

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: Mike

Last Name: Lowry

Mailing Address: 12345 no way lane

City: san antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78218

Email Address:

Organization Name:

Comment: Please do not implement any law that will limit our ability as consumers to do what we please with products that we have purchased, including but not limited to:

Prevent Us from Installing and configuring our own software and firmware on the devices

Restricting our ability to replace factory offered software with our own versions

Restricting our ability to modify factory settings

thanks!

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: Durofchalk

Mailing Address: 1270 W Peachtree St NW

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30309

Email Address: nrofchalk@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. Additionally, I would like to emphasize that wireless networking research depends on the ability of researchers to investigate and modify their devices and Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. For example, users have in the past fixed serious bugs in their wifi drivers. These actions 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: Gordon

Last Name: Smith

Mailing Address: 20 Rustic Lane

City: Plaistow

Country: United States

State or Province: NH

ZIP/Postal Code: 03865

Email Address: gsmith2016@gmail.com

Organization Name:

Comment: If you are going to add restrictions in regards to the usability of RF devices, please try to limit the law amongst the software that can be installed. You're giving this industry a dangerous amount of power that could potentially be abused to affect underlying methods like the Operating System of a computer, as well as general large changes to the software. This seems to indicate that you are not in favor of open-source projects (Linux being a huge one), which I assume has something to do with telemetry and tapping in via surveillance. So you shouldn't do that, even though I know what the government wants.

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: Zapolsky

Mailing Address: 30 W Snell Rd Apt 1

City: Oshkosh

Country: United States

State or Province: WI

ZIP/Postal Code: 54901

Email Address: benzapman@gmail.com

Organization Name:

Comment: Default settings are ALWAYS insecure. Preventing changes is an invitation for everything to be hacked. Literally everything. In addition, security flaws can't be corrected through updates/patches the physical hardware would need to be replaced. The icing on the cake is the fact that the open source community would be hurt and they provide the software that runs over half of the internet. Plus every super expensive router/firewall in every company would need to be replaced instead of a simple software update everytime a bug is found.

In summary...

Costs go way up.

Work goes way up.

Security goes way down.

This will enable even children to hack into secure systems for fun and cause chaos. It is scary just how easy it is if a flaw is discovered and is not patched.

Let IT Professionals do their job.

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: Nedobity

Mailing Address: 81 Baldwinville State Road

City: Winchendon

Country: United States

State or Province: MA

ZIP/Postal Code: 01475

Email Address: amw.drizz@gmail.com

Organization Name:

Comment: By forcibly restricting via software or hardware means to limit radio transmission devices. Be it computers, cell phones, routers, wireless access points; will cause businesses; those who manufacture said devices, to further lock down everything on the given system. Giving various manufactures this power, would result in system wide lock downs under the guise of 'complying with the law'; and would over flow in to related devices that do not have radios built in to them. Eg: Desktop without a wireless card would be locked by the manufacture as it has the capability of having a wireless card.

People will always attempt to tamper with devices; while it is not ideal, wholesaling the requirement to lock down devices that have or could have wireless devices will be damaging over all to the end consumer. Manufactures would have no incentive to update the underlying software, and consumers who wish to update it; would be unable to do so.

As is in the current state; manufactures have very little incentive to update any code. And most do not. By allowing this to proceed manufactures will not update code; but instead push new(er) devices out on the consumer. And cost minded consumers will not want to upgrade, esp when the only benefit is a software revision.

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: Fletcher

Mailing Address: 7343 CO RD 45

City: Alger

Country: United States

State or Province: OH

ZIP/Postal Code: 45812

Email Address: justin.s.fletcher@gmail.com

Organization Name:

Comment: I would like to respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Our (The consumer's) ability to fix security flaws and other problems are needed. If this was passed for cars it would be like buy a brand a car and changing the oil but only being able to buy the oil from the manufacturer. What about choice and freedom to choose the best that America can produce?

Just because I like Ford vehicles, does not mean that I like Ford brand spark plugs, oil or other parts. Say I buy a new pair of shoes and would like to put a padded insert, but the company says that I can only put their inserts in them. How many jobs would be lost from companies like Dr. Scholls and many others shutting down. It makes sense only for the manufacture of the product. They can keep a monopoly on the software so us consumers are forced to use theirs and theirs alone. If this is passed than millions of dollars and possibly thousands of jobs would be lost. The ability to choose is a fundamental right for the consumer. Just 20 years ago, products were made for the consumer, not for the sole profit of companies. Products were made to be fixed by the people who bought them, made to last years and not be replaced when the next one came out. I don't want to buy a new product and the manufacturer decides to stop supporting it and I'm forced to buy a new one. Honestly, if this is passed the american people will end up paying a hefty price for it. This will only end up hurting the working class and will make the rich even richer.

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: joe

Last Name: pont

Mailing Address: 211 pine hill road

City: wood river junction

Country: United States

State or Province: RI

ZIP/Postal Code: 02894

Email Address: joepont@gmail.com

Organization Name:

Comment: Fcc please let people install and use devices as they choose on their devices. People should be allowed to use devices as they choose. I feel this is a major threat to how people use their electronics. This would not be good for freedom. 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: Michael

Last Name: Miloff

Mailing Address: 82 Sherwood Lane

City: West Seneca

Country: United States

State or Province: NY

ZIP/Postal Code: 14224

Email Address:

Organization Name:

Comment: I oppose the new rule as they limit a user's freedom to install the software of their own choosing and limit the ability of security researchers to check for vulnerabilities in networking devices which makes us all more vulnerable. The new regulations will stifle innovation in open source software which makes up much of the Android OS (<https://source.android.com/>), the base of Mac OS X <https://www.apple.com/opensource/>, and Linux Distributions that run much of the internet including facebook.com and google.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: matthew

Last Name: ramsey

Mailing Address: 851 ted a crozier blvd

City: clarksville

Country: United States

State or Province: TN

ZIP/Postal Code: 37043

Email Address:

Organization Name:

Comment: While it is understandable that there may be a necessity to govern RF devices, i don't think there is any benefit to to controlling the hardware surrounding it.

Additionally, man will always want to play and take apart, as is the reason behind building a pc. We should not proactively make rules assuming hardware and software will be abused

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: Raymond

Last Name: Stevens

Mailing Address: 90 Annette Place

City: Middletown

Country: United States

State or Province: CT

ZIP/Postal Code: 06457

Email Address:

Organization Name:

Comment: Sections A.b, 3.c, and 3.d are burdensome, impractical, and chilling.

Security researchers would be locked out of systems and unable to study the security, safety, and stability of RF devices that the FCC approves and now proposes to make even more difficult to ensure their safety, in an ironic twist.

Home prototypers and 'makers' would be burdened by this proposal. This proposal would also serve to help cripple aftermarket retailers who do hundreds of millions of dollars in business each year.

Consumer freedom and choice would be hampered by this proposal. The ability to control the systems they own could be locked down in entirety and the American consumer locked out under the excuse of the simple non-threatening guise of "radio security".

The FCC should ask itself: is this really something the Commission should concern themselves with, of all the other more pressing issues? Or is this a backdoor attempt by large industry players to further stamp out third party innovation, bad press for security flaws, and consumer 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: Harold

Last Name: Shepherd

Mailing Address: 228 stone creek lane

City: valparaiso

Country: United States

State or Province: IN

ZIP/Postal Code: 46383

Email Address:

Organization Name:

Comment: Quit trying to stifle advancement of technology against users for your corporate donors.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Cox

Mailing Address: 10 High Street

City: North Sydney

Country: Canada

State or Province: Nova Scotia

ZIP/Postal Code: B2A 2A4

Email Address: mj\_cox@outlook.com

Organization Name:

Comment:

\*\*\*COPY-PASTED MESSAGE\*\*\*

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.

\*\*\*END OF COPY-PASTED MESSAGE\*\*\*

\*\*\*Personally written message\*\*\*

This proposal is absolutely insane and should have been thrown in the trash. It is absolutely ludicrous that you would even consider it. Besides the fact that this proposal is literally insane and inane lets look at devices that are actually intentionally locked down to prevent things like piracy and freedom. iOS is a prime example of a device that is pretty locked down. Same with official android devices. Xbox 360's are locked down. Nintendo Wii's are locked down. Satellite TV is locked down yet still people can watch it for free. This proposal will do nothing except make it slightly harder for people to do. People will still do it, it will just make criminals out of electronics enthusiasts.

WE should have the right to chose which software we use and install on our devices. This proposal is nothing but an attack on FREE and open-source wares. It should be Illegal to lock down devices! Companies are intentionally forcing us to use the software that came with the device.

Lets look at South Korea. It is illegal to sell devices that have bloat ware pre-installed that you cannot uninstall. I think America and the FCC should follow this path and make devices more open and free. Why should it be against the law to install a certain firmware on my phone? As the owner of the device who paid money for it I should have the right to use which ever software I choose.

The only conclusion I can come up with is that you're being bribed to even consider this completely insane proposal. Please make the right decision and defend the freedom of consumers.

Thank you,

Michael Cox

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: Harrison

Last Name: Krug

Mailing Address: 237 Russett Rd.

City: Chestnut Hill

Country: United States

State or Province: MA

ZIP/Postal Code: 02467

Email Address:

Organization Name:

Comment: Please do not implement this policy, as it is a disgusting affront to our personal liberties. 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: Lemme

Mailing Address: 9 Thunder Trail

City: Cranston

Country: United States

State or Province: RI

ZIP/Postal Code: 02921

Email Address:

Organization Name:

Comment: No, just no. I'm no linguist, so I'll copy the points made by librewiki:

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.

A law like this will cause far more problems and inconveniences than good.

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: Jessica

Last Name: Vanderhoff

Mailing Address: 182 Elkwood Ave Unit A

City: Imperial Beach

Country: United States

State or Province: CA

ZIP/Postal Code: 91932

Email Address: jessicavanderhoff@gmail.com

Organization Name:

Comment: This is a violation of personal freedoms, pure and simple.

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: Karl

Last Name: Pattyn

Mailing Address: 8060 Niwot Rd #28

City: Longmont

Country: United States

State or Province: CO

ZIP/Postal Code: 80503

Email Address: crazykarlpattyn@yahoo.com

Organization Name:

Comment: This proposed rule severely restricts the freedom of the individual concerning his or her own property. It allows companies to dictate how an individual can use his or her property, even when said property is no longer owned by the company. It hampers innovation and invention by restricting the freedoms to explore new avenues of technological improvement. This rule essentially enacts a dictatorship over the behavior and activity of people and their wireless technology, and should not be enacted. Please reconsider before making this a 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: Rafael

Last Name: Meza Solorio

Mailing Address: 2001 Serenity

City: Medford

Country: United States

State or Province: OR

ZIP/Postal Code: 97504

Email Address: RMProductions26@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: Joshua

Last Name: kolb

Mailing Address: 835 N Salina St

City: Syracuse

Country: United States

State or Province: NY

ZIP/Postal Code: 13208

Email Address: joshkolb@gmail.com

Organization Name:

Comment: There is no way to secure a device completely, with most devices not receiving security updates for extended periods of time. We need to be able to modify our devices to enhance security as no company will give security updates forever.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Adam

Last Name: Bahe

Mailing Address: 60 E. Monroe Unit 1507

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60603

Email Address: adambahe@gmail.com

Organization Name:

Comment: This sounds exceedingly extreme for what I'm sure are edge cases. Never in my life has any modular wireless radio been modified in such a way that affects me. I'm currently sitting in downtown Chicago, living in a 73 story residential building. Smack dab in the middle of the Loop. I'm surrounded by literally \_hundreds\_ of wireless radios. None of which are impeding upon my use of anything, licensed or not.

I'm sure there are some edge cases, but I think currently we do a very good job at figuring out how to deal with them or finding out who is causing them.

This just seems like bringing down an iron fist on a fringe problem. I am 100% against it. And this is coming from a 15 year IT professional. I currently work for a prop trading firm which heavily relies on wireless microwave transmission from Chicago to NYC.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: LeBlanc

Mailing Address: 3205 Hwy 308

City: Napoleonville

Country: United States

State or Province: LA

ZIP/Postal Code: 70390

Email Address:

Organization Name:

Comment: The federal government should not be in the business of regulating what private citizens can do with devices they own. Its as simple as that. The FCC attempting to lock down devices to only run "approved" software, is limiting what people can do with those devices. I think it is truly a bad idea.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: Lane

Mailing Address: 6104 North Paulina Street, Apartment 3

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60660

Email Address: jon@dorsal.tk

Organization Name:

Comment: Requiring lock-down and conformance labeling for SDR devices effectively ruins their usefulness as SDR devices. The whole point of SDR is that they can be arbitrarily reconfigured at run time. A much better solution is to continue in the manner the FCC already does for HAM Radio - let devices do what they may, and if someone uses a device improperly blame them, not the device.

Requiring lock-down for devices with 802.11\* wifi radios is, if anything, even less sensible. Such a rule would make it impossible to install an alternate operating system on any computer or mobile device containing such a chip, and completely ignores the fact that such chips can be installed at any time with expansion cards or USB peripherals. If lock-down for wifi devices is required, it should be at the hardware or firmware level on the chip itself, without needlessly impinging on the rights of independent driver authors, hobbyist operating system programmers, or anyone who wants to change the software running on their computer or mobile device. One important system that would be irreparably damaged by this rule would be the Linux operating system. If it cannot be used with wifi on commercial off the shelf computers, that makes it significantly harder for developers to continue improving it, which in turn puts several of the US Navy's weapons systems at long-term risk by orphaning the operating system used, including the Zumwalt class of ships and certain types of naval drones. Therefore this rule is an unacceptable risk to national security.

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: Aditya

Last Name: Cowsik

Mailing Address: 304 Edgewood Dr.

City: Clayton

Country: United States

State or Province: MO

ZIP/Postal Code: 63105

Email Address: aditya.cowsik@gmail.com

Organization Name:

Comment: I'm concerned with the effect this change would make on the electronics industry. They would essentially make it much more difficult for open and continuing advancement. This government action would harm the whole country for no real benefit.

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: Salguero

Mailing Address: 8501 Willows Rd NE

City: Redmond

Country: United States

State or Province: WA

ZIP/Postal Code: 98052

Email Address: Accusedbold@hotmail.com

Organization Name:

Comment: It has come to my attention that the FCC has proposed, Equipment Authorization and Electronic Labeling for Wireless Devices, that will supposedly "lock down a device" such as a computer or mobile phone from users modifying it in novel and perhaps constructive ways such as fixing a security hole and even prevent them from installing certain OSs without the device functioning fully. This vexes me. I appreciate what the Federal Communications Commission has done for us and the numerous ways it elucidates telecommunications, but I really feel preventing people from modifying their own devices is overstepping some bounds. That is all I wish to say and I hope my voice is heard. If someone took the time to actually read this, then I 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: Michael

Last Name: Maul

Mailing Address: 1102 Park Ave

City: Garner

Country: United States

State or Province: NC

ZIP/Postal Code: 27529

Email Address: mike.maul@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. In particular the justification for this rule is not valid. In particular there are no cases that I know of where consumer wireless devices causes disruption to the spectrum. More importantly this rule would be practically unenforceable and would waste resources of both manufactures, the FCC and inhibit innovation and commerce.

In particular:

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: jake

Last Name: mercadante

Mailing Address: 6403 e don julio st

City: long beach

Country: United States

State or Province: CA

ZIP/Postal Code: 90815

Email Address:

Organization Name:

Comment: I would like to comment against this proposition on the grounds that:

A) This could feasibly put a stop to much development taking place on new wireless technology. Researchers depend on the ability to modify their devices with their own custom software in order to create new ideas and new inventions. These inventions end up in the hands of rescue workers in need of short range ad-hoc wifi, people living in the middle of country / on islands use this tech to increase their connectivity. This is crucial in order for every part of the country to be connected.

B) In many cases, third party programs and operating systems help users patch holes in their devices security or generally improve the overall security of the device. We need to be able to take the protection of our information (such as finances, family situations, etc...) into our own hands when the manufacturer of the device is unresponsive (this is fairly common).

C) This would have a massive impact on the billions of dollars that flow through companies that rely on being able to modify and test their new ideas. This in turn would have a major negative impact on the well being of technological commerce in the US as a whole.

Thank you for reading

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: McManus

Mailing Address: 73 Morningside

City: Torrington

Country: United States

State or Province: CT

ZIP/Postal Code: 06790

Email Address: jacobmcmanus303@gmail.com

Organization Name:

Comment: I hope that you consider the importance of the consumer and end-user's control over devices they purchase. This policy could stifle new research into wireless networking, and disallow consumers to fix problems their wireless device's manufacturers had left in, especially involving security.

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: Erich

Last Name: Warner

Mailing Address: 6342 Cambridge Dr

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78218

Email Address:

Organization Name:

Comment: Please do not implement this proposal. This proposal is extremely anti-consumer in that it will enable corporations to bulk billions of dollars out of consumers by overcharging for devices with limited, mid range and high end capabilities and this regulation will remove consumers' ability to chose to run different software to achieve the capability they want or need.

In addition:

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 for reading this comment.

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: Rice

Mailing Address: 2217 Halcyon Ln

City: Vienna

Country: United States

State or Province: VA

ZIP/Postal Code: 22181

Email Address:

Organization Name:

Comment: I payed for a great number of things in my life which possess FCC regulated connectivity, I deserve to do what I want with them.

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: Steven

Last Name: Powers

Mailing Address: 35740 Riverside Dr SW

City: Albany

Country: United States

State or Province: OR

ZIP/Postal Code: 97321

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: Aswin

Last Name: Karuvally

Mailing Address: Karuvally, Muhamma P.O

City: Alappuzha

Country: India

State or Province: Kerala

ZIP/Postal Code: 688525

Email Address:

Organization Name:

Comment: Sir,

You have no idea what you are doing.

What is the use of computers if you cannot modify it's working?

I shall die than live among computers whose firmware/OS cannot be hacked.

By going forward with your decision, you will be seriously hampering computing research, as all of them depend upon modified firmware and software.

What if my system has a serious bug, or a feature which I would like to turn off?

For example, the aggressive throttling of CPU which can overheat my laptop.

With locked down computers, I will have no option, but to use a device with an inbuilt oven.

And for god's sake, If I am paying for the device, I should have the ability to decide what should run on the device. The manufacturing company have no right to force me to use some paid crippleware.

I don't even understand your way of thinking.

Locking down the OS/firmware is not the answer to anything.

No system is secure. Not even if you lock it down virtually.

If you want to create an unbreakable wireless system, turn it off and lock it inside a huge vault.

Think again, You have smart people. If you go ahead with this decision, I am pretty sure that many big corporations are going to pay.

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: Rad

Last Name: Sturgis

Mailing Address: 6118 turnbury park drive apt 11305

City: Sarasota

Country: United States

State or Province: FL

ZIP/Postal Code: 34243

Email Address: Radsturgis@me.com

Organization Name:

Comment: Hello. Thanks for your hard work on net neutrality. Big telecoms suck. Please do not interfere with wifi technology such as routers and phones as the large groups of people that work on these in their free time often help to make them safer in the long run. This "jailbreak" culture has helped to make iOS and iPhones far more secure then if it had been illegal to do so.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ross

Last Name: Lopata

Mailing Address: 2149 W. Ivanhoe St.

City: Chandler

Country: United States

State or Province: AZ

ZIP/Postal Code: 85224

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: Mike

Last Name: Bell

Mailing Address: 2102 Talbot Court

City: Fernandina Beach

Country: United States

State or Province: FL

ZIP/Postal Code: 32034

Email Address: ezuratechan@gmail.com

Organization Name:

Comment: To whom it may concern,

Hi.

As a lifelong Computer Scientist, I am deeply concerned about the legislation that the FCC is proposing. Were it not for my God-given right to modify my electronic devices to suit both my curiosity and my needs, I would not have a place in this world, nor would countless other individuals, institutions, organizations, etc. that depend on our right to modify our electronic devices. The legislation proposed threatens a fundamental way of life central to the maintenance and progress of computer technologies, primarily in that:

- Wireless networking research depends on the ability to freely inspect, investigate, and modify 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.

There is no other way to say this: the law in its current form is extremely flawed and will only serve to not only harm but endanger the American people. The right to modify electronic devices is God-given: anyone can do it, freely, in their own homes, schools, and workplaces, right now, without knowing a single thing about what they are doing - and in doing so, can engage in a form of self-education that would be impossible should this proposal pass.

America is a great nation - one that put Freedom of Speech at the top of the list. Well, this law is a threat to Freedom of Speech. Freedom of Speech extends into not only the things we say with our voice but the things we say with our hands as well, and that certainly includes how we might choose to modify our electronic devices.

I trust that others who care about this issue as much as I do will have the courage to speak up and make our voices heard, and that the FCC will do the right thing and not move forward with this 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: Cole

Last Name: Johnson

Mailing Address: 23 Berlamo

City: Rancho Santa Margarita

Country: United States

State or Province: CA

ZIP/Postal Code: 92688

Email Address: coleharrisjohnson@gmail.com

Organization Name:

Comment: THIS IS A BAD IDEA

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Booloodian

Mailing Address: 5401 Sandrock Dr

City: Columbia

Country: United States

State or Province: MO

ZIP/Postal Code: 65202

Email Address: michael.silverbane@gmail.com

Organization Name: Mr.

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 for your consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Austin

Last Name: Schafer

Mailing Address: 896 Sutro Ave

City: Novato

Country: United States

State or Province: CA

ZIP/Postal Code: 94947

Email Address: acsmars@gmail.com

Organization Name:

Comment: I'm a software developer for an open source software defined networking company. I am not commenting on behalf of my company in any way, but rather on behalf of a very young and very promising technology that could be stifled by this proposed regulation.

The ability for 3rd parties and end users to install their own software on all networking devices they own is essential to the expansion of SDN and all the advantages it provides to networking. This regulation could limit open SDN deployment to devices without wireless capabilities and those with SDN software installed by the manufacturer. Many SDN systems, which are designed to be modular and extensible would be ruled out entirely, which would create a compatibility divide between wired and wireless devices on present and future networks.

Limiting what software can be installed on networking devices would add more incompatibilities to a field already going to great expense to increase hardware compatibility because of the huge development costs for fragmented systems.

Users and developers need the ability to modify the software on all of their networking devices. Hardware limits on radio broadcasting and interference are both acceptable and necessary, but please allow software to keep its greatest benefit: modification.

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: Halbersma

Mailing Address: 269 La Fayette Park Pl. Apt 248

City: Los Angeles

Country: United States

State or Province: CA

ZIP/Postal Code: 90057

Email Address: chalbersma.12@gmail.com

Organization Name: N/A

Comment: This proposal now matter how well meaning is technologically illiterate. They would be used to hamstring wireless communications devices in US markets by device manufactures in order to try and make consumers purchase more hardware more often for things like wireless routers and devices.

I know that seems like a small price to pay to "improve" wireless radio transmissions. However you should know that consumers interested in purchasing "non-standard" hardware can do so now trivially from other countries. These actions will only serve to push manufacturing to other countries and further reduce the FCC's effectiveness at managing wireless transmissions inside the US. And this will come at a cost. There are heaps of companies and actors making custom firmware for "wireless devices" as specified in this proposal. Almost all of them would have to leave the US, cease doing business with US customers or go out of business.

Thank you for your consideration.

CRH

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: Nate

Last Name: Swanson

Mailing Address: 2037 Kountry Lane SE Apt 4

City: Iowa City

Country: United States

State or Province: IA

ZIP/Postal Code: 52240

Email Address: nateswanson08@gmail.com

Organization Name:

Comment: Please, allow me to do what I wish with my own devices. Don't punish many for the actions of a few.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ricardo

Last Name: Flores

Mailing Address: 11826 N Mayfair Rd

City: Spokane

Country: United States

State or Province: WA

ZIP/Postal Code: 99218

Email Address:

Organization Name:

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

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: Vinakovsky

Mailing Address: 17-18 Ellis Ave.

City: Fair Lawn

Country: United States

State or Province: NJ

ZIP/Postal Code: 07410-2165

Email Address: dvinak@gmail.com

Organization Name:

Comment: Please do not implement a rule that would restrict the freedom I have to install my own software on a device I personally own. Furthermore, this proposed legislation is very dangerous in that it would likely impede the steady march of technological progression and competition by eliminating any independent research by individuals and small organizations.

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: Jake

Last Name: Drahos

Mailing Address: 100 Linden Fulmer

City: Ames

Country: United States

State or Province: IA

ZIP/Postal Code: 50013

Email Address: j@kedrahos.com

Organization Name: Iowa State University

Comment: I am commenting with regards to the proposed rules changes that would require manufacturers to implement technical measures to restrict the software which users can install on hardware they have purchased.

As an active ham, I certainly understand the importance of respecting the laws and regulations regarding transmissions and the consequences unauthorized or ill-advised modifications, even only of software, can have on device performance. However, technical measures as implemented by manufacturers are an indiscriminate, heavy-handed, and philosophically objectionable approach to solving the problem for many reasons.

Locking down a device to prevent any and all modification will make many legitimate activities much more difficult. Some examples include education and research. I am currently a college student, and many of the engineering design projects and undergraduate research opportunities in which I participate rely on the low cost and ease of modifying software to achieve novel goals. This is a miracle of modern technology. However, these projects, even though they are done carefully and employ proper engineering practices, would be hamstrung by locked devices.

Security is also a major concern. There are many community efforts that attempt, and succeed, at providing firmware that is more secure and more quickly updated than manufacturer firmware. The use of such secure firmware is often a deliberate decision made for security-conscious applications. These community firmwares are developed properly to avoid causing interference and are held, by the community of end users, to the same or often higher standards than the manufacturer firmware. There is no reason to prohibit this activity - if anything, it should be encouraged - and properly locked-down devices would force it to stop cold.

My final comment in objection to this particular aspect of the proposed change stems from the philosophical concept of ownership of a device. Many people, myself included, feel that the freedom to modify a device is an integral part of ownership. In the case of transmitters, there is a great responsibility associated with these modifications. It is responsible of manufacturers to take steps to prevent accidental or ill-informed modifications from taking place, but it is wrong to apply a blanket prevention of any and all modifications.

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: Weise

Mailing Address: 5550 E Michigan St

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32822

Email Address: sandr0ck2003@gmail.com

Organization Name:

Comment: If I buy a device it is mine. While I will do what I want with it, it should not be a requirement to lock it down. There is no good reason for this. I can understand the radio could be modified, but anyone wanting to do something else with the radio can unlock it to begin with.

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: Ezra

Last Name: Carrick

Mailing Address: 1550 w.main #40

City: Ripon

Country: United States

State or Province: CA

ZIP/Postal Code: 95366

Email Address: ezra.carrick@gmail.com

Organization Name:

Comment: the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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: Holly

Last Name: Harding

Mailing Address: 17 Avondale Ave S

City: Waterloo

Country: Canada

State or Province: Ontario

ZIP/Postal Code: N2L 2B5

Email Address:

Organization Name:

Comment: For the love of god, don't do this.

Nothing is more likely to cause security holes go unpatched than forcing people to use the software that the hardware shipped with. We need to be opening this stuff up, not locking it down further.

There are routers that ship with and require community software, like DD-WRT. Doing this will actively harm American companies by preventing that from happening.