

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: Alexander

Last Name: Greenham

Mailing Address: 208 Quail Run

City: Sutherlin

Country: United States

State or Province: OR

ZIP/Postal Code: 97479

Email Address:

Organization Name:

Comment: Please, do not implement these rules. They are geared towards taking away the ability of end-users to install the software of their choosing on the computing devices that they or their companies own. Wireless networking research depends on the ability of researchers to investigate and modify their devices without having to go through a lengthy certification process that would pull money from them and their research.

Americans should have the right to fix security holes in their devices because the manufacturer refuses to do it themselves. Users have, in the past, fixed serious bugs in their wifi drivers; which would be banned under the NPRM. Billions of dollars of commerce/competition for/from groups, such as secure independent wifi vendors or retail/independent hotspot vendors, depend on the ability of users and companies to install the software of their choosing or modify the hardware as required.

This Ruling is restrictive and leans more towards the larger corporations who won't lose anything if their products are allowed to be modified and fixed, having the ability to modify, change, and control what happens to the device that you paid for and own is one of the basic rights as an American and a human being in the modern world we live in today. There are exceptions to this case, such as proprietary or protected works, but existing laws and rules already cover their protection. Stream lining the system that you have now is a good idea and I like that, however, the rules on the devices and their modifications really are restrictive and would hinder development in both the private and amateur sector.

Modifications to a product or device you own should be allowed, there shouldn't be an arbitrary license of agreement just because you bought the device, it really 'ought to be more open allowing the user to do as they will with the device as long as their activities aren't related to anything that could insight a war or be in conjunction with a crime.

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: Leonardo

Last Name: Schripsema

Mailing Address: ep pessoa 1844

City: Rio de Janeiro

Country: Brazil

State or Province: RJ

ZIP/Postal Code: 22411-072

Email Address:

Organization Name:

Comment: Honestly, this proposal is absurd. This basically kills open-source firmware development, creation of new OSs, and many other things. I'd be really disappointed with the FCC if this gets approved.

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: Chagnon

Mailing Address: 2854 Dresden St.

City: Columbus

Country: United States

State or Province: OH

ZIP/Postal Code: 43224

Email Address: jchagnon2@gmail.com

Organization Name:

Comment: This proposal, if implemented, will be harmful to users, and in me particular.

I am a Linux user, a DD-WRT user, and a CyanogenMod user, all of which will be severely impacted by this current proposal.

In the most general sense this regulation is just exploiting the fact that most users are not able to build their own radio transmitters. Forcing hardware manufacturers to lock down devices just harms open source software and firmware projects.

These devices are simply tools, and like any tool they have the potential to be misused, but this proposal only slightly deters anyone truly motivated but harms tinkering, hobbyist projects, and open source software. It would be like requiring scissor manufacturers to make sure that their scissors were not sharp enough to cut phone lines. Anyone motivated enough would just make themselves a knife, but people who want to use scissors as tools for completely normal and legal purposes would be harmed.

If the FCC wants to go after people misusing the wireless spectrum then by all means prosecute, but this proposal catches legal users in the crossfire. We might be a small minority, but we're the people who care the most about preserving our ability to run custom software and firmware on the devices we own.

These hobbyist activities are the things that get people interested in becoming network engineers, sysadmins, software developers, firmware developers, or hackers who find cool and interesting ways to use hardware and this proposal makes it much more difficult to do that.

I know that the proposal is written in a way that tries to preserve the freedom of users but the reality is that in practice manufacturers are just going to opt to completely lock down their devices because it's easy.

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: Brett

Last Name: Caplan

Mailing Address: 5704 231st Ave E

City: Buckley

Country: United States

State or Province: WA

ZIP/Postal Code: 98321

Email Address: caplanbuckley@gmail.com

Organization Name:

Comment: I would like to ask for the FCC not to implement these restrictions on consumers, as they would take away the ability for users to install the software of their choosing on their own devices. This would be absolutely devastating to many, in particular those who use non-proprietary software. It would also hamper users ability to fix issues with their equipment themselves; many have fixed issues with wireless adapter drivers in the past, something that would be illegal in the NPRM. Users need to be able to fix security holes and other issues in their own devices when the manufacturers have chosen not to. As a concerned consumer, I ask you to please consider these points. Thank you for your time.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Shane

Last Name: Churchman

Mailing Address: 858 Sycamore Lane

City: El Cajon

Country: United States

State or Province: CA

ZIP/Postal Code: 92026

Email Address: mythicflux@hotmail.com

Organization Name:

Comment: As a technical user employed in a STEM field I fundamentally disagree with this poorly throughout and potentially devastating proposal. If enacted it will cause untold loss of economic competitiveness and affect the fundamental livelihoods of many people in technical fields. Not to mention the civil liberties of every day consumers.

At issue is the fundamental right of people who need the ability to ensure their equipment functions in a manor they can verify and control. While there is always the risk of malicious action by a user, this risk exists regardless of what laws are set. A law such as this will not stop those with dubious intentions.

Simply, someone with malicious intend will violate the law, while an honest citizen will be negatively impacted because of unintended consequences.

Presently I operate a number of devices where I install alternative software/firmware for professional and personal reasons. I have a number of PCs, Smartphones and a couple of network WiFi routers that all use alternative firmware. In the case of many of these devices the installation of the firmware is done to address fundamental issues with the software stack of the device, as a result of the manufacturers actions.

- For example my Wifi router runs DD-WRT, an alternative router firmware, in place of the manufacturer original firmware. The latter crashes constantly and was found to contain fundamental security holes the manufacturer refused to fix, citing end of life.

- A number of tablet and smartphone devices I have provided to my family (and use my self) have alternative Android OS based firmware that replaces the stock software. The devices in question were upgraded to address security issues with the older firmware, which the developer did not want to provide security fixes for.

- All of my computing devices come with Wifi integrated. Almost all of my devices run a Linux OS (which i develop for and support for professional reasons). I cannot physically remove the Wifi devices in (which has become the standard on consumer devices), so I could be penalized should I attempt to do something I have done without issue for decades.

The simple fact is that more and more devices have wireless capabilities. The ability to buy a devices without that functionality is becoming impossible.

Users who are not committing crime and acting without nefarious intent should not penalized as a result of FCC trying to mandate something completely impractical and down right dangerous.

Do not eliminate consumer/citizen choice for the sake of an ill-conceived 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: john

Last Name: o'hara

Mailing Address: 800 College Drive Unit 62

City: Vineland

Country: United States

State or Province: NJ

ZIP/Postal Code: 08360

Email Address: john.ohara@outlook.com

Organization Name: fixthispc4.me

Comment: There seems to be a good deal of animosity towards this proposal and I can understand such. If wireless radio bearing devices are locked down, this could prevent people from installing alternative operating systems such as Linux, Solaris, and others on their Windows devices, as well as prevent people from installing one of the many competing builds of android on their phones and tablets. I, and I am sure many others, will not let this abide. The ability to install software of our choice on devices we pay fore is paramount to the flourishing economy of PC and electronic devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: adam

Last Name: page

Mailing Address: 2442 ne 48th st

City: ocala

Country: United States

State or Province: FL

ZIP/Postal Code: 34479

Email Address:

Organization Name:

Comment: This concept is so crazy it's indefensible. The idea that when you buy a computer you have no rights to the code that runs it is like saying if you buy a textbook you have no right to tear out pages, glue in your own pages, move words around... of course you do. You can do whatever you want with it because you bought it. Obviously if you want to publish your alterations and sell them for profit that's a different story (pun intended), but for person use? NO

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: Doe

Mailing Address: Elmer Street

City: Elmerville

Country: Netherlands

State or Province: Foreign

ZIP/Postal Code: 123457ABCD

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: Cody

Last Name: Kesting

Mailing Address: 2347 NW 46th Circle

City: Camas

Country: United States

State or Province: WA

ZIP/Postal Code: 98607

Email Address: cody.kesting@gmail.com

Organization Name:

Comment: This is a terrible idea. What happened to the concept of the Free Market making these decisions?

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: bahehs

Last Name: aldeen

Mailing Address: 3108 north oleander ave

City: ELMWOOD PARK

Country: United States

State or Province: IL

ZIP/Postal Code: 60707

Email Address: zalloumaldeen@live.com

Organization Name:

Comment: This is a very bad proposal. Consumers buy products and expect them to work. Consumers buy products with their hard earned money and they should be in full control of what they own. Having a product that you own yet you can not modify it to your needs demonstrates that this proposal will have a negative impact on electronics.

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: Estrada

Mailing Address: 7219 Union Avenue

City: Whittier

Country: United States

State or Province: CA

ZIP/Postal Code: 90602

Email Address:

Organization Name:

Comment: Device manufactures shouldn't be required to lock their devices open source hardware is essential for the maker community.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Pavel

Last Name: Selivanov

Mailing Address: Moskovski prospect, 91/140

City: Voronezh

Country: Russia

State or Province: Voronezhskaya oblast

ZIP/Postal Code: 394053

Email Address: selivan5@yandex.ru

Organization Name:

Comment: Limiting owner's ability to modify device firmware has 2 major consequences.

First, open-source enthusiast and students projects that create alternative firmware will die. This will stop many interesting innovations, that can create new technologies, which can provide benefit to whole industry, or can become start of new successful business(Apple started like that). And this will prevent talented students from joining the industry.

Second, full control over firmware will come to large companies. This will lead to security problems - only target for large companies is profit, they do not care much about user's privacy and security. And this will lead to restriction of user's freedom not to use soft he/she does not want to use.

You should really reconsider your solution.

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: Mark

Last Name: Cohen

Mailing Address: 805 Clausun Dr

City: Durham

Country: United States

State or Province: NC

ZIP/Postal Code: 27713

Email Address:

Organization Name:

Comment: This is the most cancerously stupid thing to come out of the US government regarding technology in recent memory. This is an extremely heavy-handed attempt to lock down user experiences, and flies in the face of every free market principle this country ostensibly upholds; it's like Stalinism for phones. If this passes, I will literally - not figuratively, literally - move to Norway.

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: Ryder

Mailing Address: 300 Quinton Ct. Apt. 16201

City: Lexington

Country: United States

State or Province: KY

ZIP/Postal Code: 40509

Email Address:

Organization Name:

Comment: As a person who has supported the FCC's ruling on Network Neutrality, I am asking the FCC not to implement rules and regulations which take away the ability of users to configure their devices how they wish, and install systems and firmware of their choosing. What the FCC has proposed is something that will cause great harm to professional and enthusiast technicians, researchers and developers under the guise of security: Fields of study into wireless technology requires researchers' ability to modify and configure their devices in certain ways. Under the FCC's proposal, researchers will be vastly restricted from being able to conduct research, testing, configuration and conclusions in studies, thereby damaging innovation into wireless technology. If the FCC seeks security into wireless technology, it needs to allow professional researchers the ability to conduct related experiments without restrictions. Technicians who use devices with a certain security hole from a manufacturer who has not fixed this issue, need the freedom to resolve the vulnerability themselves. Under the FCC's proposal, technology users will not be able to continue to resolve critical vulnerabilities in their devices for personal security, and will be reliant upon untrustworthy manufacturers. Retail hotspot and secure wifi vendors rely on the ability to install their own software and firmware into devices, which would be restricted by the FCC's ruling, causing massive losses in profit. Importantly to many that has caused a large portion of concern, under the FCC's proposal, Personal Computer users and Technical people would be hindered from installing alternative and custom operating systems, firmware and hardware for their personal use, as well as on Web servers, which is very important to system administrators who maintain web sites and web applications. People need to be able to do certain things with their devices and the wireless portions of them. It is essential that the FCC does not introduce regulations which tamper with these aspects that are crucial to innovation, research, commerce, internet traffic, systems administration and the hobbies of technical people.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Rohrlach

Mailing Address: 2739 Donna Ave

City: Bozeman

Country: United States

State or Province: MT

ZIP/Postal Code: 59718

Email Address:

Organization Name:

Comment: To whom it may concern:

The ability to install and modify firmware on electronic devices is important to to both hobbyists and professionals alike. The open ecosystem of low-level software engineering allows people to fulfill special needs that may not be met by a manufacturer. In addition, the ability to work on our own hardware furthers the cause of both security and that of attracting new people to these fields. Please do not force us out of our equipment.

Best wishes,

Matthew

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: julia

Last Name: amine

Mailing Address: 15550 north star lane

City: prescott

Country: United States

State or Province: AZ

ZIP/Postal Code: 86305

Email Address: amineskyblu@gmail.com

Organization Name: Select...

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.

THIS IS ANOTHER LIST OF RULES AND REGULATIONS WRITTEN BY PEOPLE THAT DO NOT HAVE THE PUBLIC'S INTEREST AT HEART AND POSSIBLY PASSED BY REPRESENTATIVES THAT DO NOT UNDERSTAND THE TECHNOLOGY NOR THE POSSIBLE IMPLICATIONS TO FREE SPEECH AND INNOVATION.

Julia Amine

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Stumpf

Mailing Address: 8342 Monique way

City: Cypress

Country: United States

State or Province: CA

ZIP/Postal Code: 90630

Email Address:

Organization Name:

Comment: I wonder if this would effect my ability to get cheap products from overseas to make my own little projects with, would u need to apply for a license, would all the overseas companies need to, and if they didn't would their products become useless? Also, I don't believe the government SHOULD control my internal network infrastructure.

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: Lucien

Last Name: Walters

Mailing Address: 23 The Tynings

City: Stroud

Country: United Kingdom

State or Province: Gloucestershire

ZIP/Postal Code: GL6 9EW

Email Address: bliequearts@gmail.com

Organization Name:

Comment: As a user and advocate of free open-source software GNU/Linux in particular I find the notion that wireless devices should be locked or otherwise shielded from modification by their user(s) very concerning. Giving consumers the freedom to modify the software that operates the technology they own is an important part of placing them in control of said technology.

In the case of a locked or closed system, users may unknowingly be the subjects of privacy invasion and digital spying, perhaps never as relevant an issue as it is today. Additionally, bugs in software running within closed systems can have a serious security impact on users. With a closed system, technologically adept users are not only unable to find problems and report or even fix them, but are unable to apply fixes provided by the technology community. There have been many cases in the past of bugs in closed-source software remaining unnoticed for long periods of time, something that free public source-code review would likely prevented. The poor track record of many companies in terms of maintaining software for older products only serves to suggest that hobbyists are a more reliable source of updates, but locked systems prevent this significant community contribution.

I understand that the majority of users do not realise the importance of or care for the ability to modify software of wireless devices, but that makes it no less necessary. In fact, as many enthusiasts report security flaws in commercial software, all users benefit, whether theyre aware of it or not, from wireless systems not being forcefully locked.

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: S

Last Name: Fortune

Mailing Address: 11201 Byfield Ct

City: Richmond

Country: United States

State or Province: VA

ZIP/Postal Code: 23229

Email Address:

Organization Name:

Comment: To hell with this

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jesse

Last Name: Litton

Mailing Address: 960 Crannog Way

City: Conroe

Country: United States

State or Province: TX

ZIP/Postal Code: 77301

Email Address: federalregister.gov@eternaldusk.com

Organization Name: n/a

Comment: As a networking/IT professional, as well as a consumer versed in open source operating platforms, I strongly recommend that the FCC \*NOT\* implement any rules that interfere with our ability to run whatever software we choose on our computing devices.

I have bought many devices such as routers where the vendor has been totally negligent to fix security flaws and other bugs with their software. The ability to install open firmware as a replacement is a necessity in these situations. Rules to the contrary would put consumers at risk.

Artificially restricting users for fear of a few rare situations that would be better addressed upon infringement is not only harmful to consumers: Secure wifi and retail hotspot vendors depend upon the ability to control their own software stacks in order to provide their services. NPRM will destroy billion-dollar businesses.

This is also harmful to the progress of computing in general. Open source operating systems drivers cannot be locked down in any meaningful way, a majority of the users are also the developers of the drivers - there is no vendor providing drivers. Open source software is the powerhouse behind the internet, and cutting Americans off from it or adding additional hurdles will simply put us behind other nations.

Also, access to the source of these drivers and the ability to make/test changes is invaluable to security researchers. Artificial restrictions would only harm the security of American computing systems and create much greater risk than the issues NPRM was meant to address.

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: Sanchez

Mailing Address: 21 Hillcrest Ave

City: Ellenville

Country: United States

State or Province: NY

ZIP/Postal Code: 12428

Email Address:

Organization Name:

Comment: This is an absolute horrible idea. Consumers should be free to use their devices which they purchase however they please. There is no reason anyone should be locked into using a proprietary OS such as Windows because the hardware is locked down. The same goes with mobile phones. Users should have the ability to install custom aftermarket firmware if they please for security reasons or other reasons. Look at the stagefright vulnerability. Most people with locked devices are still vulnerable and will remain vulnerable to it whereas most aftermarket firmware such as CyanogenMod include patches for these security holes as soon as possible. OEMs are slow to patch these security holes and their patches have to go through the cellular providers too. Do not force manufacturers to lock down their products. All it does is hurt consumers and the security of their devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anurag

Last Name: Choudhury

Mailing Address: 135 N Misty Dawn Dr

City: The Woodlands

Country: United States

State or Province: TX

ZIP/Postal Code: 77385

Email Address:

Organization Name:

Comment: Dear FCC,

I would like to implore that you do not implement the proposed rules. While signal bands are a resource that should be regulated, this large scale lock-down or radio firmware is a terrible method of regulation that will prove harmful in short and long term.

Instead, illegal use of restricted bands should be directly punished instead of harming the wide ecosystem of software revolving around RF devices.

For the continued existence of essential programs like OpenWRT and innovative research in collaborative band sharing like mesh networks, wireless device's firmware must NOT be locked down.

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: Edgar

Last Name: Hassler

Mailing Address: PO Box 25616

City: Tempe

Country: United States

State or Province: AZ

ZIP/Postal Code: 85285

Email Address: ehassler@gmail.com

Organization Name:

Comment: No. The change to approval is too restrictive.

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: Pravin

Last Name: Bashyal

Mailing Address: Bharatpur 2

City: Chitwan

Country: Nepal

State or Province: Bagmati

ZIP/Postal Code: 44201

Email Address: pravin.bashyal@gmail.com

Organization Name:

Comment: Why is fcc always against open source? This is not acceptable or fcc will have consequences.

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: Randy

Last Name: Hart

Mailing Address: 7220 Holworthy Way

City: Sacramento

Country: United States

State or Province: CA

ZIP/Postal Code: 95842

Email Address:

Organization Name:

Comment: This ruling would be the biggest mistake the FCC had ever made. It is not only taking away multiple rights of US citizens, it is hindering forward development and betterment of technology for use by humans. Please, I'd you have the least bit of common sense in your department, do not pass this ruling.

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: Benjamin

Last Name: Barr

Mailing Address: 2727 Pleasant Valley Road

City: Harrisonburg

Country: United States

State or Province: VA

ZIP/Postal Code: 22801

Email Address: bbarr807@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: James

Last Name: Stager

Mailing Address: 6 Ryder Ct.

City: Dix Hills

Country: United States

State or Province: NY

ZIP/Postal Code: 11746

Email Address:

Organization Name:

Comment: Locking down the firmware for new devices

creates severe issues not only for home users

but also network engineers like myself. Some businesses aren't made of money and need reliable, cheap SOHO routers loaded with custom Linux firmware. When anyone spends money on a device they deserve total control of it as long as it's function does not impede others.

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: Jaya

Last Name: Kumar

Mailing Address: 2217 Lennox Place

City: Santa Clara

Country: United States

State or Province: CA

ZIP/Postal Code: 95054

Email Address: k.jayakumar+fcc@gmail.com

Organization Name: Private Individual

Comment: Dear FCC,

Thank you for giving us the opportunity to provide feedback on your proposed rule. I strongly urge the FCC to not implement this rule.

This rule will have the effect that it will take away the ability of users to install the software of their choosing on their computing devices that they have purchased.

Recent history has shown that significant innovation and improvement in consumer products has come from engineers and developers being able to freely modify and control and develop and test changes in consumer level products. Wireless networking research is heavily reliant on the ability of researchers to investigate and modify their devices.

Users must have 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. Such an action would be made infeasible 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 attention.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Benjamin

Last Name: Kirkbride

Mailing Address: 1525 N Kohler Rd

City: Orrville

Country: United States

State or Province: OH

ZIP/Postal Code: 44667

Email Address: BenjaminKirkbride@gmail.com

Organization Name:

Comment: As a constituent, I believe that further restrictions on the wireless spectrum as proposed would be extremely harmful. My beliefs can be summarized as follows:

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Bryan

Mailing Address: 928 Rhode Island St.

City: Sturgeon Bay

Country: United States

State or Province: WI

ZIP/Postal Code: 54235

Email Address: drewbryandrewbryan@gmail.com

Organization Name:

Comment: How does this possibly help the end use? This only benefits big corporate interests. This is wrong and an infringement on freedom. Please don't do this. This will destroy creativity.

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: Lee

Last Name: Griner

Mailing Address: 2134 SE North Blackwell Dr

City: Port St Lucie

Country: United States

State or Province: FL

ZIP/Postal Code: 34952

Email Address: lee.griner@gmail.com

Organization Name:

Comment: Respectfully, the FCC is encroaching on freedoms that they know nothing about. The devices that people rely on, even for their health, only progress further by the efforts of citizens who own the devices, not the manufacturer. Manufacturers leave critical holes in software that never get fixed and hold software freedoms from the user. These security holes would cost billions of dollars in damage, had some random Joe not tested a patch on his own hardware and brought it to the attention of higher organizations.

Please stop these tirades of making rules for technologies our government does not understand. 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: Kirk

Last Name: Sharrar

Mailing Address: 2180 Capital Ave

City: Medford

Country: United States

State or Province: OR

ZIP/Postal Code: 97504

Email Address: sharrark@gmail.com

Organization Name:

Comment: Using your comment and the article I created a nice well explained comment to post:

Dear FCC,

From my point of view you should be doing the exact opposite. It should be illegal for OEMs and ISPs to lock down devices they sell to consumers. The fact that my phone's bootloader is locked, preventing me from updating my phone's OS with security patches, is asinine. You should be suing and fining the companies that do this because it's entirely anti-consumer.

This would more than likely restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc. And also prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes.

Moreover it will ban installation of custom firmware on your Android phone and surely discourage the development of alternative free and open source WiFi firmware, like OpenWrt.

Imagine in case of disaster it will infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel.

It's not only Anti-Consumer but also prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

Sincerely

Kirk Sharrar

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: Thayer

Mailing Address: 614 Franklin St

City: Hinsdale

Country: United States

State or Province: IL

ZIP/Postal Code: 60521

Email Address: benthayer2365@gmail.com

Organization Name:

Comment: I have a hobby for exploring what I can do with comouters. One of those hobbies is to see what I can do with new operating systems. I even have a friend that made his own operating system. We'd like to be able to keep doing that without having to worry about anything legal

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: Ryley

Last Name: Noel

Mailing Address: 489 River Valley Drive

City: Grand Bay-Westfield

Country: Canada

State or Province: New Brunswick

ZIP/Postal Code: E5K 1B1

Email Address: limelimes1@gmail.com

Organization Name:

Comment: Hello FCC, I'd like to kindly ask you to not implement rules rules that take away the ability of users to install the software of their choosing on their computing devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ian

Last Name: Dunbar

Mailing Address: 140 e Washington Ave

City: Bethlehem

Country: United States

State or Province: PA

ZIP/Postal Code: 18018

Email Address: iancdunbar@hotmail.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: Greg

Last Name: Schwartz

Mailing Address: 146 East St

City: Hadley

Country: United States

State or Province: MA

ZIP/Postal Code: 01035

Email Address: gcschwartz@gmail.com

Organization Name:

Comment: If I own a device, I should be able to modify that device in any way as long as I am not breaking other regulations, like FCC broadcast limits. There are many reasons why people might modify or replace the software on their wireless routers including:

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.

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Thank you for your time.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Gary

Last Name: McGill

Mailing Address: 255 saint andrews st

City: hayward

Country: United States

State or Province: CA

ZIP/Postal Code: 94544

Email Address:

Organization Name:

Comment: I believe consumers such as myself should be able to replace firmware on wireless devices.

Replacing the firmware on devices, such as Linksys WRT54GL, with firmware such as OpenWRT, improves security. Backdoor's that hackers leverage can be removed, and VPN can be natively installed, which secures all internet traffic inside a residence.

Replacing firmware will also allow wireless routers to have an extended life, reducing landfill.

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: Richard

Last Name: Sturgill

Mailing Address: 1175 Canandaigua Rd

City: Palmyra

Country: United States

State or Province: NY

ZIP/Postal Code: 14522

Email Address:

Organization Name:

Comment:

The locking of device firmware to prevent potential abuse, which has not been shown to pose a significant problem, creates vastly more problems than it solves. The whole premise is akin to locking people out of the engine of their car in order to prevent them from circumventing emissions regulations.

Furthermore, this is a serious encroachment of on the rights of ownership. Owners should have the right to use any hardware they purchase in any way that they see fit within the bounds of lawful purposes, this includes developing their own software or fixing broken manufacturer's software.

Regulations that would take ownership away from the purchaser of a product overstep the scope of their purpose by preventing perfectly lawful use of equipment. The proposed regulations do not adhere to the legal principle of "least restrictive means" and will almost certainly not stand up against any serious legal challenge.

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: Alexander

Last Name: Smith

Mailing Address: 1312 N. Claremont, #3

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60622

Email Address: aosmith@gmail.com

Organization Name:

Comment: To who it may concern:

It is crucial that Americans continue to be able to install custom firmware on their own equipment. So called "locked down" devices would prohibit true ownership and stifle innovation.

This includes but is not limited to:

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Roland

Last Name: Ryan

Mailing Address: 1920 County Road CC

City: Hartford

Country: United States

State or Province: WI

ZIP/Postal Code: 53027

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: John

Last Name: Johnson

Mailing Address: 59 Hawkins Cres

City: Winnipeg

Country: Canada

State or Province: Manitoba

ZIP/Postal Code: R2N1H7

Email Address: theodorec1998@gmail.com

Organization Name:

Comment: First and foremost, I believe the FCC should not implement rules that take away the users freedom to install the software of their choosing on their electronic devices. Users should be able to manipulate and control all aspects of devices that they own and that they have paid for.

People need the ability to fix security holes in their devices when the manufacturer chooses to not do so, particularly when the manufacturer wants you to buy the latest product rather than to stick with your otherwise perfectly functional device.

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.

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: anon

Last Name: ymous

Mailing Address: 438 stanford road

City: fairless hills

Country: United States

State or Province: PA

ZIP/Postal Code: 19030

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.

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: Mark

Last Name: Garfin

Mailing Address: 502 1/2 Spring Street

City: River Falls

Country: United States

State or Province: WI

ZIP/Postal Code: 54022

Email Address: fcccomments@superkuh.com

Organization Name:

Comment: The idea that software defined radio devices need to be locked down so that the firmware cannot be modified is contrary to the entire idea of a software defined radio. This rule change is so broad that consumer wireless routers would fall under the software defined radio rules. This alone shows the drafters of the rules do not understand what SDR is.

Being able to change the channels of a wifi router does not make it a software defined radio. By conflating these things the FCC will only hobble consumer devices and leave them unable to upgrade and deal with security issues in a timely manner since the companies which sell such routers are often very slow or even incapable of fixing such holes.

Legislation of software will not fix this issue. It will only create more problems. Please stay out of software pre-crime and go back to dealing with actual emissions.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Chris

Last Name: Stout

Mailing Address: General Delivery

City: Olympia

Country: United States

State or Province: WA

ZIP/Postal Code: 98502

Email Address:

Organization Name:

Comment: This plan is absolutely asinine.

When I purchase a device I expect to be able to use it as I please. I imagine that the modifications that the FCC wants to prevent that would cause interference are already against policy.