

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.

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: Clint

Last Name: Nichols

Mailing Address: 675 Glenbrook Dr

City: Ione

Country: United States

State or Province: CA

ZIP/Postal Code: 95640

Email Address:

Organization Name:

Comment: Do not waste government efforts trying to prevent people from modifying their wireless devices. It would be a futile attempt at best even if you do but trust me when I tell you not to bother. If you really think you're going to stifle the genius that is the wireless device modification community then I feel bad for you. These are some of the most dedicated hard working individuals that America (and the world) have at hand. So please save my tax dollars and go repair a road or police actual violent crime/private property disputes and not waste your time on something that isn't achievable. The people are more bright and nimble than the sluggish overbearing giant that is the US government.

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: Egan

Mailing Address: Landman2@hotmail.ca

City: Calgary

Country: Canada

State or Province: Alberta

ZIP/Postal Code: T2X3H6

Email Address:

Organization Name:

Comment: Here in Canada, basically all of our electronics come from the U.S. So any changes to laws and/policies regarding electronics and wireless technologies affects Canadians just as much as Americans.

Reasons these new anti consumer rules for American electronics are bad:

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

Individuals 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.

Individuals should have full control over all aspects of their devices, utilizing digital locks prevents friendly innovation and encourages users to seek out methods to break these locks. Individuals should be able to control, manipulate, fix, research, view, etc... all aspects of their devices.

American business will loose out to companies based in countries where they do not have to follow these new rules.

Mesh networking can allow individuals to communicate freely in an uncensored manor independent of the normal Internet. This has huge benefits for disasters, social media, and future illiterations of the Internet. These new rules would push the mesh networking community underground and prevent any new mesh networking inventions that may some day rival the traditional Internet.

These new rules are not needed!