

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kevin

Last Name: Wisher

Mailing Address: 6380 East 50 North

City: Greentown

Country: United States

State or Province: IN

ZIP/Postal Code: 46936

Email Address:

Organization Name:

Comment: To whom it may concern,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Please see the list below for which I feel strongly about.

- 1) Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- 2) Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- 3) Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- 4) Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 5) 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.

To whom it may concern,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Please see the list below for which I feel strongly about.

- 1) Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- 2) Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- 3) Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- 4) Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 5) 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: M

Last Name: Yudkowsky

Mailing Address: 2952 W Fargo

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60645-1223

Email Address:

Organization Name: Disaggregte Corporation

Comment: The proposed rule restricts my ability to properly and securely operate routers.

While it is possible, in principle, that a router may at some point operate outside parameters when used with third-party software, this risk is minuscule. The benefits of third-party software far outweigh the risks.

Third-party software can and does make routers more secure. The software can, from time to time, rejuvenate an old piece of equipment that otherwise barely functions; for that matter, new equipment that barely functions can be made to operate.

Third-party software encourages innovation in software; it also provides users the ability to permit functions (e.g., dynamic DNS or SIP routing) not envisioned by the original hardware developers.

Finally, hardware is freely available that can easily be converted into routers. I will pursue that route if the FCC restricts me from the purchase of commercial routers that can be re-programmed. The choice is not between no third-party firmware and only commercial firmware; it's between tested and approved hardware and home-brewed hardware.

As such, the benefits of third-party software are so great, and the risks so small, that third-party software should not be restricted from routers.

The proposed rule restricts my ability to properly and securely operate routers.

While it is possible, in principle, that a router may at some point operate outside parameters when used with third-party software, this risk is minuscule. The benefits of third-party software far outweigh the risks.

Third-party software can and does make routers more secure. The software can, from time to time, rejuvenate an old piece of equipment that otherwise barely functions; for that matter, new equipment that barely functions can be made to operate.

Third-party software encourages innovation in software; it also provides users the ability to permit functions (e.g., dynamic DNS or SIP routing) not envisioned by the original hardware developers.

Finally, hardware is freely available that can easily be converted into routers. I will pursue that route if the FCC restricts me from the purchase of commercial routers that can be re-programmed. The choice is not between no third-party firmware and only commercial firmware; it's between tested and approved hardware and home-brewed hardware.

As such, the benefits of third-party software are so great, and the risks so small, that third-party software should not be restricted from routers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Lankford

Mailing Address: 8942 Christian Light Rd.

City: Fuquay Varina

Country: United States

State or Province: NC

ZIP/Postal Code: 27526

Email Address:

Organization Name:

Comment: There isn't anything the lawyers and bureaucrats at the FCC don't want to find a way to regulate regardless of whether there is any justifiable reason for doing so. The FCC is desperate to justify its existence, and they'll harass and annoy and invent new powers as needed to keep themselves busy. The things they hate most is innovation and consumer freedom. WiFi works and works well without "guidance" from beancounters and officialdom because very competent programmers designed standards that allow interoperability and interoperability depends on conformance to those same standards. Dismantle the FCC. We'll keep our wifi as it is.

There isn't anything the lawyers and bureaucrats at the FCC don't want to find a way to regulate regardless of whether there is any justifiable reason for doing so. The FCC is desperate to justify its existence, and they'll harass and annoy and invent new powers as needed to keep themselves busy. The things they hate most is innovation and consumer freedom. WiFi works and works well without "guidance" from beancounters and officialdom because very competent programmers designed standards that allow interoperability and interoperability depends on conformance to those same standards. Dismantle the FCC. We'll keep our wifi as it is.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Alschuler

Mailing Address: PO Box 325

City: Warren

Country: United States

State or Province: IL

ZIP/Postal Code: 61087

Email Address: matthew@cottonexpressions.com

Organization Name:

Comment: I am concerned about limiting the ability of consumers, and small business owners, like myself, to install well tested open source firmware on internet routers.

I have also found it very useful to be able to install software that has options unavailable with stock firmware, or that fixes bugs with stock firmware.

Limiting the ability of consumers to use their own equipment will result in weaker internet security, not great.

Please reconsider the draconian regulations being proposed.

Thank you,

Matthew Alschuler, President

Cotton Expressions, Ltd

I am concerned about limiting the ability of consumers, and small business owners, like myself, to install well tested open source firmware on internet routers.

I have also found it very useful to be able to install software that has options unavailable with stock firmware, or that fixes bugs with stock firmware.

Limiting the ability of consumers to use their own equipment will result in weaker internet security, not great.

Please reconsider the draconian regulations being proposed.

Thank you,

Matthew Alschuler, President

Cotton Expressions, Ltd

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: Antonio

Last Name: Gomes

Mailing Address: 35 Reed Ave

City: Chicopee

Country: United States

State or Province: MA

ZIP/Postal Code: 01020

Email Address: gomes-tony@hotmail.com

Organization Name:

Comment: Unfortunately, the paperwork is too vague and allows these rules to be applied to hardware such as home "routers". The inability for the end user to use "modified" or "custom" firmware would leave some security loopholes open. Most of the "custom" firmware out there has been written to address and close such security loopholes or address concerns of such kind (ie: heartbleed bug). Most manufacturers of these devices refuse to or stop "supporting" "older" legacy devices (sometimes within such a short span as 6 months from the date of release) due to the fact that if they kept them up to date they wouldn't make a sale on their next device. People pick up where these manufacturers have stopped and continue to patch security holes in firmware with these custom images, allowing the devices to continue to be used and closing those security loop holes. If implemented, this rule would stop people from using these modified firmware to close such holes. Yes custom firmware adds other function or enables other features also, but it's constant development ensures that the latest security measures are instituted. Also this rule would stop further development or research into "foreign" products, maybe stopping us from finding deliberate flaws from manufacturers in other countries (think Chinese company's' based products). I would not be against this rule if it had an expiration date: example: this rule does not apply to any device one year after it's model release. This would allow those custom images to pick up where manufacturers leave off and continue to update devices.

Unfortunately, the paperwork is too vague and allows these rules to be applied to hardware such as home "routers". The inability for the end user to use "modified" or "custom" firmware would leave some security loopholes open. Most of the "custom" firmware out there has been written to address and close such security loopholes or address concerns of such kind (ie: heartbleed bug). Most manufacturers of these devices refuse to or stop "supporting" "older" legacy devices (sometimes within such a short span as 6 months from the date of release) due to the fact that if they kept them up to date they wouldn't make a sale on their next device. People pick up where these manufacturers have stopped and continue to patch security holes in firmware with these custom images, allowing the devices to continue to be used and closing those security loop holes. If implemented, this rule would stop people from using these modified firmware to close such holes. Yes custom firmware adds other function or enables other features also, but it's constant development ensures that the latest security measures are instituted. Also this rule would stop further development or research into "foreign" products, maybe stopping us from finding deliberate flaws from manufacturers in other countries (think Chinese company's' based products). I would not be against this rule if it had an expiration date: example: this rule does not apply to any device one year after it's model release. This would allow those custom images to pick up where manufacturers leave off and continue to update 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: Joshua

Last Name: Parker

Mailing Address: 450 w. Kelso st. #18

City: Tucson

Country: United States

State or Province: AZ

ZIP/Postal Code: 85706

Email Address:

Organization Name:

Comment: Please don't limit people. This is taking away our freedoms.

Please don't limit people. This is taking away our freedoms.

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: Reid

Last Name: McKenzie

Mailing Address: 711 West 32nd Street

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78705

Email Address:

Organization Name:

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

My reasons for making this request include:

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

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

My reasons for making this request include:

- * 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 harming users.
- * 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: David

Last Name: Stirtz

Mailing Address: 2536 Lincoln Street

City: Minneapolis

Country: United States

State or Province: MN

ZIP/Postal Code: 55418

Email Address: david@mn-networking.com

Organization Name:

Comment: As a technology worker and hobbyist this proposed ruling is ill-conceived. I understand the premise for the ruling, and see the benefits to it, but I do not believe the benefits outweigh the cost. All of my devices are running on modified firmware (DDWRT and Tomato), running on store bought routers and wireless devices, because the manufacturers of these devices have failed time and again to provide adequate security or functionality. The hardware in most devices is more than adequate for their purpose but the software (firmware) is typically what fails to live up to expectations. Common claims such as "speeds up to X" rarely pan out until the device has been loaded with open source firmware. Please reconsider this proposed rule; there are far too many groups out there (techies, hackers, security minded individuals) that will be hurt by this proposed rule. I also sincerely believe that it will give manufacturers of consumer products even less incentive to make their products work better, through increased cost of complexity and regulations, which will lead to everyone being hurt.

As a technology worker and hobbyist this proposed ruling is ill-conceived. I understand the premise for the ruling, and see the benefits to it, but I do not believe the benefits outweigh the cost. All of my devices are running on modified firmware (DDWRT and Tomato), running on store bought routers and wireless devices, because the manufacturers of these devices have failed time and again to provide adequate security or functionality. The hardware in most devices is more than adequate for their purpose but the software (firmware) is typically what fails to live up to expectations. Common claims such as "speeds up to X" rarely pan out until the device has been loaded with open source firmware. Please reconsider this proposed rule; there are far too many groups out there (techies, hackers, security minded individuals) that will be hurt by this proposed rule. I also sincerely believe that it will give manufacturers of consumer products even less incentive to make their products work better, through increased cost of complexity and regulations, which will lead to everyone being hurt.

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: Moore

Mailing Address: 198 E Milton St #3

City: Lebanon

Country: United States

State or Province: OR

ZIP/Postal Code: 97355-3447

Email Address: dwmoar@findmoore.net

Organization Name:

Comment: Please do not take away the ability of users to install 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.

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.

Please do not take away the ability of users to install 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.

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.

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: Arthur

Last Name: Tanner

Mailing Address: 12309 Melody Turn

City: Bowie

Country: United States

State or Province: MD

ZIP/Postal Code: 20715

Email Address: aseataner@yahoo.com

Organization Name:

Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I would also call to your attention the following facts:

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.

This rule would severely hamper the extremely useful activity of amateur radio operators who over the past few years have developed mesh networking capability using firmware especially designed for that purpose. The developers of this capability, which has far ranging impact for emergency communications in cases of disaster, have recently won the annual Amateur Radio Relay League(ARRL) Microwave Development Award.

In summary, please do not restrict the ability of anyone to modify and improve router firmware. It is in no one's best interest to do 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 computing devices. I would also call to your attention the following facts:

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.

This rule would severely hamper the extremely useful activity of amateur radio operators who over the past few years have developed mesh networking capability using firmware especially designed for that purpose. The developers of this capability, which has far ranging impact for emergency communications in cases of disaster, have recently won the annual Amateur Radio Relay League(ARRL) Microwave Development Award.

In summary, please do not restrict the ability of anyone to modify and improve router firmware. It is in no one's best interest to 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: Germano

Last Name: Massullo

Mailing Address: Via F.U.

City: Rome

Country: Italy

State or Province: RM

ZIP/Postal Code: 00100

Email Address:

Organization Name:

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

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Josh

Last Name: Potter

Mailing Address: 610 Prairie Ln

City: Columbia

Country: United States

State or Province: MO

ZIP/Postal Code: 65202

Email Address: joshpotter@gmail.com

Organization Name:

Comment: Making changes like this is just going to stifle innovation. If someone breaks the law by illegally modifying the power, then punish the actual crime. I should be able to freely tinker with my firmware and I can do that without breaking FCC rules.

Making changes like this is just going to stifle innovation. If someone breaks the law by illegally modifying the power, then punish the actual crime. I should be able to freely tinker with my firmware and I can do that without breaking FCC rules.

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: Alessandro

Last Name: Selli

Mailing Address: Via Ilia 20

City: Roma

Country: Italy

State or Province: RM

ZIP/Postal Code: 00181

Email Address: alessandroselli@linux.com

Organization Name:

Comment: Given the number of devices in use on the Internet that suffer from firmware that is affected by security bugs of the most diverse nature and gravity (<http://www.computerweekly.com/news/2240163351/Android-devices-vulnerable-to-security-breaches> , <http://www.networkworld.com/article/2899733/security/at-least-700000-routers-given-to-customers-by-isps-are-vulnerable-to-hacking.html>) and the bad work manufactures are doing in providing updates to the affected firmware and devices (many times because they no longer support a product a few years after it went to the market), preventing people from updating the manufacturer's firmware with a third party one is a very effective way to guarantee the Internet will become an ever more vulnerable an unworkable, disfunctional mess.

Another point comes to mind against this proposal of yours: more firmwares available for the same devices, designed by different teams and developers, will cause a healthy competition and diversity of purpose for the various software solutions devised by those teams to run on the given hardware. This is the best environment where brilliant ideas and project are developed, emerge and produce not just new and better products, but innovation and creativity of the same kind that allowed the IT to explode in the seventies to invent the personal computer market and become something very few people thought could develop out of the hardware then available.

Locking down devices and preventing developers to work on third party firmware just does not sound any good an idea technology- and market-wise.

Given the number of devices in use on the Internet that suffer from firmware that is affected by security bugs of the most diverse nature and gravity (<http://www.computerweekly.com/news/2240163351/Android-devices-vulnerable-to-security-breaches> , <http://www.networkworld.com/article/2899733/security/at-least-700000-routers-given-to-customers-by-isps-are-vulnerable-to-hacking.html>) and the bad work manufactures are doing in providing updates to the affected firmware and devices (many times because they no longer support a product a few years after it went to the market), preventing people from updating the manufacturer's firmware with a third party one is a very effective way to guarantee the Internet will become an ever more vulnerable an unworkable, disfunctional mess.

Another point comes to mind against this proposal of yours: more firmwares available for the same devices, designed by different teams and developers, will cause a healthy competition and diversity of purpose for the various software solutions devised by those teams to run on the given hardware. This is the best environment where brilliant ideas and project are developed, emerge and produce not just new and better products, but innovation and creativity of the same kind that allowed the IT to explode in the seventies to invent the personal computer market and become something very few people thought could develop out of the hardware then available.

Locking down devices and preventing developers to work on third party firmware just does not sound any good an idea technology- and market-wise.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: stephen

Last Name: lewis

Mailing Address: 24650 n rimrock rd

City: hayden

Country: United States

State or Province: ID

ZIP/Postal Code: 83835

Email Address: lewis+fcc@freeshell.org

Organization Name: citizen of united states

Comment: I am running DD-WRT on a Linksys WRT54-GL and

Gentoo Linux on a Samsung Galaxy Tab.

Without the ability to reflash the firmware I would not be able to run my own software on my own devices.

Please don't restrict the ability to reflash firmware into routers, tablets or phones.

This will have the following negative effects:

Encourage monopoly behaviour by manufacturers who may not act in the best interest of end-user.

Delay the implementation of bug fixes, must wait for "official" release of fixed firmware.

Prevent innovation which encourages stagnation and premature obsolescence frequently favored by monopoly manufacturer.

Prevent the use of low cost embedded processors for experimental software, hobby use and education.

The ability to run custom software has these advantages:

Allows hobby use of low cost platforms.

Encourages quick turnaround for bug fixes and blocking malware.

Extends life of products beyond officially supported platforms thus lowering the cost and increasing utility for the end user.

Allows use of products in entirely new and innovative ways beyond the imagination of original manufacturer.

Suggestions:

The FCC already has in place a system of Amateur License requirements. I hold a Technician Class License. Maybe instead of the wholesale elimination of equipment use perhaps a Technician License could be required to reflash firmware. Amateurs are already presumed to have sufficient understanding and maturity to respect licensed radio frequency bands.

I am running DD-WRT on a Linksys WRT54-GL and Gentoo Linux on a Samsung Galaxy Tab.

Without the ability to reflash the firmware I would not be able to run my own software on my own devices. Please don't restrict the ability to reflash firmware into routers, tablets or phones.

This will have the following negative effects:

Encourage monopoly behaviour by manufacturers who may not act in the best interest of end-user.

Delay the implementation of bug fixes, must wait for "official" release of fixed firmware.

Prevent innovation which encourages stagnation and premature obsolescence frequently favored by monopoly manufacturer.

Prevent the use of low cost embedded processors for experimental software, hobby use and education.

The ability to run custom software has these advantages:

Allows hobby use of low cost platforms.

Encourages quick turnaround for bug fixes and blocking malware.

Extends life of products beyond officially supported platforms thus lowering the cost and increasing utility for the end user.

Allows use of products in entirely new and innovative ways beyond the imagination of original manufacturer.

Suggestions:

The FCC already has in place a system of Amateur License requirements. I hold a Technician Class License. Maybe instead of the wholesale elimination of equipment use perhaps a Technician License could be required to reflash firmware. Amateurs are already presumed to have sufficient understanding and maturity to respect licensed radio frequency bands.

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: Hoover

Mailing Address: 1118 Wild Cherry Drive

City: Carrollton

Country: United States

State or Province: TX

ZIP/Postal Code: 75010

Email Address: larry_hoover@rocketmail.com

Organization Name: N/A

Comment: Thank you for reading my comment.

I am against the proposed changes described in the Equipment Authorization regulations.

There is no legitimate reason to restrict changes to the devices as proposed. Americans are innovators and find many ways to give new and important life to devices to make them more useful and to keep them running for years.

These proposed changes will restrict legitimate uses and new uses. Why stifle innovation. The devices are useful in many ways and for many other purposes.

Wireless devices can give new life to communication systems when primary systems fail to operate or are damage due to nature disaster.

Does the FCC want to be responsible for the loss of life that may result when a natural disaster damages normal or primary communications systems and this ruling prevents citizens from implementing a system that could keep First Responders and Rescue Units helping save lives.

Consider the benefit of such innovations - this is the heart of the American spirit; to make the world a better place by being helpful and resilient.

Thank you for reading my comment.

I am against the proposed changes described in the Equipment Authorization regulations.

There is no legitimate reason to restrict changes to the devices as proposed. Americans are innovators and find many ways to give new and important life to devices to make them more useful and to keep them running for years.

These proposed changes will restrict legitimate uses and new uses. Why stifle innovation. The devices are useful in many ways and for many other purposes.

Wireless devices can give new life to communication systems when primary systems fail to operate or are damage due to nature disaster.

Does the FCC want to be responsible for the loss of life that may result when a natural disaster damages normal or primary communications systems and this ruling prevents citizens from implementing a system that could keep First Responders and Rescue Units helping save lives.

Consider the benefit of such innovations - this is the heart of the American spirit; to make the world a better place by being helpful and resilient.

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: Charlie

Last Name: Goodwin

Mailing Address: 100 North Village Road

City: Warner

Country: United States

State or Province: NY

ZIP/Postal Code: 03278-0000

Email Address:

Organization Name:

Comment: I hope you will not prohibit users and small businesses from modifying software on routers etc. Many of the most widely sold devices have software that has weaknesses. To ban modifications by users would stifle progress and eventually limit the quality of wifi devices.

I hope you will not prohibit users and small businesses from modifying software on routers etc. Many of the most widely sold devices have software that has weaknesses. To ban modifications by users would stifle progress and eventually limit the quality of wifi 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: Andrew

Last Name: Beck

Mailing Address: 418 Treeview Drive

City: Wadsworth

Country: United States

State or Province: OH

ZIP/Postal Code: 44281

Email Address:

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.

Respectfully,

Andrew Beck

418 Treeview Drive

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.

Respectfully,

Andrew Beck

418 Treeview Drive

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Adam

Last Name: Dane

Mailing Address: 3347 Castle Crest Drive

City: Vestavia

Country: United States

State or Province: AL

ZIP/Postal Code: 35216-4220

Email Address:

Organization Name:

Comment: I support the FCC's mandate to manage the public's spectrum for effective and efficient uses, including regulating against the interference between devices. The FCC should and must also work to ensure that they do not inadvertently infringe on common law rights of individuals and consortia to modify and use their equipment. Insofar as this proposal would curtail the spread of free software improvements that would not increase interfering uses, it should be rewritten.

I support the FCC's mandate to manage the public's spectrum for effective and efficient uses, including regulating against the interference between devices. The FCC should and must also work to ensure that they do not inadvertently infringe on common law rights of individuals and consortia to modify and use their equipment. Insofar as this proposal would curtail the spread of free software improvements that would not increase interfering uses, it should be rewritten.

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 T.

Last Name: Stager

Mailing Address: 6 Ryder CT

City: Dix Hills

Country: United States

State or Province: NY

ZIP/Postal Code: 11746

Email Address:

Organization Name:

Comment: Fascist police state.

Fascist police state.

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: Nicholas

Last Name: Vail-Stein

Mailing Address: 1116 R. Gowdy Ave.

City: Point Pleasant Boro.

Country: United States

State or Province: NJ

ZIP/Postal Code: 08742

Email Address: nickviiking@aol.com

Organization Name:

Comment: There are many reasons to complain about this. It is a full restriction of software freedom, and can completely destroy privacy. To put it in perspective it is like only allowing for computers to come with Microsoft Windows installed. which the court has found unconstitutional, through illegal acts of software bundling. the main reason for the wanting of the ban is to stop people from doing illegal actions with their routers, but it is most likely a hidden motive to put back doors into routers for surveillance. This is the very same surveillance that violates privacy and leaves open gates for private information to be hacked by a third party.

There are many reasons to complain about this. It is a full restriction of software freedom, and can completely destroy privacy. To put it in perspective it is like only allowing for computers to come with Microsoft Windows installed. which the court has found unconstitutional, through illegal acts of software bundling. the main reason for the wanting of the ban is to stop people from doing illegal actions with their routers, but it is most likely a hidden motive to put back doors into routers for surveillance. This is the very same surveillance that violates privacy and leaves open gates for private information to be hacked by a third party.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Wilkie

Mailing Address: 21 Solmar Drive

City: Rochester

Country: United States

State or Province: NY

ZIP/Postal Code: 14624

Email Address: fuzzyhypothesis@yahoo.com

Organization Name:

Comment: Please do not implement these new rules.

I am a fan and user of the software project dd-wrt (www.dd-wrt.com) in which I will replace existing firmware for wireless routers with the opensource software to keep the routers up to day, and in new features, and provide a better interface in which to manage my house network. If you enact these rules, it would kill of this opensource project, and force myself, and many others, to use stock proprietary firmware on the routers.

The stock firmware is typically limited by the manufacture in features, and is rarely updated. So any security issues found the average consumer will not get a fix for them and will be forced to buy new equipment. Assuming of course that equipment would have the fix.

Please do not implement these new rules.

I am a fan and user of the software project dd-wrt (www.dd-wrt.com) in which I will replace existing firmware for wireless routers with the opensource software to keep the routers up to day, and in new features, and provide a better interface in which to manage my house network. If you enact these rules, it would kill of this opensource project, and force myself, and many others, to use stock proprietary firmware on the routers.

The stock firmware is typically limited by the manufacture in features, and is rarely updated. So any security issues found the average consumer will not get a fix for them and will be forced to buy new equipment. Assuming of course that equipment would have the fix.

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: Lorenzo

Last Name: Quatrini

Mailing Address: N/A

City: N/A

Country: Ireland

State or Province: N/A

ZIP/Postal Code: N/A

Email Address:

Organization Name:

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

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jeremy

Last Name: Betz

Mailing Address: 192 Tanglewood Circle

City: Milford

Country: United States

State or Province: CT

ZIP/Postal Code: 06461

Email Address:

Organization Name:

Comment: I am concerned about the unintended consequences of the proposed rule to lock down wifi devices. As my familys IT person, I have often flashed open source firmware to older devices to upgrade their security fixing holes in the original firmware, and generally prolong the devices lifespan to keep it out of the landfill. I also understand that many of the aforementioned security concerns have been found by researchers installing custom software on wifi devices to make their research affordable and possible.

As a licensed amateur radio operator, I understand the need to protect our spectrum and operate within the rules but I fear that this regulation will do far more harm than the concerns it seeks to rectify.

I am concerned about the unintended consequences of the proposed rule to lock down wifi devices. As my familys IT person, I have often flashed open source firmware to older devices to upgrade their security fixing holes in the original firmware, and generally prolong the devices lifespan to keep it out of the landfill. I also understand that many of the aforementioned security concerns have been found by researchers installing custom software on wifi devices to make their research affordable and possible.

As a licensed amateur radio operator, I understand the need to protect our spectrum and operate within the rules but I fear that this regulation will do far more harm than the concerns it seeks to rectify.

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: Jared

Last Name: Croy

Mailing Address: 201 E 21st #M509

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78730

Email Address:

Organization Name:

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

My reasons for making this request include:

- * 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.

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

My reasons for making this request include:

- * 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.

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: Kessler

Mailing Address: 1608 Linscomb Ave

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78704

Email Address: djkessler@me.com

Organization Name:

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

My reasons for making this request include:

- * 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.

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

My reasons for making this request include:

- * 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.

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: Roger

Last Name: Dwight

Mailing Address: 121 High Street

City: Columbus

Country: United States

State or Province: OH

ZIP/Postal Code: 43210

Email Address:

Organization Name:

Comment: Hello,

I'm a professional network engineer and would prefer for the FCC not to get involved with regulating network technology at this level. I disagree that there are problems severe enough to mandate this level of regulation and feel that regulation would increase the level of engineering needed to implement newer technologies.

Additionally, I'm skeptical that a reasonable and efficient enforcement process could be developed on a budget that we all could live with.

-Roger

Hello,

I'm a professional network engineer and would prefer for the FCC not to get involved with regulating network technology at this level. I disagree that there are problems severe enough to mandate this level of regulation and feel that regulation would increase the level of engineering needed to implement newer technologies.

Additionally, I'm skeptical that a reasonable and efficient enforcement process could be developed on a budget that we all could live with.

-Roger

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: Fowlie

Mailing Address: 18 - 9th St

City: Carle Place

Country: United States

State or Province: NY

ZIP/Postal Code: 11514

Email Address: twist@fowlie.net

Organization Name:

Comment: I believe that the proposed rule is extraordinarily poorly thought out. While I can understand the importance of ensuring good conduct in the utilization of radio frequencies, this is equivalent to applying a sledgehammer to the problem.

In this world of SOC's, placing onerous restrictions on the overall behaviour of a physical device in order to control one aspect of it is blatant overreach. It limits the possibilities and potential for consumers to be able to learn, improve and develop in these critical skills. The problem you are attempting to solve may well be solved in a better way by those who are able to tinker and improve the devices they have.

When we are confronted with a need for greater engagement in STEM-abilities, preventing individuals from being able to interact at a deeper level with their devices is going to add another obstacle to growing our own engineers and technicians.

Would it not be better to engage the community that builds, modifies and improves these devices to see if there are collaborative solutions that would support property rights, develop inquisitive minds, and promote the skills our country will need more and more? You have access to many bright minds in the FCC, why not see what more creative solutions can be found?

I believe that the proposed rule is extraordinarily poorly thought out. While I can understand the importance of ensuring good conduct in the utilization of radio frequencies, this is equivalent to applying a sledgehammer to the problem.

In this world of SOC's, placing onerous restrictions on the overall behaviour of a physical device in order to control one aspect of it is blatant overreach. It limits the possibilities and potential for consumers to be able to learn, improve and develop in these critical skills. The problem you are attempting to solve may well be solved in a better way by those who are able to tinker and improve the devices they have.

When we are confronted with a need for greater engagement in STEM-abilities, preventing individuals from being able to interact at a deeper level with their devices is going to add another obstacle to growing our own engineers and technicians.

Would it not be better to engage the community that builds, modifies and improves these devices to see if there are collaborative solutions that would support property rights, develop inquisitive minds, and promote the skills our country

will need more and more? You have access to many bright minds in the FCC, why not see what more creative solutions can be found?

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: Chad

Last Name: Rosenberg

Mailing Address: 518 Maple Way

City: Ashland

Country: United States

State or Province: OR

ZIP/Postal Code: 97520

Email Address: abditus@gmail.com

Organization Name: FlowJo, LLC

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. As a software professional and someone who has to constantly think about security in their career, this will weaken our ability as community and society to spot and fix critical security bugs, hurt open source software, and stifle innovation.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. As a software professional and someone who has to constantly think about security in their career, this will weaken our ability as community and society to spot and fix critical security bugs, hurt open source software, and stifle innovation.

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: Scott

Last Name: Marshall

Mailing Address: 1000 Bee Hollow Dr.

City: Lehighton

Country: United States

State or Province: PA

ZIP/Postal Code: 18235

Email Address: smmarshall561@gmail.com

Organization Name: Oath Accountability Project

Comment: Please do not implement the rules that remove the liberty of software for 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. 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 the rules that remove the liberty of software for 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. 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: Dustin

Last Name: Lloyd

Mailing Address: 15217 Green Acres rd

City: Beaverdam

Country: United States

State or Province: VA

ZIP/Postal Code: 23015

Email Address:

Organization Name:

Comment: Please do not implement the rules that remove the liberty of software for 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. 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 the rules that remove the liberty of software for 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. 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: Bryan

Last Name: Lloyd

Mailing Address: 15217 Green Acres rd

City: Beaverdam

Country: United States

State or Province: VA

ZIP/Postal Code: 23015

Email Address:

Organization Name:

Comment: Please do not implement the rules that remove the liberty of software for 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. 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 the rules that remove the liberty of software for 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. 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: Shawn

Last Name: Hughes

Mailing Address: 2167 Colfax Ave Apt 4

City: Benton Harbor

Country: United States

State or Province: MI

ZIP/Postal Code: 49022

Email Address: fragtaginja@gmail.com

Organization Name:

Comment: Computer technology advances at an exponential rate. Banning the modification of Wifi routers is a terrible idea that could seriously impact the security of all kinds of information. Are you intentionally trying to make people more susceptible to hacking?

Computer technology advances at an exponential rate. Banning the modification of Wifi routers is a terrible idea that could seriously impact the security of all kinds of information. Are you intentionally trying to make people more susceptible to hacking?

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: Jessie

Last Name: Holt

Mailing Address: 1343 N. Lasalle St.

City: Indianapolis

Country: United States

State or Province: IN

ZIP/Postal Code: 46201

Email Address:

Organization Name:

Comment: I am communicating to you to explain the great concern people feel towards this rule and many other internet regulations in general. Over the past few years, many whistleblowers such as Manning and Snowden leaked information which pertains heavily to this nation. Now while some were unjustified (Manning - listing soldiers' locations, thus endangering soldiers) some were more than justified (Snowden - sharing what was an illegal invasion of privacy into people's lives which was supposed to be mainly targeting terrorists - and many more problems he found). Many people put themselves in Snowden's shoes, and feel effectively betrayed by him getting threatened with persecution, and feel that could happen to them. They also feel a trial would be rigged, and that Snowden in some way or form will be gravely wronged. Many hackers who work for the government agree but hide it, and they get paid arguably low wages, so taking up black hat hacking jobs that harm the government becomes a viable option to them when they feel a government that underpays them is too corrupt to work for and serve. Another restriction would make these and others resist and challenge the government, which you should try to keep from happening.

People value their privacy, so much so that they'd happily risk danger online for the right to control their WiFi routers and WiFi boxes. They wish for their privacy to be protected, and they wish for the method of protection to be in their hands. They're sure many in the government could do a good job at helping with privacy and securing the nation, but that's the nation - people want to secure themselves. They wish for the government sector and its regulations to remain there and stay out of the public domain as much as reasonably possible. They feel that this is reasonable and offensive to violate, to the point many will stop supporting you and even more will challenge your authority. People will in general do so peacefully, but aggressively. I wish to think there are some who will read this plea and resist regulations without something of a people's council on rights protection, one that is truly well-versed on matters and even technical workings of the internet (I am sure many at the FCC are, but not all, which can cause understanding and misguidance by some ulteriorly motivated lobbyists and a few ill-informed advisers). I understand such a body doesn't appear overnight, but work should be done to establish it.

I have another suggestion - poll the general and internet populous, and ask what should be done about certain problems. A few answers can be the answers the FCC is considering, while one is to leave the problem alone with another being to research the matter further, and one section can be labeled 'other' and allow a custom answer to be suggested. Let the people have a say, and discuss with them the measures you consider - this will ease their concerns and lead to more effective measures.

I am grateful for everything all of you have done to help protect the internet and its users, and wish you the best of luck in handling all of this - it's a big burden. Try to work with people, and they are more inclined to try to work with you.

I am communicating to you to explain the great concern people feel towards this rule and many other internet

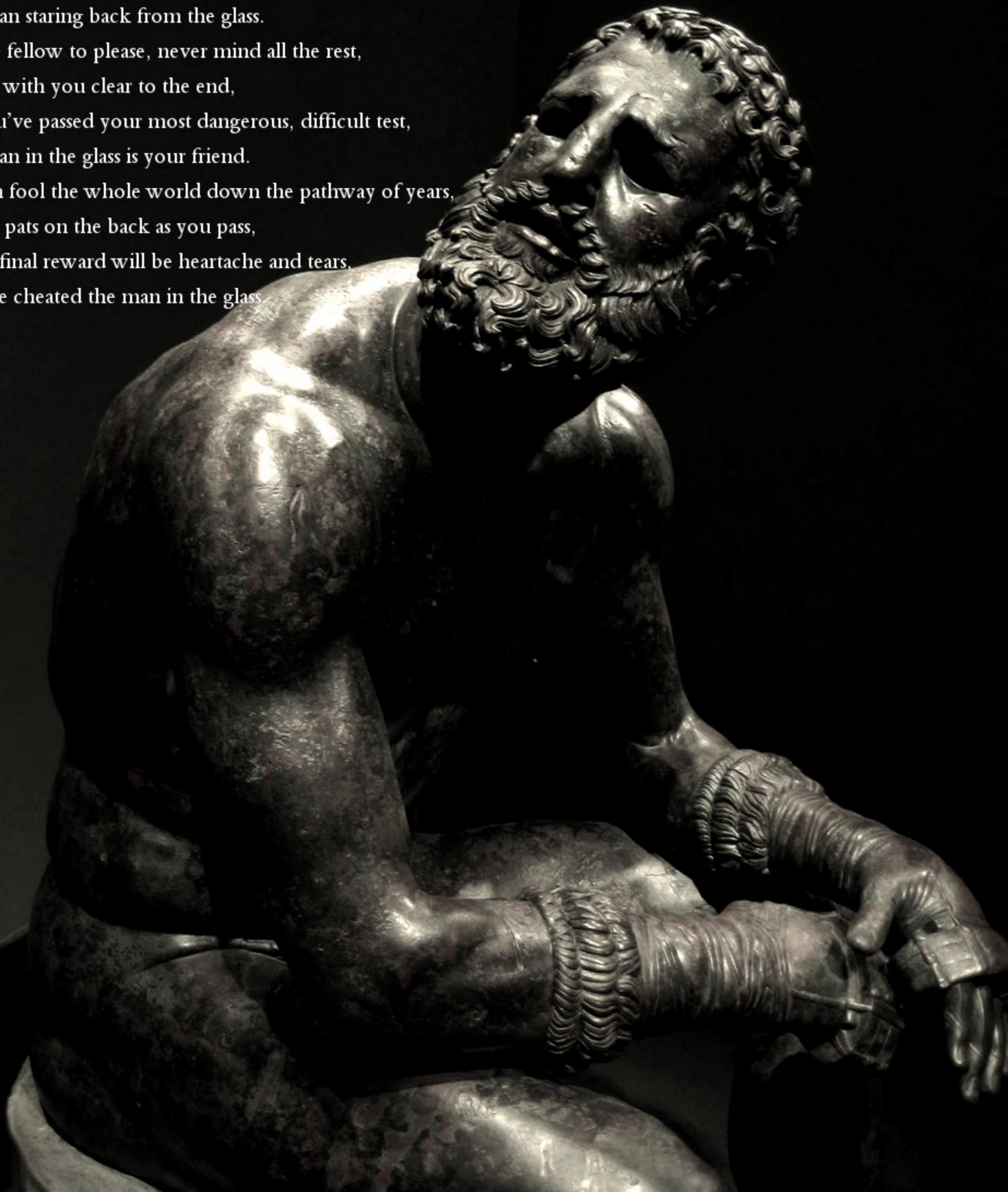
regulations in general. Over the past few years, many whistleblowers such as Manning and Snowden leaked information which pertains heavily to this nation. Now while some were unjustified (Manning - listing soldiers' locations, thus endangering soldiers) some were more than justified (Snowden - sharing what was an illegal invasion of privacy into people's lives which was supposed to be mainly targeting terrorists -and many more problems he found). Many people put themselves in Snowden's shoes, and feel effectively betrayed by him getting threatened with persecution, and feel that could happen to them. They also feel a trial would be rigged, and that Snowden in some way or form will be gravely wronged. Many hackers who work for the government agree but hide it, and they get paid arguably low wages, so taking up black hat hacking jobs that harm the government becomes a viable option to them when they feel a government that underpays them is too corrupt to work for and serve. Another restriction would make these and others resist and challenge the government, which you should try to keep from happening.

People value their privacy, so much so that they'd happily risk danger online for the right to control their WiFi routers and WiFi boxes. They wish for their privacy to be protected, and they wish for the method of protection to be in their hands. They're sure many in the government could do a good job at helping with privacy and securing the nation, but that's the nation - people want to secure themselves. They wish for the government sector and its regulations to remain there and stay out of the public domain as much as reasonably possible. They feel what this is reasonable and offensive to violate, to the point many will stop supporting you and even more will challenge your authority. People will in general do so peacefully, but aggressively. I wish to think there are some who will read this plea and resist regulations without something of a people's council on rights protection, one that is truly well versed on matters and even technical workings of the internet (I am sure many at the FCC are, but not all, which can cause understanding and misguidance by some ulteriorly motivated lobbyists and a few ill informed advisers). I understand such a body doesn't appear overnight, but work should be done to establish it.

I have another suggestion - poll the general and internet populous, and ask what should be done about certain problems. A few answers can be answers the FCC is considering, while one is to leave the problem alone with another being to research the matter further, and one section can be labeled 'other' and allow a custom answer be suggested. Let the people have a say, and discuss with them the measures you consider - this will ease their concerns and lead to more effective measures.

I am grateful for everything all of you have done to help protect the internet and its users, and wish you the best of luck in handling all of this - it's a big burden. Try to work with people, and they are more inclined to try to work with you.

When you get what you want in your struggle for self,
And the world makes you king for a day,
Then go to the mirror and look at yourself,
And see what that man has to say.
For it isn't a man's father, mother or wife,
Whose judgement upon him must pass,
The fellow whose verdict counts most in life,
Is the man staring back from the glass.
He's the fellow to please, never mind all the rest,
For he's with you clear to the end,
And you've passed your most dangerous, difficult test,
If the man in the glass is your friend.
You can fool the whole world down the pathway of years,
And get pats on the back as you pass,
But the final reward will be heartache and tears,
If you've cheated the man in the glass.



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: Melissa

Last Name: Cuneo

Mailing Address: 651 Westover Hills Blvd

City: Richmond

Country: United States

State or Province: VA

ZIP/Postal Code: 23225

Email Address:

Organization Name:

Comment: 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.

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Peter

Last Name: Mueller

Mailing Address: Street

City: Cologne

Country: Germany

State or Province: NRW

ZIP/Postal Code: 50829

Email Address:

Organization Name:

Comment: Dear Sir or Madam,

with this comment I am respectfully asking the FCC to not implement rules that will 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.
- All users 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.
- In my opinion these rules are the results of successful lobby work of big IT companies like Microsoft and Apple to eliminate Open Source software.
- Linux and other Open Source operating systems have change the IT world in a only positive way as on the opposite site companies like Microsoft are killing innovation and data privacy

It is shame that this kind of rules is even considered to decided. You will kill with these rules fine software projects as DD-WRT or maybe even Linux itself.

Hopefully you are understand that these rules are definitely not the right way to prevent users for modifying software for Wifi modules.

Kind Regards

Dear Sir or Madam,

with this comment I am respectfully asking the FCC to not implement rules that will 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.
- All users 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.
- In my opinion these rules are the results of successful lobby work of big IT companies like Microsoft and Apple to eliminate Open Source software.
- Linux and other Open Source operating systems have change the IT world in a only positive way as on the opposite site companies like Microsoft are killing innovation and data privacy

It is shame that this kind of rules is even considered to decided. You will kill with these rules fine software projects as DD-WRT or maybe even Linux itself.

Hopefully you are understand that these rules are definitely not the right way to prevent users for modifying software for Wifi modules.

Kind Regards

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mridul

Last Name: Malpotra

Mailing Address: mridul.malpotra@gmail.com

City: New Delhi

Country: India

State or Province: Delhi

ZIP/Postal Code: 110020

Email Address: mridul.malpotra@gmail.com

Organization Name:

Comment: The FCC,

Device firmware changes have been an important aspect to ensure that people have the freedom to flash and install what they desire. Being in a third world country myself, software like DD-WRT proves to be a boon, allowing custom firmware flashing for my wireless access point that gives me the freedom to tweak my modem to my feature requirement.

As a student, it helps me understand the open source firmware and help in the bug-fixing process. Having an open platform for router firmware ensures the quality of the code remains. Obfuscation does not bring security. Having an open platform gives researchers and developers the capability to make better, improved software that withstands the security requirements, while allowing users with a host of options.

The freedom of users to decide what they want is important and should not be neglected. I request you to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

The FCC,

Device firmware changes have been an important aspect to ensure that people have the freedom to flash and install what they desire. Being in a third world country myself, software like DD-WRT proves to be a boon, allowing custom firmware flashing for my wireless access point that gives me the freedom to tweak my modem to my feature requirement.

As a student, it helps me understand the open source firmware and help in the bug-fixing process. Having an open platform for router firmware ensures the quality of the code remains. Obfuscation does not bring security. Having an open platform gives researchers and developers the capability to make better, improved software that withstands the security requirements, while allowing users with a host of options.

The freedom of users to decide what they want is important and should not be neglected. I request you to not implement rules that take away the ability of users to install the software of their choosing on their computing 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: Erica

Last Name: Moore

Mailing Address: 11989 Coverstone Hill Circle

City: Manassas

Country: United States

State or Province: VA

ZIP/Postal Code: 20109

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

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: Alberto

Last Name: Trevino

Mailing Address: 1532 Mountain View Dr.

City: Spanish Fork

Country: United States

State or Province: UT

ZIP/Postal Code: 84660

Email Address: alf@mypals.org

Organization Name: Private citizen

Comment: I don't see why the government needs to be approving software updates on RF devices. For home 802.11 wireless, that would mean extra hurdles for open source router firmware. This has two problems:

1. Older devices known to have defective software could not be updated after the manufacturer has abandoned the product.
2. The requirement to run only approved software is very suspicious when other government agencies are demanding backdoors into encryption algorithms or equipment.

I fail to see what the harm really is. Suppose someone modifies the software on any transmission device to broadcast either outside its allowed frequencies or at a higher power than allowed. Any possible interference caused by the offending parties could be reported back to the FCC and then handled by you, right? Yet the losses to being unable to use open source software on these modules would be much, much greater than the possible abuse. Yet another case of government's cure being worse than the disease.

I don't see why the government needs to be approving software updates on RF devices. For home 802.11 wireless, that would mean extra hurdles for open source router firmware. This has two problems:

1. Older devices known to have defective software could not be updated after the manufacturer has abandoned the product.
2. The requirement to run only approved software is very suspicious when other government agencies are demanding backdoors into encryption algorithms or equipment.

I fail to see what the harm really is. Suppose someone modifies the software on any transmission device to broadcast either outside its allowed frequencies or at a higher power than allowed. Any possible interference caused by the offending parties could be reported back to the FCC and then handled by you, right? Yet the losses to being unable to use open source software on these modules would be much, much greater than the possible abuse. Yet another case of government's cure being worse than the disease.

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: Jay

Last Name: Patel

Mailing Address: 1389 Glenside Drive

City: Bolingbrook

Country: United States

State or Province: IL

ZIP/Postal Code: 60490

Email Address: 3yearoldgenius@Gmail.com

Organization Name:

Comment: This regulation is excessive and anti-open source. It should be rejected.

This regulation is excessive and anti-open source. It should be rejected.