

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: Luis

Last Name: Rodas

Mailing Address: 385 Eppd Bridge Road unit 17

City: Athens

Country: United States

State or Province: GA

ZIP/Postal Code: 30606

Email Address: LuisRRodas@gmail.com

Organization Name: null

Comment: No. I am not renting the device in question, I am purchasing it. If I want to change anything about it I should be able to. I decide that not the seller or manufacture.

No. I am not renting the device in question, I am purchasing it. If I want to change anything about it I should be able to. I decide that not the seller or manufacture.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Tang

Mailing Address: 1745 sw edgeing Dr.

City: Corvallis

Country: United States

State or Province: OR

ZIP/Postal Code: 97333

Email Address: Crazypizzak2@gmail.com

Organization Name: null

Comment: This is garbage. If I purchase a product I should be able to tweak it how I see fit. Year ago I bought a router and it functioned well for a while but began to have problems, I didn't want to shell out another 150\$ so I install dd-wrt a custom firmware. This bought my router back to life and I today I am happy with the performance. Same goes with outdated cell phones I have owned long ago, I was able to revive them by installing custom operating systems and use them long enough that the battery started to degrade. Locking down devices is a bad thing, not only is it going to upset people that like their things to be their things but it will contribute to the mind set that once something is broken you should buy a new one instead of fixing the perfectly good thing that you already have.

In this day and age a toilet with WiFi is likely to happen and I'd like to be able to unclog it regardless if I'm allowed to or not.

This ruling is garbage. Stop catering to large companies.

This is garbage. If I purchase a product I should be able to tweak it how I see fit. Year ago I bought a router and it functioned well for a while but began to have problems, I didn't want to shell out another 150\$ so I install dd-wrt a custom firmware. This bought my router back to life and I today I am happy with the performance. Same goes with outdated cell phones I have owned long ago, I was able to revive them by installing custom operating systems and use them long enough that the battery started to degrade. Locking down devices is a bad thing, not only is it going to upset people that like their things to be their things but it will contribute to the mind set that once something is broken you should buy a new one instead of fixing the perfectly good thing that you already have.

In this day and age a toilet with WiFi is likely to happen and I'd like to be able to unclog it regardless if I'm allowed to or not.

This ruling is garbage. Stop catering to large companies.

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: Darrien

Last Name: Glasser

Mailing Address: 617 Middlesex Turnpike

City: Billerica

Country: United States

State or Province: MA

ZIP/Postal Code: 01821

Email Address: darrienglasser@outlook.com

Organization Name: null

Comment: The idea of locking computers (mobile or not) down to specific and possibly proprietary operating systems is simply ridiculous. For those without the capital to afford proprietary operating systems, this makes home built computers (desktops or the like) impossible. And for those who would like to load alternative operating systems on their computer (GNU/Linux, BSD, etc.), or it is critical that they do so for their jobs, this proposal is twice as ridiculous. I'm currently typing this out right now, on my laptop, running Linux, and as a Computer Science Major (with a field eventually in the same area), it is essential that I'm able to run Linux, and other open source operating systems on my computer. Simply running the default OS would not be feasible.

Alternatively, when talking about mobile devices (e.g. smartphones, tablets, etc.), most mobile devices lose support from manufacturers after two years longest. For anybody looking to keep a mobile device for more than two years, or someone who buys a mobile device, say, a year after it is released, and then decides to keep it for two years, the ability to load third party/aftermarket OSes onto the device is very necessary, as older versions of the OS do not get security updates once the OEM stops supporting it.

Finally, putting in place such a rule would shut down projects like the Raspberry Pi (a singleboard computer that people can load any OS they want onto), which is used to teach computer science, and server fundamentals/simple programming to students and hobbyists. Such a rule would be hugely detrimental to those attempting to learn computer science on their own, and scrap many in-school projects where the learning is dependent on such devices, and their ability to load alternative operating systems on the device.

All in all, this rule is not feasible, and simply does not make sense to implement. It would disrupt far too much, with little to no gain.

The idea of locking computers (mobile or not) down to specific and possibly proprietary operating systems is simply ridiculous. For those without the capital to afford proprietary operating systems, this makes home built computers (desktops or the like) impossible. And for those who would like to load alternative operating systems on their computer (GNU/Linux, BSD, etc.), or it is critical that they do so for their jobs, this proposal is twice as ridiculous. I'm currently typing this out right now, on my laptop, running Linux, and as a Computer Science Major (with a field eventually in the same area), it is essential that I'm able to run Linux, and other open source operating systems on my computer. Simply running the default OS would not be feasible.

Alternatively, when talking about mobile devices (e.g. smartphones, tablets, etc.), most mobile devices lose support from manufacturers after two years longest. For anybody looking to keep a mobile device for more than two years, or someone who buys a mobile device, say, a year after it is released, and then decides to keep it for two years, the ability

to load third party/aftermarket OSes onto the device is very necessary, as older versions of the OS do not get security updates once the OEM stops supporting it.

Finally, putting in place such a rule would shut down projects like the Raspberry Pi (a singleboard computer that people can load any OS they want onto), which is used to teach computer science, and server fundamentals/simple programming to students and hobbyists. Such a rule would be hugely detrimental to those attempting to learn computer science on their own, and scrap many in-school projects where the learning is dependent on such devices, and their ability to load alternative operating systems on the device.

All in all, this rule is not feasible, and simply does not make sense to implement. It would disrupt far too much, with little to no gain.

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: tom

Last Name: lukeywood

Mailing Address: tomlukeywood@fastmail.co.uk

City: sheffield

Country: United Kingdom

State or Province: South Yorkshire

ZIP/Postal Code: s66fb

Email Address: tomlukeywood@fastmail.co.uk

Organization Name: null

Comment: I ask the FCC to not implement these rules that would stop people from changing the software on there routers.

if people have no means of changing the firmware on there router they will be unable to fix security holes in there device when the manufacturer will not do so.

users have in the past fixed serious security bug in there wifi drivers, which would be banned under the NPRM.

taking away peoples freedom to improve there routers firmware and to use the router as they wish is completely not necessary.

if users are using there routers in ways that would have a negative impact on RF transmissions then this behavior alone should be illegal.

I ask the FCC to not implement these rules that would stop people from changing the software on there routers.

if people have no means of changing the firmware on there router they will be unable to fix security holes in there device when the manufacturer will not do so.

users have in the past fixed serious security bug in there wifi drivers, which would be banned under the NPRM.

taking away peoples freedom to improve there routers firmware and to use the router as they wish is completely not necessary.

if users are using there routers in ways that would have a negative impact on RF transmissions then this behavior alone should be illegal.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Cole

Last Name: Danis

Mailing Address: 13042 E 28th St

City: Tulsa

Country: United States

State or Province: OK

ZIP/Postal Code: 74134

Email Address: danis.cole@gmail.com

Organization Name: null

Comment: This is a bad idea. A HORRIBLE IDEA. There shouldn't be limitations on what I can do with a device, unless it's specifically harming the carrier in some way. I bought the device - it's mine.

As a group are literally destroying the ideas, and freedoms of the American people.

This is a bad idea. A HORRIBLE IDEA. There shouldn't be limitations on what I can do with a device, unless it's specifically harming the carrier in some way. I bought the device - it's mine.

As a group are literally destroying the ideas, and freedoms of the American people.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Alexandr

Last Name: Abdulov

Mailing Address: thrxdesu@gmail.com

City: Minsk

Country: Belarus

State or Province: Minsk

ZIP/Postal Code: 22017

Email Address: null

Organization Name: null

Comment: U.A.S you are crazy :/

U.A.S you are crazy :/

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: Bettke

Mailing Address: 626 Idrathernot post mystreetaddress

City: Myrtle Beach

Country: United States

State or Province: SC

ZIP/Postal Code: 29579

Email Address: null

Organization Name: null

Comment: This proposal is very concerning as it hinders my ability to explore as researcher, software engineer, and general computer enthusiast.

Vendors are already notoriously bad at providing security patches. This is why I choose to use third-party software and on occasion write my own firmware for my wireless devices.

This proposal is anti-consumer. If I buy a device I should be free to modify it as I please. If the concern is tampering that results in harmful interference, a blanket ban on software modification is overkill and inappropriate. Abuse of the spectrum is a separate matter entirely. As long as the device remains compliant and uses the wireless spectrum in an approved manner, the software running on it should be no business of the FCC or vendors.

This proposal is very concerning as it hinders my ability to explore as researcher, software engineer, and general computer enthusiast.

Vendors are already notoriously bad at providing security patches. This is why I choose to use third-party software and on occasion write my own firmware for my wireless devices.

This proposal is anti-consumer. If I buy a device I should be free to modify it as I please. If the concern is tampering that results in harmful interference, a blanket ban on software modification is overkill and inappropriate. Abuse of the spectrum is a separate matter entirely. As long as the device remains compliant and uses the wireless spectrum in an approved manner, the software running on it should be no business of the FCC or vendors.

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: Joel

Last Name: Martin

Mailing Address: 3012 Franciscan Drive

City: Arlington

Country: United States

State or Province: TX

ZIP/Postal Code: 76015

Email Address: fcc@martintribe.org

Organization Name:

Comment: Locking down WiFi access points so that only authorized firmware images can be loaded will have the effect of stifling the huge amount of innovation that happens in the custom firmware space. Open Source firmwares for wifi access points will effectively be killed due to the integrated SoC (System on a Chip) nature of most modern access point/consumer routers.

This will also effectively increase the insecurity of WiFi routers because it will not prevent motivated attackers from exploiting firmware vulnerabilities. Access point OEMs are notoriously bad about providing timely security patches. Locking down WiFi access points will not solve that problem. In fact, it will make WiFi access point security worse because users will be unable to take security into their own hands and install trusted third party open source firmware images that are kept up to date with security patches.

This will personally impact me because I always install open source firmware images on my access points so that I am able to use more powerful and secure firmware images than the OEM provides.

This proposed rule change will provide a false sense of security while taking away power from end-users and putting it into the hands of unreliable and inconsistent OEM manufacturers.

Locking down WiFi access points so that only authorized firmware images can be loaded will have the effect of stifling the huge amount of innovation that happens in the custom firmware space. Open Source firmwares for wifi access points will effectively be killed due to the integrated SoC (System on a Chip) nature of most modern access point/consumer routers.

This will also effectively increase the insecurity of WiFi routers because it will not prevent motivated attackers from exploiting firmware vulnerabilities. Access point OEMs are notoriously bad about providing timely security patches. Locking down WiFi access points will not solve that problem. In fact, it will make WiFi access point security worse because users will be unable to take security into their own hands and install trusted third party open source firmware images that are kept up to date with security patches.

This will personally impact me because I always install open source firmware images on my access points so that I am able to use more powerful and secure firmware images than the OEM provides.

This proposed rule change will provide a false sense of security while taking away power from end-users and putting it into the hands of unreliable and inconsistent OEM manufacturers.

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: Neal

Last Name: Becker

Mailing Address: 6810 Falstone Dr

City: Frederick

Country: United States

State or Province: MD

ZIP/Postal Code: 21702

Email Address: ndbecker2@gmail.com

Organization Name:

Comment: I use dd-wrt on my home routers. One reason it's vital is that this software is regularly updated with security updates. The record of OEMs providing security updates for routers after sale is dismal. The idea of an outright ban on 3rd-party router software is far too blunt an instrument for the intended purpose.

I use dd-wrt on my home routers. One reason it's vital is that this software is regularly updated with security updates. The record of OEMs providing security updates for routers after sale is dismal. The idea of an outright ban on 3rd-party router software is far too blunt an instrument for the intended purpose.

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: Paris

Last Name: Jones

Mailing Address: 707 West 21st Street

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78705

Email Address:

Organization Name:

Comment: Dear FCC,

As a long time user of OpenWrt, DDWRT, Tomato, and other third-party router firmware I humbly request that you drop proposed requirements that wifi devices lock-down their firmware.

This sweeping proposal will not just affect me, but thousands of others who rely on Linux-based after-market distributions like CyanogenMod or OpenWRT. This proposal will stifle competition and remove consumer's ability to modify their own hardware.

I hope this proposal will not go through.

Thank you.

Dear FCC,

As a long time user of OpenWrt, DDWRT, Tomato, and other third-party router firmware I humbly request that you drop proposed requirements that wifi devices lock-down their firmware.

This sweeping proposal will not just affect me, but thousands of others who rely on Linux-based after-market distributions like CyanogenMod or OpenWRT. This proposal will stifle competition and remove consumer's ability to modify their own hardware.

I hope this proposal will not go through.

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: Jacob

Last Name: Carter

Mailing Address: 1337 N 1230 W

City: Orem

Country: United States

State or Province: UT

ZIP/Postal Code: 84057

Email Address: lagonium@gmail.com

Organization Name:

Comment: I express concern about the intent and results of this regulation/rulemaking. As such, I oppose its implementation/codification as presently written.

This rule appears to require some kind of lockdown on software which interfaces with a wireless radio - these radios being and becoming more prevalent in everyday items such as computers, cell phones, tablets, watches, and even shoes.

As is usually the case with rulemaking, the terms used in the text are too broad. It could be read to mean that *any* software must be locked down and irreplaceable by the end user (consumer/purchaser).

This overreach could potentially mean that a person who purchases a computer can never change the operating system it uses (could not switch from a Microsoft product to some version of BSD or Linux for example). It could also mean that someone who purchases an Android device could not install a different OS/ROM of their choice (such as AOSP or Cyanogenmod). Why could it mean these things? Because an Operating System is 'software' that can interface with a wireless radio of some kind.

I urge the FCC not to adopt this new rule, as it would:

-Eliminate the consumer/user's right/ability to repair, modify, or re-use a device for a different purpose because they would be unable to change the software running on it

-Decrease the ability of security researchers to modify devices using wireless radios for their research purposes

-Eliminate the incentive for corporations to actually issue security or other updates to their products' software, because by not issuing updates they could force people to buy new products

-Decrease faith in the United States Governmental Agencies even further, as this is an apparent overreach and (perhaps unwitting) attempt to divest the People of America of one of their inalienable rights (the right to own property and control its use)

-Decrease user/consumer faith in the devices which they use, as they could not determine whether illegal/unlawful/annoying spying is taking place upon them within the non-open-source software which runs on the vast majority of wireless devices

-Discourage innovation and technological advancement in general by negating the ability of a user/consumer to modify software on a wireless-enabled device

I express concern about the intent and results of this regulation/rulemaking. As such, I oppose its implementation/codification as presently written.

This rule appears to require some kind of lockdown on software which interfaces with a wireless radio - these radios being and becoming more prevalent in everyday items such as computers, cell phones, tablets, watches, and even shoes.

As is usually the case with rulemaking, the terms used in the text are too broad. It could be read to mean that *any* software must be locked down and irreplaceable by the end user (consumer/purchaser).

This overreach could potentially mean that a person who purchases a computer can never change the operating system it uses (could not switch from a Microsoft product to some version of BSD or Linux for example). It could also mean that someone who purchases an Android device could not install a different OS/ROM of their choice (such as AOSP or Cyanogenmod). Why could it mean these things? Because an Operating System is 'software' that can interface with a wireless radio of some kind.

I urge the FCC not to adopt this new rule, as it would:

- Eliminate the consumer/user's right/ability to repair, modify, or re-use a device for a different purpose because they would be unable to change the software running on it

- Decrease the ability of security researchers to modify devices using wireless radios for their research purposes

- Eliminate the incentive for corporations to actually issue security or other updates to their products' software, because by not issuing updates they could force people to buy new products

- Decrease faith in the United States Governmental Agencies even further, as this is an apparent overreach and (perhaps unwitting) attempt to divest the People of America of one of their inalienable rights (the right to own property and control its use)

- Decrease user/consumer faith in the devices which they use, as they could not determine whether illegal/unlawful/annoying spying is taking place upon them within the non-open-source software which runs on the vast majority of wireless devices

- Discourage innovation and technological advancement in general by negating the ability of a user/consumer to modify software on a wireless-enabled device

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: Ashok

Last Name: Rao

Mailing Address: 8818 Tallyho Trail

City: Potomac

Country: United States

State or Province: MD

ZIP/Postal Code: 20854

Email Address: ashok_rao@yahoo.com

Organization Name: Great Arbor Communications

Comment: Good Afternoon

I am the founder and President of Great Arbor Communications LLC located in Potomac, MD. We develop wireless routers for niche applications. One of our products - the GAC-252 wireless router allows users to get WiFi access with only a Dial up Internet connection. Our customers often live in parts of the country which do not have access to broadband and/or cannot afford the cost of a broadband connection. This WiFi dial up router allows them to use their smartphones, tablets, and other devices to access the Internet wirelessly. We believe we perform a valuable service for the community and our comments section on www.greatarbor.com/products.html reflects that. This low- end segment has been completely ignored by mainstream wireless router manufacturers.

As a tiny company servicing a niche market - the most effective way we could build these units was by taking COTS wireless routers and modifying the firmware with an open source Linux distribution - OpenWrt. While we only make some modifications to the IP networking layer and web interface in these router and not to the wireless portion, the underlying Linux operating system however has had to develop drivers for the wireless chips within the router. These modifications have been done by the Linux Developer community in a very responsible fashion abiding by the power emission regulations for IEEE 802.11 standard WiFi service.

Another product we offer is the Thuraya XT-Hotspot which has also been developed using the Openwrt distribution on a COTS router. This product creates a WiFi connection to Thuraya satellite data link allowing users to access the satellite data link completely wirelessly. This product has generated more than a \$100,000 in US export revenues and a significant amount of Federal and State Taxes have been incurred on sales of this product.

The new regulations being proposed by the FCC will create an enormous burden for our company. Under the rules proposed by the FCC, devices with radios may be required to prevent modifications to firmware. That means the hardware we buy will not be able to be modified and we will have to develop our own hardware and go through our own certification process. Our business cannot afford the costs and complexities associated with hardware development and certification. This will effectively kill this small business leaving thousands of current and future users without access to a WiFi Dial up connection. We also know of many small companies like Great Arbor who are using the same firmware modification procedure to create a variety of tailored products for particular market segments. The proposed regulation will stifle the innovation being created with OpenWrt and other firmware distributions around the world.

We respectfully urge the commission to not go forward with this new regulation.

Ashok Rao, Ph.D

Great Arbor Communications
Potomac, Maryland
ashok@greatarbor.com

Good Afternoon

I am the founder and President of Great Arbor Communications LLC located in Potomac, MD. We develop wireless routers for niche applications. One of our products - the GAC-252 wireless router allows users to get WiFi access with only a Dial up Internet connection. Our customers often live in parts of the country which do not have access to broadband and/or cannot afford the cost of a broadband connection. This WiFi dial up router allows them to use their smartphones, tablets, and other devices to access the Internet wirelessly. We believe we perform a valuable service for the community and our comments section on www.greatarbor.com/products.html reflects that. This low- end segment has been completely ignored by mainstream wireless router manufacturers.

As a tiny company servicing a niche market - the most effective way we could build these units was by taking COTS wireless routers and modifying the firmware with an open source Linux distribution - OpenWrt. While we only make some modifications to the IP networking layer and web interface in these router and not to the wireless portion, the underlying Linux operating system however has had to develop drivers for the wireless chips within the router. These modifications have been done by the Linux Developer community in a very responsible fashion abiding by the power emission regulations for IEEE 802.11 standard WiFi service.

Another product we offer is the Thuraya XT-Hotspot which has also been developed using the Openwrt distribution on a COTS router. This product creates a WiFi connection to Thuraya satellite data link allowing users to access the satellite data link completely wirelessly. This product has generated more than a \$100,000 in US export revenues and a significant amount of Federal and State Taxes have been incurred on sales of this product.

The new regulations being proposed by the FCC will create an enormous burden for our company. Under the rules proposed by the FCC, devices with radios may be required to prevent modifications to firmware. That means the hardware we buy will not be able to be modified and we will have to develop our own hardware and go through our own certification process. Our business cannot afford the costs and complexities associated with hardware development and certification. This will effectively kill this small business leaving thousands of current and future users without access to a WiFi Dial up connection. We also know of many small companies like Great Arbor who are using the same firmware modification procedure to create a variety of tailored products for particular market segments. The proposed regulation will stifle the innovation being created with OpenWrt and other firmware distributions around the world.

We respectfully urge the commission to not go forward with this new regulation.

Ashok Rao, Ph.D
Great Arbor Communications
Potomac, Maryland
ashok@greatarbor.com

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michaal

Last Name: Rutlege

Mailing Address: 5960C Mendocino Dr

City: Dallas

Country: United States

State or Province: TX

ZIP/Postal Code: 75248

Email Address: null

Organization Name: null

Comment: Requiring that all Wi-Fi routers be locked down from consumer modification prevents end users from running custom software more suited to their personal router usage. Power users, especially, benefit from the ability to extend their routers software capabilities through third-party, often open source, router firmwares. These firmwares tend to be more robust and less vulnerable than the manufacturer's own firmware, as there tends to be a more active community behind the third-party firmware. This alleviates end user frustration on missing features, convoluted configuration interfaces (which tend to be over-complicated on manufacturer firmwares) and reduced functionality. Please do not blindly enforce this policy, we end users understand your need to ensure routers are using only approved frequencies, and most of us adhere to that on our own. Do not punish us for the actions of the few who do not wish to work within reasonable guidelines and laws.

Requiring that all Wi-Fi routers be locked down from consumer modification prevents end users from running custom software more suited to their personal router usage. Power users, especially, benefit from the ability to extend their routers software capabilities through third-party, often open source, router firmwares. These firmwares tend to be more robust and less vulnerable than the manufacturer's own firmware, as there tends to be a more active community behind the third-party firmware. This alleviates end user frustration on missing features, convoluted configuration interfaces (which tend to be over-complicated on manufacturer firmwares) and reduced functionality. Please do not blindly enforce this policy, we end users understand your need to ensure routers are using only approved frequencies, and most of us adhere to that on our own. Do not punish us for the actions of the few who do not wish to work within reasonable guidelines and laws.

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: Eric

Last Name: Lambart

Mailing Address: N. Oatman Ave.

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97217-5834

Email Address: eric-fedreg@lambart.net

Organization Name: Self

Comment: To whom it may concern:

I am writing in response to the recently proposed rules changes regarding home wireless internet ("WiFi") routers.

Firmware from router manufacturers is notoriously insecure. So much so that many security experts recommend installing third-party firmware--see:

<http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

A manufacturer isn't required to provide fixes to the user even if the device is found to be insecure or operating outside of authorization, so why on earth would you propose to prevent people (and businesses) from being allowed to secure their networks?

When an old router proves to be insecure or otherwise defective, "just buy a new one" is not an acceptable alternative. It makes bad economic sense, is simply wasteful, and there is obviously NO guarantee that the new hardware will be any less flawed, or in need of patching, as the hardware it was purchased to replace.

The new rule also prevents device owners from ensuring that their router is running trustworthy firmware, free of "backdoors" and other poor security practices that are well-known to plague the hardware and software industries.

With nearly all of these routers being manufactured in China, a nation known to engage in state-sponsored espionage (industrial and otherwise), it seems ludicrous to propose that US citizens and corporations be prevented from ensuring their foreign-made routers are secure enough to protect their privacy and financial details. Many responsible corporate IT departments routinely install superior firmware to help secure their networks against hostile intrusion, and this rule would explicitly ban these network-security "best practices".

It is completely unacceptable that FCC has decided to take away yet another freedom for people (and corporations) to lawfully operate the devices they own within the current (and reasonable) regulatory practices.

Please reconsider your decision.

Sincerely,

Eric Lambart

U.S. Citizen and Software Engineer

To whom it may concern:

I am writing in response to the recently proposed rules changes regarding home wireless internet ("WiFi") routers.

Firmware from router manufacturers is notoriously insecure. So much so that many security experts recommend installing third-party firmware--see:

<http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

A manufacturer isn't required to provide fixes to the user even if the device is found to be insecure or operating outside of authorization, so why on earth would you propose to prevent people (and businesses) from being allowed to secure their networks?

When an old router proves to be insecure or otherwise defective, "just buy a new one" is not an acceptable alternative. It makes bad economic sense, is simply wasteful, and there is obviously NO guarantee that the new hardware will be any less flawed, or in need of patching, as the hardware it was purchased to replace.

The new rule also prevents device owners from ensuring that their router is running trustworthy firmware, free of "backdoors" and other poor security practices that are well-known to plague the hardware and software industries.

With nearly all of these routers being manufactured in China, a nation known to engage in state-sponsored espionage (industrial and otherwise), it seems ludicrous to propose that US citizens and corporations be prevented from ensuring their foreign-made routers are secure enough to protect their privacy and financial details. Many responsible corporate IT departments routinely install superior firmware to help secure their networks against hostile intrusion, and this rule would explicitly ban these network-security "best practices".

It is completely unacceptable that FCC has decided to take away yet another freedom for people (and corporations) to lawfully operate the devices they own within the current (and reasonable) regulatory practices.

Please reconsider your decision.

Sincerely,
Eric Lambart
U.S. Citizen and Software Engineer

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: Maxwell

Mailing Address: 9817 Moyer Raod

City: Damascus

Country: United States

State or Province: MD

ZIP/Postal Code: 20872

Email Address: notify@weathercloset.com

Organization Name:

Comment: I would strongly urge the Commission to avoid creating a rule which will remove the ability of the end user (and owner of the device) to load software of their choosing. If it is deemed necessary to more tightly control the behavior of radios in certain spectrums, I would urge language to very narrowly define these requirements so as to preserve the rights of the end user and owner to access modify and replace the manufacturer-provided software and/or firmware. Additionally I would urge a grandfather clause to permit those using this software today to continue doing so.

To do otherwise would be to impinge on the natural right of the owners of these devices, as well as retarding the progress of these technologies, most especially in regard to cybersecurity.

I would strongly urge the Commission to avoid creating a rule which will remove the ability of the end user (and owner of the device) to load software of their choosing. If it is deemed necessary to more tightly control the behavior of radios in certain spectrums, I would urge language to very narrowly define these requirements so as to preserve the rights of the end user and owner to access modify and replace the manufacturer-provided software and/or firmware. Additionally I would urge a grandfather clause to permit those using this software today to continue doing so. To do otherwise would be to impinge on the natural right of the owners of these devices, as well as retarding the progress of these technologies, most especially in regard to cybersecurity.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Chris

Last Name: Hauca

Mailing Address: W5774 North Drive

City: Elkhorn

Country: United States

State or Province: WI

ZIP/Postal Code: 53121

Email Address: hauca@hotmail.com

Organization Name: US Citizen

Comment: Dear FCC,

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

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

Sincerely,
Chris Hauca

Dear FCC,

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

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

Sincerely,
Chris Hauca

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Ramsey

Mailing Address: 6000 Reynolds Drive #875

City: Rochester

Country: United States

State or Province: NY

ZIP/Postal Code: 14623

Email Address:

Organization Name:

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Fred

Last Name: Clift

Mailing Address: 352 N 470 W

City: Lindon

Country: United States

State or Province: UT

ZIP/Postal Code: 84042

Email Address: fred@clift.org

Organization Name: -

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ben

Last Name: Greear

Mailing Address: 2417 Main Street, STE 201

City: Ferndale

Country: United States

State or Province: WA

ZIP/Postal Code: 98248

Email Address: greearb@candelatech.com

Organization Name: Candela Technologies Inc

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

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

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

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

Thanks,
Ben Greear

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

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

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

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

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

Thanks,
Ben Greear

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Lloyd

Last Name: Brown

Mailing Address: 196 W Pacific Dr

City: American Fork

Country: United States

State or Province: UT

ZIP/Postal Code: 84003

Email Address:

Organization Name:

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

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

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

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

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

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

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

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

device manufacturers, to close known security holes.

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Daniel

Last Name: Thompson

Mailing Address: 11121 Appletree Lane

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78726

Email Address: fcc@danielthompson.net

Organization Name:

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Glen

Last Name: Stewart

Mailing Address: 733 Story Dr

City: Fairfield

Country: United States

State or Province: OH

ZIP/Postal Code: 45014

Email Address: glen_stewart@associate.com

Organization Name:

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matt

Last Name: Neilsen

Mailing Address: 10904 Schoenfeld CT

City: St. Louis

Country: United States

State or Province: MO

ZIP/Postal Code: 63123

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

Organization Name:

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Trevor

Last Name: Lee

Mailing Address: 19655 clubhouse drive

City: Denver

Country: United States

State or Province: CO

ZIP/Postal Code: 80138

Email Address:

Organization Name:

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joshua

Last Name: Urbain

Mailing Address: 216 S Chapman St

City: Chesaning

Country: United States

State or Province: MI

ZIP/Postal Code: 48616

Email Address: null

Organization Name: null

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Darren

Last Name: Jones

Mailing Address: 1022 Ringwood Road

City: Bournemouth

Country: United Kingdom

State or Province: Dorset

ZIP/Postal Code: BH11 9LA

Email Address: djaychela@gmail.com

Organization Name:

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: Gervais

Mailing Address: 1398, rue de l'Oural

City: Quebec City

Country: Canada

State or Province: Quebec

ZIP/Postal Code: G1C 7Y6

Email Address: jgervais@gmail.com

Organization Name:

Comment: To whom it may concern,

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

Thanks

Jonathan Gervais

To whom it may concern,

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

Thanks

Jonathan Gervais

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Magnus

Last Name: Kwan

Mailing Address: 1735 Tyler Drive

City: Monterey Park

Country: United States

State or Province: CA

ZIP/Postal Code: 91755

Email Address:

Organization Name:

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Merriam

Mailing Address: 121 E 17th St

City: Pittsburg

Country: United States

State or Province: CA

ZIP/Postal Code: 94565

Email Address:

Organization Name:

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ron

Last Name: Light

Mailing Address: 520 W 103rd St

City: Kansas City

Country: United States

State or Province: MO

ZIP/Postal Code: 64114

Email Address: Ron@RonLight.com

Organization Name: Bright Light Investments LLC

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

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

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Justin

Last Name: Rosko

Mailing Address: 7824 Hampton Forest Lane

City: Chesterfield

Country: United States

State or Province: VA

ZIP/Postal Code: 23832

Email Address: rosjustinm@yahoo.com

Organization Name:

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Justin

Last Name: Cole

Mailing Address: 108 oakview ave.

City: Pittsburgh

Country: United States

State or Province: PA

ZIP/Postal Code: 15218

Email Address: justincole01@gmail.com

Organization Name:

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

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

Thank you

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

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

Thank you

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Jones

Mailing Address: 100 cashew ct

City: longwood

Country: United States

State or Province: FL

ZIP/Postal Code: 32750

Email Address: cjflow@hotmail.com

Organization Name:

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

My reasons for this include but are not limited to:

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

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

My reasons for this include but are not limited to:

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jesse

Last Name: Robinson

Mailing Address: 2343 Clover Ln

City: Janesville

Country: United States

State or Province: WI

ZIP/Postal Code: 53545

Email Address: colecago@gmail.com

Organization Name:

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jeff

Last Name: Monahan

Mailing Address: P.O. Box 192

City: Dayton

Country: United States

State or Province: OR

ZIP/Postal Code: 97114

Email Address: jeff@oregon.com

Organization Name:

Comment: To whom it may concern,

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

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

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

Thank you for reading this.

To whom it may concern,

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

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

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

Thank you for reading this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matt

Last Name: Poindexter

Mailing Address: 17243 E Lakeview Dr

City: Mayer

Country: United States

State or Province: AZ

ZIP/Postal Code: 86333

Email Address: mw@chiefpoints.com

Organization Name: Revolutionized Computing

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brian

Last Name: Livermore

Mailing Address: 4408 W Kogel Dr

City: Sioux Falls

Country: United States

State or Province: SD

ZIP/Postal Code: 57107

Email Address: livermob@gmail.com

Organization Name:

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

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

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Hunt

Mailing Address: 107 30th Ave E

City: Tuscaloosa

Country: United States

State or Province: AL

ZIP/Postal Code: 35404

Email Address: ttg@cpan.org

Organization Name:

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Mason

Mailing Address: 5123 SE 40th Ave

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97202

Email Address: cmason@cmason.com

Organization Name:

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

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

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

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

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

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

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

Thank you for listening.

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

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

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

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

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

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

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

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

Thank you for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: George

Last Name: Cash

Mailing Address: 8726 Bexar Dr

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77064

Email Address: hextejas@fastmail.com

Organization Name: None

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Nadeau

Mailing Address: 29 Short St Apt 1

City: Vergennes

Country: United States

State or Province: VT

ZIP/Postal Code: 05491

Email Address:

Organization Name:

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Radu

Last Name: Motisan

Mailing Address: Timisoara

City: Timisoara

Country: Romania

State or Province: Timis

ZIP/Postal Code: 300414

Email Address: radhoo.tech@gmail.com

Organization Name: n/a

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

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

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

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

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

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

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

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