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: Mike
Last Name: Apt.
Mailing Address: 10300 Jollyville Rd Apt 220
City: Austin
Country: United States
State or Province: TX
ZIP/Postal Code: 78759
Email Address: realmikeazn@gmail.com
Organization Name: Home
Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

We would love to innovate and grow by making our own changes or modification.

Here is what I need
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 listen to the money loving corporation and preventing freedom on information.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Kevin
Last Name: Neves
Mailing Address: 225 sackville st
City: toronto
Country: Canada
State or Province: Ontario
ZIP/Postal Code: m5a 0b9
Email Address: redline14k@gmail.com
Organization Name:
Comment: The notion of not allowing Open Source software is the equivalent of blocking free speech. If anything Open Source should be a mandatory for any and all WiFi and other forms of communication. The reason for this is that we need to inspect and be able to audit as the public. This is the public's spectrum and the public needs to not only have access to this spectrum the full documented methods devices we use access this spectrum.

If you incorrectly select to block opensource then you may as sell close the internet, censor any free speech and close the FCC as no one will require you anymore.

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: Dennis
Last Name: Roberts
Mailing Address: 425 23rd Ave S #A001
City: Seattle
Country: United States
State or Province: WA
ZIP/Postal Code: 98144
Email Address: denrober@gmail.com
Organization Name: N/A
Comment: Please do not require vendors to disallow modification of firmware of consumer wireless devices.

Many devices that have been abandoned by the manufacture can find new life with community modified firmware.

Security flaws can be corrected outside of the manufacture release cycle.

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: Jon
Last Name: Arintok
Mailing Address: 267 Madison St
City: Boydton
Country: United States
State or Province: VA
ZIP/Postal Code: 23917-3103
Email Address:
Organization Name:
Comment: True security does not come from obscuring the way a device functions. Doing so only give malicious agents a leg up on detecting vulnerabilities. True security comes from making it as easy as possible for customers to audit a device and it's software, and report any vulnerabilities they find to the distributor/manufacturer. It has been proven again and again that "security by obscurity" does not work in the long term. Improving the customers ability to audit the products they own results in much more secure products, and has many other benefits. The rules suggested here make it more difficult for customers to know if the device they are using is secure for their particular use-case, and are therefor a step backwards for all parties involved.

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: Austin
Last Name: Gossmeyer
Mailing Address: 426 Brookside Ter
City: Moore
Country: United States
State or Province: OK
ZIP/Postal Code: 73160
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

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: Kuldeep Singh
Last Name: Dhaka
Mailing Address: Modinagar
City: Ghaziabad
Country: India
State or Province: UP
ZIP/Postal Code: 201204
Email Address:
Organization Name:
Comment: Hello,
I oppose the proposal, please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.
This will consequences like
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.
so, please drop the proposal

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: Cory
Last Name: Tobin
Mailing Address: 518 S. El Molino Ave #202
City: Pasadena
Country: United States
State or Province: CA
ZIP/Postal Code: 91101
Email Address: cory.tobin@gmail.com
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

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: Cody
Last Name: Hofstetter
Mailing Address: 8 West Blair Tract
City: Lambertville
Country: United States
State or Province: NJ
ZIP/Postal Code: 08530
Email Address: ch10031990@yahoo.com
Organization Name: CodyHofstetter.com
Comment: If the FCC passes legislation requiring manufacturers to lock down computing devices to prevent modification if they have a "modular wireless radio" or a device with an "electronic label"; clearly the FCC does not have the best interests of the American people at heart.

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: Weiss
Mailing Address: 2720 Carmel Ave
City: Clearlake
Country: United States
State or Province: CA
ZIP/Postal Code: 95422
Email Address: lazylion@lionslair.com
Organization Name: none
Comment: Schools and other non-profit organizations often require small changes to effectively implement low budget internet access. Obviously, as no manufacturers are interested in providing customized software for a few low paying customers, this requires the use of dd-wrt or other open source router software.

Furthermore, the FCC has no business whatsoever demanding that vendors implement locks on wifi enabled devices when none of those devices were ever able to generate signals outside of their respective bands in the first place, or they wouldn't have qualified for type acceptance.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Joseph
Last Name: Robinson
Mailing Address: 1100 Plum Creek Parkway Unit 11204
City: Castle Rock
Country: United States
State or Province: CO
ZIP/Postal Code: 80104
Email Address: rolandsym@gmail.com
Organization Name:
Comment: Open source software allows transparency. Disallowing open source software enables forced purchases and stifles growth. Requiring certain software only for accessing items could be a violation of the 1st amendment and seen as stifling American voices.

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: Ashton
Last Name: Alexander
Mailing Address: 5423 E Piping Rock rd
City: Scottsdale
Country: United States
State or Province: AZ
ZIP/Postal Code: 85254
Email Address: ashton.alexander@gmail.com
Organization Name:
Comment: I completely disagree with this rule change as it goes against ingenuity, and what America stands for. We should be free to take on the technologies of our choosing and regulating things such as wifi routers, or really any technology, from the ability to develop it independently goes against what I feel our founding fathers and America stands for.

Please reject and reconsider this rule change.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Alexey
Last Name: Pavlenko
Mailing Address: alexey.n.pavlenko@gmail.com
City: Krasnodar
Country: Russia
State or Province: Krasnodarsky kray
ZIP/Postal Code: 350072
Email Address:
Organization Name:
Comment: If you purchased a laptop on a system that is not necessary to me, I can not change it to another? What kind of nonsense? This limits my rights as a buyer. I do not use systems, Microsoft Corporation, and consider unacceptable when they and the like artificially limit the choice.

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: kenton
Last Name: bond
Mailing Address: 5802 e edgemont ave
City: scottsdale
Country: United States
State or Province: AZ
ZIP/Postal Code: 85257
Email Address: kentonbond@yahoo.com
Organization Name: waveforms
Comment: Dear Ms or Sirs,
Please do not implement rules that take away the ability of users to install the software of their choice on their own devices.
Americans like me need to be able to fix security holes on my devices when the manufacturer chooses not to. For example take Verizen. I had an android phone, an HTC Incredible that I had for four years and never got one update. Not one. This also happened to me on three routers. The third one, Chinese got hacked completely and after completing several clean installs with the malware reinstalling automatically so I switched routers to no avail-they shut off my cpu fan and fried the cpu and motherboard.
It would likely prevent r&d into advanced wireless technology ie mesh networking & Open Wrt. Which would infringe upon the ability of amateur radio operators to create high powered mesh networks designed to assist first responders in the event of an emergency or natural disaster. The same goes for dissidents in other countries struggling for democracy or free speech or to get info out in the event of a crackdown. Setting this kind of policy is extremely important as manufacturers will only make one design to sell in multiple markets.
Itwould prevents resellers from installing custom firmware or VPNs(esp foriegn markets) without agreeing to any condition the manufacturer chooses.
Additionally besides this proposal there is a new wifi standard coming up for mobile use. This should at least be tabled for five years until the other myriad of decisions first because leaving open source available will help fine tune kinks as the next gen comes around. I want to say I will not use it as I do want another phone because effectivly there's no warranty and no support. Some with apple I guess but with android there's just no support. If I buy a tv from costco I have three years of warranty. Why can't a phone be warranttied for two years? With open source at least i'd have a shot at fixing it.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Andrey
Last Name: S
Mailing Address: spb
City: Spb
Country: Russia
State or Province: Spb
ZIP/Postal Code: 000000
Email Address:
Organization Name:
Comment: Firmware changes MUST NOT be blocked. At least because of tons of vulnerabilities, that vendors doesn't fix at all.

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: Vadim
Last Name: Kuchin
Mailing Address: Dmitrovskoe shosse 38-1-6
City: Moscow
Country: Russia
State or Province: Moscow
ZIP/Postal Code: 127238
Email Address: kutchin@gmail.com
Organization Name:
Comment: I think that doing slows down hardware/software evolution, so I against this rule!

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: Grant
Last Name: Bierman
Mailing Address: 16101 Windham
City: Little Rock
Country: United States
State or Province: AR
ZIP/Postal Code: 72206-6134
Email Address:
Organization Name:
Comment: Please FCC do not implement rules that take away the ability of users to install the software of their choosing on their computing devices for reason such as:

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.

Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes

Ban installation of custom firmware on your Android phone

Discourage the development of alternative free and open source WiFi firmware, like OpenWrt

Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses."

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: Feodor
Last Name: Petrov
Mailing Address: 1234567890
City: Moscow
Country: Russia
State or Province: 00000000
ZIP/Postal Code: 0000000000
Email Address:
Organization Name:
Comment: don't deprive our freedom!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Morgan
Last Name: Gangwere
Mailing Address: 135 Hortencia Rd
City: Sandia Park
Country: United States
State or Province: NM
ZIP/Postal Code: 87047
Email Address: morgan.gangwere@gmail.com
Organization Name:
Comment: Dear FCC,

Please don't take away my ability to modify the software running on hardware that happens to have a radio in it. Doing so would, for lack of a better description, place the state of the art in an almost permanent freeze. The inability to run software that is up-to-date and secure is something that places every American at risk with no advantage to them.

The 2.4GHz spectrum has been unregulated; This has lead to serious advances in the art of radio communications, including countless new modes of high-speed, low-bandwidth, low-noise communications which benefit users far and wide. It is only because amateurs have been able to tweak their hardware through software that this is possible.

The security and freedom of users depends on the ability to modify software. Running custom operating systems such as OpenWRT/DD-WRT and Mikrotik's RouterOS make it possible to create and maintain security in an increasingly insecure world.

For example, two bugs affecting the OpenSSL and Bash projects (known as "Heartbleed" and "ShellShock", respectively) made it clear that wireless router (802.11a/b/g/n/etc) companies simply didn't care about users. Today, millions of routers in the United States alone by a single manufacturer (Actiontec) have been left unpatched of either bug.

Increasingly, Americans don't trust technology coming out of China and parts of Europe. Consumer devices made by companies such as TP-Link (of Taiwan) are however the dominant force in the United States and Europe. Worse, Americans are becoming less trusting of the software which runs on American-made hardware from companies like Linksys, who recently turned many customers sour with a forced upgrade of software which locked out users from their networks until they agreed to allow Cisco/Linksys to *remotely* administrate *Any* Cisco device within their network.

Cisco/Linksys held home consumers' networks hostage. With software.

Removing the freedom to modify software of a device containing a radio is bad for American (and non-American) businesses. Companies such as Mikrotik and Ubiquiti make consumer and professional grade equipment which is actively marketed as running open source software which a competent individual can replace, allowing for more diverse and unique usages of this hardware. Such examples include, but are definitely not limited to:

* Creating public library nodes which can be deployed into under-served areas, containing backups of the Project Gutenberg library, Wikipedia, etc. such that families which have no internet access can access essential information

* High-speed point-to-point links between mountaintops which expand Internet access into rural areas which are not accessible otherwise or for which it is prohibitively expensive to run regular copper wire service to

These are but two examples. There are many more creative, exceptional uses for hardware which contains a radio.

The freedom to modify a device containing a radio helps solve an environmental issue, one which plagues our world and our society. This issue is that of E-waste; castoff computer equipment which, due to software bugs and a lack of support from the manufacturer, becomes unusable. The freedom to modify the software can fix bugs, extending the life of hardware which would end up in a landfill otherwise. Software such as OpenWRT/DD-WRT/Tomato aims to, in many cases, keep consumer electronics out of the landfill.

Cellular phones have a similar issue. Phone manufacturers abandon devices which are not profitable, such as those which are sold and geared towards low-income individuals. These devices become the unwanted children of companies like Samsung, Kyocera, and Motorola. Their existence is to create a temporary profit and their support ends long before their usefulness.

Third-party software such as Cyanogenmod keeps these devices secure and in many cases up to date. The work of third-party researchers exposes flaws in the baseband software, backdoors placed by the OEMs and security issues which affect hundreds of thousands to millions of people. The work these researchers do is often met with (in the worst case) threats of lawsuits from the equipment manufacturer or (more often) ignorance or denial on the part of the OEM.

With the "internet of things" becoming more and more a part of our lives, this security is essential. Your toaster is becoming an internet-enabled thing, and that scares security researchers.

Finally, removal of the freedom to modify software stifles innovation. Systems such as the ESP8266 and Broadcom's wireless System-on-chip are built as cheap, effective "We'll do the hard work of doing the radio stuff, you do the software stuff" development systems which allow hardware and software engineers to put new products to market. This innovation depends on the ability to easily change the software that is running on those devices.

Morgan Gangwere (KG5IXZ)

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: Devin
Last Name: Sabin
Mailing Address: 917 Crosswind Pl
City: Cockeysville
Country: United States
State or Province: MD
ZIP/Postal Code: 21030
Email Address:
Organization Name:
Comment: America was founded on being free. It grew to be a great country because we have been unrestricted. Innovation has developed here because when Americans buy something, they are allowed to use it as they wish so long as it doesn't interfere with another person's right to be free. Don't restrict our equipment as this will stifle the ingenuity of the American people and will ultimately hurt us more than any good that it can do.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Alfred
Last Name: Grundinger
Mailing Address: alfredgrundinger@gmail.com
City: Munich
Country: Germany
State or Province: Bavaria
ZIP/Postal Code: 80331
Email Address:
Organization Name:
Comment: You can't be serious? I see this organisation has problems with free software and doesn't care about consumers (or Appeal and Microsoft would be out of buissnes tomorrow) but now you are actually hindering people, to act freely, when they want to remove the shitty, buggy insecure firmware from their router and put something better on it? This is laughable, I'am very dissapointed from 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: Eric
Last Name: Woehler
Mailing Address: 212 S Cedar St
City: Monticello
Country: United States
State or Province: IA
ZIP/Postal Code: 52310
Email Address:
Organization Name:
Comment: This regulation seems like a step backwards. I believe open source provides greater security and peace of mind for consumers. And I think a regulation like this makes American hardware look sketchy. You're taking control away from consumers.

Keeping your firmware updated is going to be based on whether the company that produced it is in business and still patching. And if the company I brought my hardware from decides to stop supporting firmware for an older piece of equipment I maybe forced to buy new equipment just to fix security issues.

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: Bill
Last Name: Jones
Mailing Address: 12, 6, Barnes Ave, New York
City: New York
Country: United States
State or Province: NY
ZIP/Postal Code: 10467
Email Address:
Organization Name:
Comment: It's a very bad idea in whole! It's a direct limitation of our privacy! I would like to pay my money only for those devices that will be under my own control, but not FCC. The federal protection of software inside hardware is like grafted virus, that can control the ways you go, the ways you think! We have to choose freedom instead of federal slavery!

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: Nathaniel
Last Name: Swanson
Mailing Address: 1004 Gould RD
City: Lansing
Country: United States
State or Province: MI
ZIP/Postal Code: 48917
Email Address:
Organization Name:
Comment: Federal Communications Commission,

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

I have used in the past and plan on using in the future open source software installed by myself on my own router. It is using this software that has encouraged me to learn more about WiFi, radio waves, and other technology.

Also, I would like to live in a future where there are no black boxes. Little boxes of software that are not open source and no one can know what they do or make changes to them. The world need more open source software and this is only going to lead to impeding that goal. Please do not put yourself between me and my things.

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Brian
Last Name: Harnett
Mailing Address: 45 West 60th Street
City: New York
Country: United States
State or Province: NY
ZIP/Postal Code: 10023
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Nicholas
Last Name: Rodine
Mailing Address: 391 17th NW
City: Atlanta
Country: United States
State or Province: GA
ZIP/Postal Code: 30363
Email Address:
Organization Name:
Comment: OpenSource software allows us to trust our software. Taking away from that removes our trust.

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: Zachary
Last Name: Beals
Mailing Address: 535 Sunblest Blvd S
City: Fishers
Country: United States
State or Province: IN
ZIP/Postal Code: 46038
Email Address: zbeals1@gmail.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.

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.

Billions of dollars rest on the world's ability to trust the government in regards to spying. Billions have already been lost due to government over reach on electronic devices.