

Organization Name:

Comment: This is going to have a highly detrimental effect to the ability for others to modify their gear how they wish in terms of firmware for either higher performance, security research, or fair use. Just do some quick research on router security and you will find that the RF characteristics are minor compared to the rampant security problems modern devices represent. The ability to update, replace, or modify the firmware with something else is vital to maintain our countrys security including home use. Many businesses are now run out of residences and securing them is enough of a challenge but taking away a vital security tool would make this industry more anti-consumer and anti-security than it already is. This rule would remove the market pressure on manufacturers to at least have a facade of maintaining security.

This rule could also make HAM radios unable to be modified as well. Considering that HAM radios work well and that the vast majority stay well under their band and radiation limits this would devastate the Amateur radio operators ability to research, modify, repair, and improve vast swaths of HAM gear. Considering how vital HAM operators where during various disasters including 9/11 and Katrina this would be a serious blow to the nations communication infrastructure. Due to the factors listed above I highly recommend to the FCC that this rule be tabled until more consultation with various experts can be properly performance. I would be happy to assist the FCC if requested.

Sincerely,

William Warren

Owner Emmanuel Technology Consulting

FCC Amateur radio callsign: KB3VVT

This is going to have a highly detrimental effect to the ability for others to modify their gear how they wish in terms of firmware for either higher performance, security research, or fair use. Just do some quick research on router security and you will find that the RF characteristics are minor compared to the rampant security problems modern devices represent. The ability to update, replace, or modify the firmware with something else is vital to maintain our countrys security including home use. Many businesses are now run out of residences and securing them is enough of a challenge but taking away a vital security tool would make this industry more anti-consumer and anti-security than it already is. This rule would remove the market pressure on manufacturers to at least have a facade of maintaining security.

This rule could also make HAM radios unable to be modified as well. Considering that HAM radios work well and that the vast majority stay well under their band and radiation limits this would devastate the Amateur radio operators ability to research, modify, repair, and improve vast swaths of HAM gear. Considering how vital HAM operators where during various disasters including 9/11 and Katrina this would be a serious blow to the nations communication

infrastructure. Due to the factors listed above I highly recommend to the FCC that this rule be tabled until more consultation with various experts can be properly performance. I would be happy to assist the FCC if requested.

Sincerely,

William Warren

Owner Emmanuel Technology Consulting

FCC Amateur radio callsign: KB3VVT

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Anonymous

Mailing Address: O'Higgins 1610

City: Ciudad Autnoma de Buenos Aires

Country: Argentina

State or Province: Gran Buenos Aires

ZIP/Postal Code: 1426

Email Address: null

Organization Name: null

Comment: As a Free Software user and advocate, I am very concerned by this proposed rulemaking. It has come to my attention that it could effectively prevent people from running their own software on their computers if these have SDR capabilities.

Although I am not a resident of the United States, these regulations would very likely affect meand everyone else in the worldbecause device manufacturers that want to sell their products in the United States are unlikely to make a version compliant with these new regulations exclusively for that market. Alas, not a single one of the devices with an antenna in my vicinity lacks FCC certification. Yet, almost all of them are running custom software, without which their usefulness would be severely crippled. The computer network setup I am using right now would be outright impossible if I were restricted to running only the original manufacturer software; not to mention the security threats I would be vulnerable to if I did.

As such, I ask you to reconsider the restrictions that would be applied to end users with these new regulations, to make sure they retain all the rights to use their software of choice on their own computers.

As a Free Software user and advocate, I am very concerned by this proposed rulemaking. It has come to my attention that it could effectively prevent people from running their own software on their computers if these have SDR capabilities.

Although I am not a resident of the United States, these regulations would very likely affect meand everyone else in the worldbecause device manufacturers that want to sell their products in the United States are unlikely to make a version compliant with these new regulations exclusively for that market. Alas, not a single one of the devices with an antenna in my vicinity lacks FCC certification. Yet, almost all of them are running custom software, without which their usefulness would be severely crippled. The computer network setup I am using right now would be outright impossible if I were restricted to running only the original manufacturer software; not to mention the security threats I would be vulnerable to if I did.

As such, I ask you to reconsider the restrictions that would be applied to end users with these new regulations, to make sure they retain all the rights to use their software of choice on their own computers.

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: sandusky

Mailing Address: 1101 Four Seasons Drive

City: Mason

Country: United States

State or Province: OH

ZIP/Postal Code: 45040

Email Address: jonathan.sandusky@gmail.com

Organization Name:

Comment: This is a horrible idea. This would make it illegal to install security updates to my router and phone. Also would hinder innovation. Please don't approve this.

This is a horrible idea. This would make it illegal to install security updates to my router and phone. Also would hinder innovation. Please don't approve 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: Ramthun

Last Name: Helge

Mailing Address: Jlicher Str. 31

City: Cologne

Country: Germany

State or Province: NRW

ZIP/Postal Code: 50674

Email Address: HRamthun@gmx.de

Organization Name:

Comment: Sir,

I politely request that this rule is not implemented for the following reasons:

- Closed source routers have a long history of security issues, which are often fixed only with much delay, if at all. In particular, the lifetime of the hardware is often longer than the lifetime of support or even vendor, in which case, vulnerabilities are never closed.
- Open software has proven to be much more secure and responsive to new findings.
- Users should have a free choice of what software they use in their house.
- Current regulation of prosecuting anyone who misuses wireless devices to cause disturbances are sufficient.
- The rule is trying to solve an issue, which is not a severe problem at all.
- The rule would lead to increased bureaucracy on the side of supervisor and manufacturers.
- The reduced competition would lead to more expensive devices for the end user.
- American routers would be inferior to international ones, which do not have to adhere to this rule, leaving the manufacturer behind in the race for excellence.

Sir,

I politely request that this rule is not implemented for the following reasons:

- Closed source routers have a long history of security issues, which are often fixed only with much delay, if at all. In particular, the lifetime of the hardware is often longer than the lifetime of support or even vendor, in which case, vulnerabilities are never closed.
- Open software has proven to be much more secure and responsive to new findings.
- Users should have a free choice of what software they use in their house.

- Current regulation of prosecuting anyone who misuses wireless devices to cause disturbances are sufficient.
- The rule is trying to solve an issue, which is not a severe problem at all.
- The rule would lead to increased bureaucracy on the side of supervisor and manufacuters.
- The reduced competition would lead to more expensive devices for the end user.
- American routers would be inferior to international ones, which do not have to adhere to this rule, leaving the manufacturer behind in the race for excellence.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Rakestraw

Mailing Address: 1840 Calash Way

City: Virginia Beach

Country: United States

State or Province: VA

ZIP/Postal Code: 23454

Email Address: nofoolgm@gmail.com

Organization Name:

Comment: I have been working in the computer and network technology business for almost thirty years and have installed numerable systems such as the rf devices in question. In particular I have for more than fifteen years I have worked in cybersecurity for local Government,Federal Government and the US Military.

Commercial and foreign entities have various incentives and very often these don't include my network security. Generally, it is not in their commercial interest and they are not capable to keep up with exploits and patches with the speed and accuracy that Open Source solutions provide.

So, I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their bought and paid for computing devices. In particular, please allow Americans the ability to fix security holes in their devices when the manufacturer chooses to not do so.

I am not against updating the rules, but there are much better ways to protect the public safety than keeping people ignorant of the technology they are using through regulated commercial secrecy.

Never in my life felt strongly enough to have the compulsion to post a comment. I'm sure this comment will be thrown out as legalese is not in my short list of talents.

I have been working in the computer and network technology business for almost thirty years and have installed numerable systems such as the rf devices in question. In particular I have for more than fifteen years I have worked in cybersecurity for local Government,Federal Government and the US Military.

Commercial and foreign entities have various incentives and very often these don't include my network security. Generally, it is not in their commercial interest and they are not capable to keep up with exploits and patches with the speed and accuracy that Open Source solutions provide.

So, I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their bought and paid for computing devices. In particular, please allow Americans the ability to fix security holes in their devices when the manufacturer chooses to not do so.

I am not against updating the rules, but there are much better ways to protect the public safety than keeping people ignorant of the technology they are using through regulated commercial secrecy.

Never in my life felt strongly enough to have the compulsion to post a comment. I'm sure this comment will be thrown out as legalese is not in my short list of talents.

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: Toni

Last Name: Tiveron

Mailing Address: Via Sabotino 6

City: Treviso

Country: Italy

State or Province: Treviso

ZIP/Postal Code: 31100

Email Address: toni.tiveron@tiscali.it

Organization Name:

Comment: This will bound users to vendor. A simple example about that is:

Android phone. Vendor sells it w/ a version. A new security issue is found. Vendor will not be partial to supprt it. Will you (FCC) pay a new phone or will you allow the user to use a non OEM firmware to fix the security issue?

This will bound users to vendor. A simple example about that is:

Android phone. Vendor sells it w/ a version. A new security issue is found. Vendor will not be partial to supprt it. Will you (FCC) pay a new phone or will you allow the user to use a non OEM firmware to fix the security issue?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Benjamin

Last Name: Heath

Mailing Address: 2113 N 107th apt. 302

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98133

Email Address: null

Organization Name: null

Comment: This regulation is absurd. What sort of corporate state are we becoming that the government, lobbied by corporate interests, can declare it illegal for citizens to modify and tinker with equipment that *they* own? Far from the first-amendment rights-squashing that this measure represents, it furthermore prohibits citizens from fixing legitimate security issues their devices may have that the manufacturer will not address.

This bill represents much of the worst of our modern political system -- corporate interests which methodically and banally snuff out the ability for citizens to lead happy, curious lives.

This regulation is absurd. What sort of corporate state are we becoming that the government, lobbied by corporate interests, can declare it illegal for citizens to modify and tinker with equipment that *they* own? Far from the first-amendment rights-squashing that this measure represents, it furthermore prohibits citizens from fixing legitimate security issues their devices may have that the manufacturer will not address.

This bill represents much of the worst of our modern political system -- corporate interests which methodically and banally snuff out the ability for citizens to lead happy, curious lives.

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: Marco

Last Name: Giuntini

Mailing Address: Joan Melchior Kempestraat 117 HS

City: Amsterdam

Country: Netherlands

State or Province: Amsterdam

ZIP/Postal Code: 1051 TN

Email Address: hispanico@ninux.org

Organization Name: Ninux.org

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

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Iqbal

Last Name: Ahmed

Mailing Address: H#89, B#K, R#20 Rampura Dhaka.

City: Dhaka

Country: Bangladesh

State or Province: Dhaka

ZIP/Postal Code: 1209

Email Address: iqbalopurbo@gmail.com

Organization Name: N/A

Comment: I object this because security and privacy is important to me. If this control goes over to some else this wont be possible for us to rebuild or modify our devices.

I object this because security and privacy is important to me. If this control goes over to some else this wont be possible for us to rebuild or modify our 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: asdasd

Last Name: asdasd

Mailing Address: asd

City: asd

Country: India

State or Province: TELANGANA

ZIP/Postal Code: 500059

Email Address: asdasd@asd.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.

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

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.

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

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: Farhadur

Last Name: Fahim

Mailing Address: farhadurfahim@gmail.com

City: Dhaka

Country: Bangladesh

State or Province: Dhaka

ZIP/Postal Code: 1216

Email Address:

Organization Name:

Comment: As an user, I object this for Digital Freedom, Security, Privacy. I want my full freedom in my device.

Freedom is my right. As your proposal there will be no freedom.

In short, I object this proposal because digital freedom, data and communication security and my privacy is "very important" to me. Please, stop your current proposal as it is affecting me and the mass people on this globe who are with the wireless technology.

STOP THIS & SAVE WIFI.

As an user, I object this for Digital Freedom, Security, Privacy. I want my full freedom in my device. Freedom is my right. As your proposal there will be no freedom.

In short, I object this proposal because digital freedom, data and communication security and my privacy is "very important" to me. Please, stop your current proposal as it is affecting me and the mass people on this globe who are with the wireless technology.

STOP THIS & SAVE WIFI.