

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: Huffman

Mailing Address: 527 Saint Michael Dr

City: Middletown

Country: United States

State or Province: DE

ZIP/Postal Code: 19709

Email Address:

Organization Name:

Comment: I agree the regulations need to be kept up to date, however the proposed standard is going to impose many limitations that will stifle innovation. The ability to modify the software running a wireless device is needed to allow security holes to be fixed and features to be added after the hardware manufacture has stopped. Hardware manufactures will only support a device for as long as it is profitable not for the real length of hardware reliability. Modifying the software allows the consumer to extend the life of the hardware and keep it secure for a longer duration. Any regulations that would prevent users from writing or modifying the software on a wifi device will be a detriment to the networking community.

I agree the regulations need to be kept up to date, however the proposed standard is going to impose many limitations that will stifle innovation. The ability to modify the software running a wireless device is needed to allow security holes to be fixed and features to be added after the hardware manufacture has stopped. Hardware manufactures will only support a device for as long as it is profitable not for the real length of hardware reliability. Modifying the software allows the consumer to extend the life of the hardware and keep it secure for a longer duration. Any regulations that would prevent users from writing or modifying the software on a wifi device will be a detriment to the networking community.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Marco Antonio

Last Name: Marroquin

Mailing Address: Velzquez de Len 40 F

City: Acapulco

Country: Mexico

State or Province: Gro

ZIP/Postal Code: 39300

Email Address: fotodamaris@hotmail.com

Organization Name: Foto Damaris

Comment: FCC your new rule about third party firmwares will affect many, we use third party firmware cause stock firmware works with flaws, even expensive routers have flaws, only way to correct it is by flashing a third party firmware.

FCC your new rule about third party firmwares will affect many, we use third party firmware cause stock firmware works with flaws, even expensive routers have flaws, only way to correct it is by flashing a third party 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: Bruce

Last Name: Stockwell

Mailing Address: 107 Grant Street

City: Plainfield

Country: United States

State or Province: MA

ZIP/Postal Code: 01070

Email Address:

Organization Name:

Comment: Dear Sir or Madam:

We respectfully request you do NOT implement the proposed WiFi firmware rules you are considering.

1. The IOT (Internet of Things) marketplace would be significantly stifled and impaired.
2. The research, development and expansion of WiFi depends on the ability of researchers to investigate and modify their devices. This affects all people in all industries.
3. People must have the ability to alter firmware for security reasons, as well! (serious bugs or security issues in their wifi drivers) This would be banned under the NPRM.
4. Research, development and implementation of WiFi devices would be devastated.
5. The economic impact to the USA would be substantial!

We have enough issues to deal with now, without having our hands tied any further.

Thank you for your consideration.

Respectfully submitted by:

Bruce Stockwell
107 Grant Street
Plainfield, Ma 01070

Dear Sir or Madam:

We respectfully request you do NOT implement the proposed WiFi firmware rules you are considering.

1. The IOT (Internet of Things) marketplace would be significantly stifled and impaired.
2. The research, development and expansion of WiFi depends on the ability of researchers to investigate and modify their devices. This affects all people in all industries.

3. People must have the ability to alter firmware for security reasons, as well! (serious bugs or security issues in their wifi drivers) This would be banned under the NPRM.

4. Research, development and implementation of WiFi devices would be devastated.

5. The economic impact to the USA would be substantial!

We have enough issues to deal with now, without having our hands tied any further.

Thank you for your consideration.

Respectfully submitted by:

Bruce Stockwell
107 Grant Street
Plainfield, Ma 01070

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: Joseph

Last Name: Henderson

Mailing Address: 3908 Westporter Drive

City: Sacramento

Country: United States

State or Province: CA

ZIP/Postal Code: 95826

Email Address: gnufreeme@hushmail.com

Organization Name:

Comment: I'm against locking out third party software from wifi/sdr devices for the same reason I'm against lock out in all other devices. It stifles innovation and at the same time will not accomplish the goals it seeks. Those who wilfully violate are smart enough to circumvent this proposed rule change but this will have a chilling effect on the growth of this important public space.

We the people need the ability to invent our way out of problems and need regulatory bodies to design schemes that have that important public interest in mind. To do this we need access to the source code we use in our lives and the ability to modify and share. Does anyone deny the effect this process has had on technology with the growth of GNU/Linux, Bitcoin and other such free/open tech?

A good example of coming innovation in this field is the next generation of internet access using mesh networking. This is too important to the future of humanity to allow potential roadblocks & stifle this ultimate goal of a free-to-use internet made up of mesh nodes running free software.

Also people who want to use all free/open-source technology deserve to be able to communicate with their friends in our world without being forced to use secret specs/firmware, etc.

Thank you for your time and consideration and urge you to deny this proposal and work with the tech community. We can solve many problems in a clever but still freedom-respecting way. Let us fix it.

I'm against locking out third party software from wifi/sdr devices for the same reason I'm against lock out in all other devices. It stifles innovation and at the same time will not accomplish the goals it seeks. Those who wilfully violate are smart enough to circumvent this proposed rule change but this will have a chilling effect on the growth of this important public space.

We the people need the ability to invent our way out of problems and need regulatory bodies to design schemes that have that important public interest in mind. To do this we need access to the source code we use in our lives and the ability to modify and share. Does anyone deny the effect this process has had on technology with the growth of GNU/Linux, Bitcoin and other such free/open tech?

A good example of coming innovation in this field is the next generation of internet access using mesh networking. This is too important to the future of humanity to allow potential roadblocks & stifle this ultimate goal of a free-to-use internet made up of mesh nodes running free software.

Also people who want to use all free/open-source technology deserve to be able to communicate with their friends in our world without being forced to use secret specs/firmware, etc.

Thank you for your time and consideration and urge you to deny this proposal and work with the tech community. We can solve many problems in a clever but still freedom-respecting way. Let us fix it.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ty

Last Name: Brown

Mailing Address: 1652 Electric Avenue

City: Crofton

Country: United States

State or Province: MD

ZIP/Postal Code: 21114

Email Address: tybrowniv@gmail.com

Organization Name: DET5 Labs

Comment: It is very important to note that this is not in the best interests of the customer.

For almost two decades, these proposed regulations have not been in place. The result has been an explosion of benefits, for the customer, writ large.

Keep in mind that when I say "The Customer", I mean private citizens, corporations, government, public safety, inventors, and students. All walks of life.

Mandating a locked down firmware/software layer on wireless devices is literally removing innovation, and giving corporate interests a lock on this technology. This is a growing trend in technology that is going to destroy open development at the expense of (short term) profits. In the long term, overseas development will continue, possibly at an even faster pace.

Please, do not allow these rule changes to take place.

It is very important to note that this is not in the best interests of the customer.

For almost two decades, these proposed regulations have not been in place. The result has been an explosion of benefits, for the customer, writ large.

Keep in mind that when I say "The Customer", I mean private citizens, corporations, government, public safety, inventors, and students. All walks of life.

Mandating a locked down firmware/software layer on wireless devices is literally removing innovation, and giving corporate interests a lock on this technology. This is a growing trend in technology that is going to destroy open development at the expense of (short term) profits. In the long term, overseas development will continue, possibly at an even faster pace.

Please, do not allow these rule changes to take place.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Dmitry

Last Name: Khudyakov

Mailing Address: st.Zarechnaya 20. r.145

City: Balashikha

Country: Russia

State or Province: Mos. Area

ZIP/Postal Code: 143905

Email Address:

Organization Name:

Comment: I think its stupid idea.

I think its stupid idea.

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: Filipe

Last Name: Polido

Mailing Address: Leiria

City: Leiria

Country: Portugal

State or Province: PT

ZIP/Postal Code: 2400

Email Address: polido@gmail.com

Organization Name:

Comment: Dear Sir.

Sorry in advance for any mistakes, English is not my natural language.

Please consider this proposal.

I have installed hundreds of wireless devices as part of my day job.

If we had to rely on original firmware it would give us a lot of problems as the manufacturer doesn't update and fix security issues.

So please, let projects like DD-WRT make our life (technicians) easier.

We've seen countless reports where security through obscurity doesn't work, making illegal for us to find bugs and use different firmware will increase attacks in long terms.

I understand that changing radio features is problematic, but, consider the proposal to lock only the radio, not the firmware itself.

Many companies have a SoC, so locking radio without locking the rest of the system is almost impossible. I believe that companies should be obligated to fix security bugs in time at least.

On a side note, 80% of original firmware just plain sucks and it's very limited.

Thank you for your attention.

Dear Sir.

Sorry in advance for any mistakes, English is not my natural language.

Please consider this proposal.

I have installed hundreds of wireless devices as part of my day job.

If we had to rely on original firmware it would give us a lot of problems as the manufacturer doesn't update and fix security issues.

So please, let projects like DD-WRT make our life (technicians) easier.

We've seen countless reports where security through obscurity doesn't work, making illegal for us to find bugs and use different firmware will increase attacks in long terms.

I understand that changing radio features is problematic, but, consider the proposal to lock only the radio, not the firmware itself.

Many companies have a SoC, so locking radio without locking the rest of the system is almost impossible. I believe that companies should be obligated to fix security bugs in time at least.

On a side note, 80% of original firmware just plain sucks and it's very limited.

Thank you for your attention.

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: tobias

Last Name: saunders

Mailing Address: 11 Acacia Road

City: London

Country: United Kingdom

State or Province: London

ZIP/Postal Code: CR4 1SF

Email Address: fcc@tdos.co.uk

Organization Name:

Comment: I think this is a bad idea and will stifle innovation.

I think this is a bad idea and will 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: Ronald

Last Name: Lipsi

Mailing Address: 347 Mingle Inn Road

City: Berwick

Country: United States

State or Province: PA

ZIP/Postal Code: 18603

Email Address: barblipsi@yahoo.com

Organization Name: Mrs.

Comment: Please do not take away the ability of the consumer to add software of their choosing to devices they own. If you do this, it will stifle future technological advances into wireless devices as the creators need to be able to legally modify their devices. Not only that but you will be denying device owners the right to fix security issues with their devices when manufacturers are unwilling or unable to do so. This can only make us more vulnerable.

Thank you for your time and consideration.

Please do not take away the ability of the consumer to add software of their choosing to devices they own. If you do this, it will stifle future technological advances into wireless devices as the creators need to be able to legally modify their devices. Not only that but you will be denying device owners the right to fix security issues with their devices when manufacturers are unwilling or unable to do so. This can only make us more vulnerable.

Thank you for your time and consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: federico

Last Name: la morgia

Mailing Address: federico.lamorgia@gmail.com

City: pescara

Country: Italy

State or Province: pescara

ZIP/Postal Code: 65123

Email Address: federico.lamorgia@gmail.com

Organization Name:

Comment: prego leggere anche se non scritto in inglese

<https://blog.ninux.org/2015/09/02/la-fcc-contro-i-firmware-open-source-fai-sentire-la-tua-voce/>

prego leggere anche se non scritto in inglese

<https://blog.ninux.org/2015/09/02/la-fcc-contro-i-firmware-open-source-fai-sentire-la-tua-voce/>

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: Maxim

Last Name: Vorontsov

Mailing Address: 4283 Express Lane

City: Sarasota

Country: United States

State or Province: FL

ZIP/Postal Code: 34238

Email Address: 6012030@gmail.com

Organization Name:

Comment: 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.

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: Marco

Last Name: Caselli

Mailing Address: Via G.Tomasi di Lampedusa 58

City: Caltanissetta

Country: Italy

State or Province: Caltanissetta

ZIP/Postal Code: 93100

Email Address: casellimarco@libero.it

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: Ilaria

Last Name: De Marinis

Mailing Address: Via dei Tizii 6

City: Rome

Country: Italy

State or Province: Italy

ZIP/Postal Code: 00185

Email Address: occhidaorientale@gmail.com

Organization Name:

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

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ipoo

Last Name: Roo

Mailing Address: 37 New Street

City: Pontypool

Country: United Kingdom

State or Province: Wales

ZIP/Postal Code: NP4 6LG

Email Address: ipooroo@hotmail.co.uk

Organization Name:

Comment: The freedom to do what we want with devices we owned will be infringed here!

What would make more sense is to limit what the actual HARDWARE can do, not the software.

The freedom to do what we want with devices we owned will be infringed here!

What would make more sense is to limit what the actual HARDWARE can do, not the software.

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: Keim

Mailing Address: 1940 S. 25th St.

City: Lincoln

Country: United States

State or Province: NE

ZIP/Postal Code: 68502

Email Address: email@jameskeim.com

Organization Name:

Comment: I would ask that you reconsider any action that might prohibit modifying the firmware on routers and wifi equipment. While the state of router firmware has improved and there are more wifi devices being sold with non-buggy firmware, this has not always been the case. I've had routers in the past that were terribly buggy and needed to be "reset" every few hours (unplugged and then plugged back in). The router company was not addressing the bugs in their firmware with any speed. I started using an open source firmware and found that people who were having similar problems addressed the bugs in the firmware and created very stable firmwares that prompted the companies to adopt their fixes.

Please don't punish people who are not running their routers outside of bandwidths approved by the FCC with a regulation that has such a serious impact on innovation. In fact, I have recently avoided the back door that was targeted by malicious hackers by using open source third-party firmware on the routers I administer.

Again, I respectfully request that you do not prohibit modification to router and wifi equipment firmware.

Thanks,
James Keim

I would ask that you reconsider any action that might prohibit modifying the firmware on routers and wifi equipment. While the state of router firmware has improved and there are more wifi devices being sold with non-buggy firmware, this has not always been the case. I've had routers in the past that were terribly buggy and needed to be "reset" every few hours (unplugged and then plugged back in). The router company was not addressing the bugs in their firmware with any speed. I started using an open source firmware and found that people who were having similar problems addressed the bugs in the firmware and created very stable firmwares that prompted the companies to adopt their fixes.

Please don't punish people who are not running their routers outside of bandwidths approved by the FCC with a regulation that has such a serious impact on innovation. In fact, I have recently avoided the back door that was targeted by malicious hackers by using open source third-party firmware on the routers I administer.

Again, I respectfully request that you do not prohibit modification to router and wifi equipment firmware.

Thanks,
James Keim

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: Gregg

Last Name: Levine

Mailing Address: 4-21 27 AVE APT10D

City: Astoria

Country: United States

State or Province: NY

ZIP/Postal Code: 11102

Email Address: gregg@levine,name

Organization Name:

Comment: Sirs,

I do not believe that this is an appropriate way to properly manage the spectrum that WiFi uses. The third party firmware that all of you mention by name simply replaces the typically poorly written commercial, and yes also open source, firmware, with one that is well written and properly documented.

It also stays well within the letter of the law concerning the spectrum that Wifi normally works in.

In fact, a lot of people, can and will view this as typical government meddling, and insist that all of you are infringing on their rights. To properly manage the region that your offices are concerned with would to be allow it, provided that each and every individual does not change any of the features enclosed inside his devices.

For example our routers use specific channels. The ones sold in Europe, use other channels, and the ones sold in Asia also use specific ones. We can not change our devices to use theirs.

A better method would be to make that function hardcoded into the routers, and have the specific vendors do so within a preset period of time.

Sirs,

I do not believe that this is an appropriate way to properly manage the spectrum that WiFi uses. The third party firmware that all of you mention by name simply replaces the typically poorly written commercial, and yes also open source, firmware, with one that is well written and properly documented.

It also stays well within the letter of the law concerning the spectrum that Wifi normally works in.

In fact, a lot of people, can and will view this as typical government meddling, and insist that all of you are infringing on their rights. To properly manage the region that your offices are concerned with would to be allow it, provided that each and every individual does not change any of the features enclosed inside his devices.

For example our routers use specific channels. The ones sold in Europe, use other channels, and the ones sold in Asia also use specific ones. We can not change our devices to use theirs.

A better method would be to make that function hardcoded into the routers, and have the specific vendors do so within a preset period of time.

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: Keith

Last Name: Konnerth

Mailing Address: 3817 Brendan Ln Apt 1

City: North Olmsted

Country: United States

State or Province: OH

ZIP/Postal Code: 44070

Email Address: einstine85@yahoo.com

Organization Name:

Comment: Dear Sirs/Madams,

I must respectfully request that the Commission reevaluate this rule.

As a licensed Amateur Radio operator, I am legally allowed to modify radios, especially to operate out of their intended frequency bands, weather the radio has been merely verified, been Declared to Conform, or been Certified.

These rules would greatly inhibit any Amateur licensee from modifying equipment for use in the authorized Amateur bands, and without experimentation and tinkering, it will be very hard to find new uses for older equipment, new methods of communication, and ways to reduce bandwidth needed to carry out communications.

Thank you for your time.

Keith Konnerth; KC8YJW

Dear Sirs/Madams,

I must respectfully request that the Commission reevaluate this rule.

As a licensed Amateur Radio operator, I am legally allowed to modify radios, especially to operate out of their intended frequency bands, weather the radio has been merely verified, been Declared to Conform, or been Certified.

These rules would greatly inhibit any Amateur licensee from modifying equipment for use in the authorized Amateur bands, and without experimentation and tinkering, it will be very hard to find new uses for older equipment, new methods of communication, and ways to reduce bandwidth needed to carry out communications.

Thank you for your time.

Keith Konnerth; KC8YJW

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: Shane

Last Name: Burkle

Mailing Address: 608 Portsmouth Ln

City: Foster City

Country: United States

State or Province: CA

ZIP/Postal Code: 94404

Email Address:

Organization Name:

Comment: This is a poor choice, I highly suggest you revisit this. DDWRT and OpenWRT have brought new features and life into consumer products that otherwise were crappy regurgitations of their parent companies that aimed to take the customer of his money while leaving him with an intentionally inferior product.

This is a poor choice, I highly suggest you revisit this. DDWRT and OpenWRT have brought new features and life into consumer products that otherwise were crappy regurgitations of their parent companies that aimed to take the customer of his money while leaving him with an intentionally inferior product.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Diego

Last Name: Villarreal

Mailing Address: 420 Plymouth Lane

City: Laredo

Country: United States

State or Province: TX

ZIP/Postal Code: 78041

Email Address: diegov00@gmail.com

Organization Name:

Comment: I urge the commission to reconsider the importance of having open-source hardware and to the consider the positives of flashing software independent from the manufacturers and the negatives of the forcing manufacturers to implement restrictions.

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.

Implementing restrictions means having to develop software and shifting resources and manpower currently being used to give the consumer a better experience. It means added costs that will force smaller companies to be less competitive and encouraging a monopolization by bigger companies as well as limiting new entries into the market.

Certain companies focus their market strategy on consumers who are only buying their products based on their flexibility to personally tweak with the software.

Custom software allows consumers to upgrade their hardware to optimize the slow network speeds offered by telecom companies who have refused to upgrade their networks to the higher standards available in other countries. Telecom companies are stifling American ingenuity by accepting stagnant network speeds in an effort to operate on 95% margins. As well as the FCC/FTC allowing major telecom companies merging making an effective cartel/monopoly. The proposed rule would be the final nail in the coffin when it comes to the internet.

This rule along with the other governmental decisions are effectively diminishing our right to free speech by turning the internet our greatest avenue to disseminate our opinions into a less effective system.

I urge the commission to reconsider the importance of having open-source hardware and to the consider the positives of flashing software independent from the manufacturers and the negatives of the forcing manufacturers to implement restrictions.

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.

Implementing restrictions means having to develop software and shifting resources and manpower currently being used to give the consumer a better experience. It means added costs that will force smaller companies to be less

competitive and encouraging a monopolization by bigger companies as well as limiting new entries into the market.

Certain companies focus their market strategy on consumers who are only buying their products based on their flexibility to personally tweak with the software.

Custom software allows consumers to upgrade their hardware to optimize the slow network speeds offered by telecom companies who have refused to upgrade their networks to the higher standards available in other countries. Telecom companies are stifling American ingenuity by accepting stagnant network speeds in an effort to operate on 95% margins. As well as the FCC/FTC allowing major telecom companies merging making an effective cartel/monopoly. The proposed rule would be the final nail in the coffin when it comes to the internet.

This rule along with the other governmental decisions are effectively diminishing our right to free speech by turning the internet our greatest avenue to disseminate our opinions into a less effective system.

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: Diego

Last Name: Villarreal

Mailing Address: 420 Plymouth Lane

City: Laredo

Country: United States

State or Province: TX

ZIP/Postal Code: 78041

Email Address: diegov00@gmail.com

Organization Name:

Comment: I urge the commission to reconsider the importance of having open-source hardware and to the consider the positives of flashing software independent from the manufacturers and the negatives of the forcing manufacturers to implement restrictions.

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.

Implementing restrictions means having to develop software and shifting resources and manpower currently being used to give the consumer a better experience. It means added costs that will force smaller companies to be less competitive and encouraging a monopolization by bigger companies as well as limiting new entries into the market.

Certain companies focus their market strategy on consumers who are only buying their products based on their flexibility to personally tweak with the software.

Custom software allows consumers to upgrade their hardware to optimize the slow network speeds offered by telecom companies who have refused to upgrade their networks to the higher standards available in other countries. Telecom companies are stifling American ingenuity by accepting stagnant network speeds in an effort to operate on 95% margins. As well as the FCC/FTC allowing major telecom companies merging making an effective cartel/monopoly. The proposed rule would be the final nail in the coffin when it comes to the internet.

This rule along with the other governmental decisions are effectively diminishing our right to free speech by turning the internet our greatest avenue to disseminate our opinions into a less effective system.

I urge the commission to reconsider the importance of having open-source hardware and to the consider the positives of flashing software independent from the manufacturers and the negatives of the forcing manufacturers to implement restrictions.

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.

Implementing restrictions means having to develop software and shifting resources and manpower currently being used to give the consumer a better experience. It means added costs that will force smaller companies to be less

competitive and encouraging a monopolization by bigger companies as well as limiting new entries into the market.

Certain companies focus their market strategy on consumers who are only buying their products based on their flexibility to personally tweak with the software.

Custom software allows consumers to upgrade their hardware to optimize the slow network speeds offered by telecom companies who have refused to upgrade their networks to the higher standards available in other countries. Telecom companies are stifling American ingenuity by accepting stagnant network speeds in an effort to operate on 95% margins. As well as the FCC/FTC allowing major telecom companies merging making an effective cartel/monopoly. The proposed rule would be the final nail in the coffin when it comes to the internet.

This rule along with the other governmental decisions are effectively diminishing our right to free speech by turning the internet our greatest avenue to disseminate our opinions into a less effective system.

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: Garrett

Last Name: Gregor

Mailing Address: 3601 Arapahoe Avenue

City: Boulder

Country: United States

State or Province: CO

ZIP/Postal Code: 80303

Email Address: garrett.gregor@gmail.com

Organization Name:

Comment: I respectfully ask that the FCC 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.

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brandon

Last Name: Whaley

Mailing Address: 610 W Princess Anne Rd

City: Norfolk

Country: United States

State or Province: VA

ZIP/Postal Code: 23517-1835

Email Address: redkrieg@gmail.com

Organization Name:

Comment: As a consumer whose budget precludes me from purchasing enterprise grade equipment and support, I am forced to use consumer grade equipment for my home wireless needs. This equipment tends to last 4-10 years in my experience, but software support for home equipment rarely goes more than two. When vulnerabilities in these devices are discovered, it can often take months to get a vendor to release a new firmware update to address the issue. In the case of older equipment, it is likely to never happen. For this reason, I have used open source firmware on all of my and my family's routers. Updates are easy to get and help ensure that my equipment cannot be compromised due to some known vulnerability, even when that equipment is well over 5 years old. I understand that using the radios in a non-standards compliant way is possible with this software, but I have never done so, and I think the warnings in most custom software's interfaces are sufficient to prevent someone from violating FCC guidelines in the US unknowingly. If someone does exceed the intended radio parameters of the device, I believe the FCC should take action. Modifications with an effect strong enough to interfere with nearby radios should be easy to locate with even amateur-grade equipment today. Please do not put rules in to effect that prevent valid and arguably necessary hobbyist use of this affordable equipment in the future.

As a consumer whose budget precludes me from purchasing enterprise grade equipment and support, I am forced to use consumer grade equipment for my home wireless needs. This equipment tends to last 4-10 years in my experience, but software support for home equipment rarely goes more than two. When vulnerabilities in these devices are discovered, it can often take months to get a vendor to release a new firmware update to address the issue. In the case of older equipment, it is likely to never happen. For this reason, I have used open source firmware on all of my and my family's routers. Updates are easy to get and help ensure that my equipment cannot be compromised due to some known vulnerability, even when that equipment is well over 5 years old. I understand that using the radios in a non-standards compliant way is possible with this software, but I have never done so, and I think the warnings in most custom software's interfaces are sufficient to prevent someone from violating FCC guidelines in the US unknowingly. If someone does exceed the intended radio parameters of the device, I believe the FCC should take action. Modifications with an effect strong enough to interfere with nearby radios should be easy to locate with even amateur-grade equipment today. Please do not put rules in to effect that prevent valid and arguably necessary hobbyist use of this affordable equipment in the future.

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: Nicolaus

Last Name: Eddy

Mailing Address: 3057 Whites Chapel Parkway

City: Trussville

Country: United States

State or Province: AL

ZIP/Postal Code: 35173

Email Address: nicolaus.eddy@gmail.com

Organization Name:

Comment: Please do not lock down our networking hardware. Open source router firmware (such as DD-WRT) support is a main purchasing point for millions of tinkerer/power-users to make an automated home network. Taking away this freedom leaves us to rely on OEM firmware that is rarely updated and often featureless. Some OEM firmware is even have known security bugs that are never fixed. Open source firmware allows for patching of these issues and standards to be implemented much quicker and easier.

Please do not lock down our networking hardware. Open source router firmware (such as DD-WRT) support is a main purchasing point for millions of tinkerer/power-users to make an automated home network. Taking away this freedom leaves us to rely on OEM firmware that is rarely updated and often featureless. Some OEM firmware is even have known security bugs that are never fixed. Open source firmware allows for patching of these issues and standards to be implemented much quicker and easier.

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: Philip

Last Name: Smith

Mailing Address: 6021 California Ave SW

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98136

Email Address: phil.h.smith@gmail.com

Organization Name:

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

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

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

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

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

Consider the industry of after-market modifications for cars, which demonstrates the perfectly feasible harmony that can exist between user customizations and the (very necessary) laws ensuring proper operation and our safety. There is no need to outlaw the industry, but merely to stop offenders as they are found.

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.

Consider the industry of after-market modifications for cars, which demonstrates the perfectly feasible harmony that can exist between user customizations and the (very necessary) laws ensuring proper operation and our safety. There is no need to outlaw the industry, but merely to stop offenders as they are 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: Jackson

Last Name: Thatcher

Mailing Address: 1708 West South Fork Drive

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 858045

Email Address: tomtommy7066@gmail.com

Organization Name:

Comment: This could be a huge poential security threat, being stuck with the same firmware for the life of a product opens the door to massive security issues. Also, if the law extends to phones and other integrated devices it hinders the ability of consumers to upgrade or modify their firmware in ways that are totally benign to wireless communications.

This could be a huge poential security threat, being stuck with the same firmware for the life of a product opens the door to massive security issues. Also, if the law extends to phones and other integrated devices it hinders the ability of consumers to upgrade or modify their firmware in ways that are totally benign to wireless communications.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: john

Last Name: vanbuskirk

Mailing Address: 1820 W Lindner Ave

City: Mesa

Country: United States

State or Province: AZ

ZIP/Postal Code: 85202

Email Address: jvanb231@gmail.com

Organization Name:

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

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

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Tannenbaum

Mailing Address: 1510 Clay St

City: Oakland

Country: United States

State or Province: CA

ZIP/Postal Code: 94612

Email Address:

Organization Name:

Comment: Dear Federal Communications Commission of the United States,

I sincerely ask you not to implement this proposed rule as it would severely impact the freedom of Americans.

If this rule passes, Americans will no longer be able to fix crucial security bugs in their devices.

In the past, many users and researchers have used the ability to modify their devices to fix crucial problems that were completely ignored by the device manufacturers.

It is also important to understand that a lot of commerce, such as WiFi vendors and public hotspot vendors, depend on the ability of their users to install the software of their choosing. Passing the rule would take away millions of commerce dollars.

I hope you will understand the points that I have brought up and do not proceed with the implementation of this rule. Thank you.

Dear Federal Communications Commission of the United States,

I sincerely ask you not to implement this proposed rule as it would severely impact the freedom of Americans.

If this rule passes, Americans will no longer be able to fix crucial security bugs in their devices.

In the past, many users and researchers have used the ability to modify their devices to fix crucial problems that were completely ignored by the device manufacturers.

It is also important to understand that a lot of commerce, such as WiFi vendors and public hotspot vendors, depend on the ability of their users to install the software of their choosing. Passing the rule would take away millions of commerce dollars.

I hope you will understand the points that I have brought up and do not proceed with the implementation of this rule. Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ross

Last Name: Fisher

Mailing Address: 612 Anchor Drive 101

City: Lafayette

Country: United States

State or Province: IN

ZIP/Postal Code: 47905

Email Address: zorrobyte@gmail.com

Organization Name:

Comment: What, seriously? I have to deal with manufacturers of my electronic goods stripping my rights from using my devices as I see fit for educational and personal uses, and now the FCC wants to further clamp down?

What is this about restricting my ability to install a free and open source operating system on my own personal computer, that I built from scratch? My cell phone which I would have no use for unless I am free to install my own software? Several of my routers that I have tweaked and installed open source software on (that would of otherwise of been trashed)?

I completely fail to see how this change would positively impact anyone but the companies manufacturing the devices by giving them free range to further planned obsolescence, wasting our limited natural resources and further toxifying our planet with additional electronic waste. Seriously, again who is shoveling money into the FCC's pockets to warrant such an insane change?

What, seriously? I have to deal with manufacturers of my electronic goods stripping my rights from using my devices as I see fit for educational and personal uses, and now the FCC wants to further clamp down?

What is this about restricting my ability to install a free and open source operating system on my own personal computer, that I built from scratch? My cell phone which I would have no use for unless I am free to install my own software? Several of my routers that I have tweaked and installed open source software on (that would of otherwise of been trashed)?

I completely fail to see how this change would positively impact anyone but the companies manufacturing the devices by giving them free range to further planned obsolescence, wasting our limited natural resources and further toxifying our planet with additional electronic waste. Seriously, again who is shoveling money into the FCC's pockets to warrant such an insane change?

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: Jean-Michel

Last Name: Briault

Mailing Address: 40 hbert

City: Gatineau

Country: Canada

State or Province: Quebec

ZIP/Postal Code: J8P6B7

Email Address: jmberiault@gmail.com

Organization Name:

Comment: This is bull, in no way do we need even more locks on our hardware, why are we making 1 step forward and 2 steps back again, in this day and age?

I like to be in control of my hardware and not the other way around.

This is bull, in no way do we need even more locks on our hardware, why are we making 1 step forward and 2 steps back again, in this day and age?

I like to be in control of my hardware and not the other way around.

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: Timur

Last Name: Kospanov

Mailing Address: Gagarin str. 235-3

City: Almaty

Country: Kazakhstan

State or Province: None (International)

ZIP/Postal Code: 050060

Email Address: kospanov@gmail.com

Organization Name: aquaservice

Comment: Freedom

Freedom

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: Ronald

Last Name: Bandish JR

Mailing Address: 3632 south 55th Ave

City: Cicero

Country: United States

State or Province: IL

ZIP/Postal Code: 60804

Email Address: Ronbandish@gmail.com

Organization Name:

Comment: Hello,

As someone who is concerned about this I want to let you know that this would really mess up alot of stuff if it become official. Am currently a student who is studying IT with networking being a main focus that am studying. With this law it would really make it harder to fix many different networks without modifying it. Sometime the company that make these hardware don't even want to fix any problems on their own leaving the customers to find ways to fix it themselves. Also consider the following....

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.

So please think twice about passing this rule.

From,

Ronald R Bandish JR

Hello,

As someone who is concerned about this I want to let you know that this would really mess up alot of stuff if it become official. Am currently a student who is studying IT with networking being a main focus that am studying. With this law it would really make it harder to fix many different networks without modifying it. Sometime the company that make these hardware don't even want to fix any problems on their own leaving the customers to find ways to fix it themselves. Also consider the following....

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.

So please think twice about passing this rule.

From,

Ronald R Bandish JR

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matt

Last Name: Whitted

Mailing Address: 6618 Brownfield Dr.

City: Parma

Country: United States

State or Province: OH

ZIP/Postal Code: 44129

Email Address:

Organization Name:

Comment: I respectfully ask the Commission to not implement rules requiring manufacturers to restrict the software that can be installed on hardware devices. As an I.T. and electronics professional, much of what I have learned is by experimentation. I would not be where I am today without many open source tools that may not have been possible without unrestricted hardware.

Please consider that that many emerging industries and the growing "maker" culture rely on open hardware for design and inexpensive prototyping, and that a vast majority of those who run third party software on hardware devices are doing so while following the rules.

Thank you for your consideration.

I respectfully ask the Commission to not implement rules requiring manufacturers to restrict the software that can be installed on hardware devices. As an I.T. and electronics professional, much of what I have learned is by experimentation. I would not be where I am today without many open source tools that may not have been possible without unrestricted hardware.

Please consider that that many emerging industries and the growing "maker" culture rely on open hardware for design and inexpensive prototyping, and that a vast majority of those who run third party software on hardware devices are doing so while following the rules.

Thank you for your consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ricardo

Last Name: Cabrita

Mailing Address: ricardojacabrita@gmail.com

City: Silves

Country: Portugal

State or Province: Faro

ZIP/Postal Code: 8365

Email Address: ricardojacabrita@gmail.com

Organization Name: null

Comment: Gentlemen, good night.

Due to the recent published proposal on "Equipment Authorization and Electronic Labeling for Wireless" I feel compelled to write to you from Portugal.

The implications of this proposal are terrifying, the ability to control our own computing devices is of utmost importance and should be an established right.

Without that ability it will be impossible to research and patch security holes often disregarded by manufacturers making devices, businesses and users alike much more exposed to cyber-security threats, the amount of electronic waste will significantly go up as the devices will be much less versatile, plenty of businesses will take a giant hit as they are dependent on the ability to run software of their choosing and the user's overall freedom will be terribly compromised.

The people need the right to decide which software they run, please do not take that right away. Please reconsider.

Best regards.

Gentlemen, good night.

Due to the recent published proposal on "Equipment Authorization and Electronic Labeling for Wireless" I feel compelled to write to you from Portugal.

The implications of this proposal are terrifying, the ability to control our own computing devices is of utmost importance and should be an established right.

Without that ability it will be impossible to research and patch security holes often disregarded by manufacturers making devices, businesses and users alike much more exposed to cyber-security threats, the amount of electronic waste will significantly go up as the devices will be much less versatile, plenty of businesses will take a giant hit as they are dependent on the ability to run software of their choosing and the user's overall freedom will be terribly compromised.

The people need the right to decide which software they run, please do not take that right away. Please reconsider.

Best regards.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Caleb

Last Name: Godwin

Mailing Address: 6718 Dam Number 4 Rd.

City: Sharpsburg

Country: United States

State or Province: MD

ZIP/Postal Code: 21782

Email Address:

Organization Name:

Comment: Although I understand the desire to restrict custom radio firmware, it is necessary to look at the ramifications of these proposed measures.

These measures could effectively restrict or ban the installation of open source operating systems such as GNU/Linux, OpenBSD, and FreeBSD on the PCs and laptops that we have paid for. This is an important ability for people who care about software freedom and the privacy-conscious.

Furthermore, these measures would prevent individuals from installing custom firmware on Android phones. This, again, is a matter of importance for the privacy-conscious and free software advocates, as open source alternatives to Android such as Replicant exist to free a user's device.

In short, the proposed measures would end up further restricting what an end-user can do with his or her devices. For many, phones and computers are not simply appliances, but devices that can run any software that the user wishes.

It is important to maintain every freedom that we can.

Although I understand the desire to restrict custom radio firmware, it is necessary to look at the ramifications of these proposed measures.

These measures could effectively restrict or ban the installation of open source operating systems such as GNU/Linux, OpenBSD, and FreeBSD on the PCs and laptops that we have paid for. This is an important ability for people who care about software freedom and the privacy-conscious.

Furthermore, these measures would prevent individuals from installing custom firmware on Android phones. This, again, is a matter of importance for the privacy-conscious and free software advocates, as open source alternatives to Android such as Replicant exist to free a user's device.

In short, the proposed measures would end up further restricting what an end-user can do with his or her devices. For many, phones and computers are not simply appliances, but devices that can run any software that the user wishes.

It is important to maintain every freedom that we can.

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: Bove

Mailing Address: 30777 S Highway 1

City: Gualala

Country: United States

State or Province: CA

ZIP/Postal Code: 95445

Email Address:

Organization Name:

Comment: Please do not make it so that users cannot install new software of choosing on their computers, routers, radios, etc.

I am a Linux user who depends on the ability to install Linux on my computer, in order to have an operating system that I am comfortable with and does everything I need it to.

For example, the music production I do in Linux cannot be done on Mac or Windows without spending thousands of dollars I don't have on extra equipment.

Another example: sometimes the software/firmware installed on any given router is not good enough for the applications that said router can and should be fully capable of. If I wanted to set up Wake-On-LAN on my desktop computer (to save power and yet still be able to use it via RDP or VNC) and it lived behind a router, I would need said router to be able to send the magic packet over broadcast instead of a specific IP address. Some router software does not support this, even though all hardware does.

This problem affects a lot of other people in other ways, too:

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

Please do not make it so that users cannot install new software of choosing on their computers, routers, radios, etc.

I am a Linux user who depends on the ability to install Linux on my computer, in order to have an operating system that I am comfortable with and does everything I need it to.

For example, the music production I do in Linux cannot be done on Mac or Windows without spending thousands of dollars I don't have on extra equipment.

Another example: sometimes the software/firmware installed on any given router is not good enough for the applications that said router can and should be fully capable of. If I wanted to set up Wake-On-LAN on my desktop computer (to save power and yet still be able to use it via RDP or VNC) and it lived behind a router, I would need said router to be able to send the magic packet over broadcast instead of a specific IP address. Some router software does not support this, even though all hardware does.

This problem affects a lot of other people in other ways, too:

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Bove

Mailing Address: 30777 S Highway 1

City: Gualala

Country: United States

State or Province: CA

ZIP/Postal Code: 95445

Email Address:

Organization Name:

Comment: Please do not make it so that users cannot install new software of choosing on their computers, routers, radios, etc.

I am a Linux user who depends on the ability to install Linux on my computer, in order to have an operating system that I am comfortable with and does everything I need it to.

For example, the music production I do in Linux cannot be done on Mac or Windows without spending thousands of dollars I don't have on extra equipment.

Another example: sometimes the software/firmware installed on any given router is not good enough for the applications that said router can and should be fully capable of. If I wanted to set up Wake-On-LAN on my desktop computer (to save power and yet still be able to use it via RDP or VNC) and it lived behind a router, I would need said router to be able to send the magic packet over broadcast instead of a specific IP address. Some router software does not support this, even though all hardware does.

This problem affects a lot of other people in other ways, too:

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

Please do not make it so that users cannot install new software of choosing on their computers, routers, radios, etc.

I am a Linux user who depends on the ability to install Linux on my computer, in order to have an operating system that I am comfortable with and does everything I need it to.

For example, the music production I do in Linux cannot be done on Mac or Windows without spending thousands of dollars I don't have on extra equipment.

Another example: sometimes the software/firmware installed on any given router is not good enough for the applications that said router can and should be fully capable of. If I wanted to set up Wake-On-LAN on my desktop computer (to save power and yet still be able to use it via RDP or VNC) and it lived behind a router, I would need said router to be able to send the magic packet over broadcast instead of a specific IP address. Some router software does not support this, even though all hardware does.

This problem affects a lot of other people in other ways, too:

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Christisen

Mailing Address: 279 Cresthill Circle

City: Valley Mills

Country: United States

State or Province: TX

ZIP/Postal Code: 76689

Email Address: mchristisen@yahoo.com

Organization Name: n/a

Comment: Hello FCC,

I depend on modifying the firmware in my 5GHz routers. Modified firmware allows me to implement tight firewalls and content filtering not available in most consumer grade routers. Additionally, being able to modify the firmware in my routing devices allows me to throttle traffic on my network, which is another feature not typically found on consumer products. This feature allows me to prevent overages on my data plan.

Being able to modify the firmware on 5GHz routers (as well as other frequency ranges) is essential to me and I do not want regulation put in place that would attempt to prevent me from doing so.

Thank you,

Matt

Hello FCC,

I depend on modifying the firmware in my 5GHz routers. Modified firmware allows me to implement tight firewalls and content filtering not available in most consumer grade routers. Additionally, being able to modify the firmware in my routing devices allows me to throttle traffic on my network, which is another feature not typically found on consumer products. This feature allows me to prevent overages on my data plan.

Being able to modify the firmware on 5GHz routers (as well as other frequency ranges) is essential to me and I do not want regulation put in place that would attempt to prevent me from doing so.

Thank you,

Matt

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 van tate

Last Name: testa

Mailing Address: 340 Carrick Way

City: Macon

Country: United States

State or Province: GA

ZIP/Postal Code: 31210

Email Address: toast27@gmail.com

Organization Name: n/a

Comment: This is unnesscessary, why would you restrict my freedom to run any operating system or firmware don't the hardware which I purchased. This will help contribute to America loosing kits position as a tech and engineering global power.

This is unnesscessary, why would you restrict my freedom to run any operating system or firmware don't the hardware which I purchased. This will help contribute to America loosing kits position as a tech and engineering global power.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jared

Last Name: Buckenberger

Mailing Address: 20813 2nd ave so

City: Des Moines

Country: United States

State or Province: WA

ZIP/Postal Code: 98198

Email Address: buckey206@gmail.com

Organization Name:

Comment: Do not take away consumer ability to install the software of their choosing on their devices. Americans need the ability to do as they wish with their devices.

Do not take away consumer ability to install the software of their choosing on their devices. Americans need the ability to do as they wish with their 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: Duke

Last Name: Glover

Mailing Address: 375 East Allen Street

City: Castle Rock

Country: United States

State or Province: CO

ZIP/Postal Code: 80108

Email Address:

Organization Name:

Comment: We should have the ability to control the devices we rightly own. Unless major retailers are planning on dropping the price of our products by a substantial amount, the inability to change certain core aspects of the technology we buy, such as flashing firmware, should be something that is allowed. DO NOT allow the FCC to ban this type of hardware administration. It is an essential part of our freedom to be able to do what we please with the technology we rightfully own.

We should have the ability to control the devices we rightly own. Unless major retailers are planning on dropping the price of our products by a substantial amount, the inability to change certain core aspects of the technology we buy, such as flashing firmware, should be something that is allowed. DO NOT allow the FCC to ban this type of hardware administration. It is an essential part of our freedom to be able to do what we please with the technology we rightfully own.