

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: Sean

Last Name: Bober

Mailing Address: 7309 5TH AVE S

City: RICHFIELD

Country: United States

State or Province: MN

ZIP/Postal Code: 55423

Email Address: smbober@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: Alexander

Last Name: Bender

Mailing Address: 9004 Woodiron Dr

City: Duluth

Country: United States

State or Province: GA

ZIP/Postal Code: 30096

Email Address: alexanderbender2010@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.

Sincerely,
Alexander Bender

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: Thomas

Last Name: Hatzopoulos

Mailing Address: 305 East 8th Street

City: Lockport

Country: United States

State or Province: IL

ZIP/Postal Code: 60441

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: Nathan

Last Name: Watkins

Mailing Address: 7391 friend rd

City: Portland

Country: United States

State or Province: MI

ZIP/Postal Code: 48875

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: Tad

Last Name: Orcot

Mailing Address: 9279 Laguna Pointe Way

City: Elk Grove

Country: United States

State or Province: CA

ZIP/Postal Code: 95758

Email Address:

Organization Name:

Comment: Please don't.

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: Belken

Mailing Address: 415 Broad Street

City: Mokane

Country: United States

State or Province: MO

ZIP/Postal Code: 65059

Email Address: rbelken@belken.us

Organization Name:

Comment: Locking out phones and routers will not make them more secure. If anything, it will allow companies and anyone crafty enough to write their own exploits into the closed off code. With open source code, people can at least find exploits and patch them. The reason we overwrite software on our phones and routers to begin with is because we don't trust the companies who made them, the company stopped providing patches for our product, or the companies who made them gave us a bad product that we want to fix. A lot of websites get DDOS'd by botnets of insecure routers that stopped being patched anyways, so I don't understand how any of this is going to help, or how any of this wont make the problem worse. We know what we are getting into when we put this software on our devices. We just want to be more secure. Do not treat us like we are idiots who can't handle the consequences of our own actions. If you are so concerned about open source software being compromised, why does so much of the us government use Linux? Why do web admins trust Linux? Do not take this right away from us.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Wood

Mailing Address: 1400 Asp Ave, Room 1142W

City: Norman

Country: United States

State or Province: OK

ZIP/Postal Code: 73072

Email Address: jameswood@ou.edu

Organization Name:

Comment: I would like to urge the people of the FCC to not implement rules that disallow control of our own devices. Experimentation with those things around us is a very common way new innovations are created. To this, I would like to add the following points:

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Without an easy way to test ideas, new wireless products will diminish.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Many times manufacturers do not wish to put money into developing security fixes for products that may have been discontinued, or are just not economically feasible to release updates for.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Many individuals are much more efficient at fixing bugs than a corporation as there are significantly more individuals working on the project as well as they are not motivated by money.

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: Constantine

Last Name: Charlamov

Mailing Address: hiangel999@gmail.com

City: Stavropol

Country: Russia

State or Province: Stavropolskiy krai

ZIP/Postal Code: 355000

Email Address:

Organization Name:

Comment: It would hit even notebooks, that nonsense.

Besides device manufactures often makes an awful firmware. In the same time nowadays mobile devices are like PC, and these HAVE TO HAVE a way to change an OS.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: Bonner

Mailing Address: 3207 scoville

City: berwyn

Country: United States

State or Province: IL

ZIP/Postal Code: 60402

Email Address: carvell86@gmail.com

Organization Name:

Comment: 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.

Users should be able to manipulate and control all aspects of their devices.

Manufactures will likely employ digital locks in the easiest manner they can rather than worrying about letting you still use your device fully to the extent of the law. This means you get locked out of other things, cannot check for back doors, etc... It's cheaper to implement a lock that encompasses the entire device rather than trying to individually lock or unlock each little line of code depending on the legalities.

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: Paul

Last Name: Whitty

Mailing Address: 1753 S DeFrame St

City: lakewood

Country: United States

State or Province: CO

ZIP/Postal Code: 80228

Email Address: whitty@colorado.edu

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: Jason

Last Name: Smidt

Mailing Address: 228 Fairmount Ave

City: Santa Cruz

Country: United States

State or Province: CA

ZIP/Postal Code: 95062

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: nobody

Last Name: nobody

Mailing Address: nobody@x.x

City: no

Country: XX

State or Province: no

ZIP/Postal Code: no

Email Address:

Organization Name:

Comment: die pls, die

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: Todd

Last Name: Wilkinson

Mailing Address: 756 S Broadway Apt 408

City: Los Angeles

Country: United States

State or Province: CA

ZIP/Postal Code: 90014

Email Address: todd.wilkinson0@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

I write to you today with great concern that companies, individuals, first-responders, and researchers will be restricted in their legal use of legally purchased wireless equipment and computing systems.

Over the last several years we have seen a large growth in radio-enabled devices. Bluetooth and Wi-Fi seem to be attached to every consumer grade computer device on the American market. It is understandable that a fear of unregulated firmware or software may be loaded on to these devices and cause interference to vital services has grown. I applaud the FCC for being forward looking in this regard.

However, disallowing modification of previously approved devices is not the answer. Americans have a long history of tinkering, hacking, fixing and improving their purchased goods. Researchers and engineers modify and adapt existing systems to meet new needs or begin the next wave of technology.

This proposal is especially scary as it becomes increasingly difficult to not have personal data stored on radio-enabled devices. Many times our most used systems, whether a laptop or a smart-phone, are vulnerable to attack with no patch in sight from service providers or the manufacturers themselves. An individual should have a right to protect their sensitive data. Alternative operating systems and hardware firmware are the best way to achieve this. We must be allowed control of our devices.

Other solutions may exist. Perhaps a device should not be certified in the first place if (with no hardware changes) it is made to operate outside FCC regulation in other markets.

I urge you to consider my concerns during your deliberations. I am confident that you will find them compelling.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nicholas

Last Name: Ericson

Mailing Address: 1149 14th Avenue South

City: Birmingham

Country: United States

State or Province: AL

ZIP/Postal Code: 35205

Email Address: Quantumpolagnus@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: justin

Last Name: meyer

Mailing Address: 3105 Larkspur Cir

City: College Station

Country: United States

State or Province: TX

ZIP/Postal Code: 77845

Email Address: triztal@yahoo.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: Gabriel

Last Name: Hernandez

Mailing Address: 16429 Cactus St

City: Hesperia

Country: United States

State or Province: CA

ZIP/Postal Code: 92345

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: jacob

Last Name: lunde

Mailing Address: 7055 Old Mayfeild Rd

City: Paducah

Country: United States

State or Province: KY

ZIP/Postal Code: 42003

Email Address: jacob.lunde@gmail.com

Organization Name: West Kentucky Technical Collage

Comment: The idea you would want to lock a device like this is outrageous. Many huge leaps were done by people looking at the source code and finding new ways for hardware to do amazing things. You even don't see the trend that even Microsoft sees. They donated 70 million to Cyanogen team so they could continue to make wonderful opensource products. When the industry is helping those in the open source fields, even many open source products are used by the government like Linux web servers (Because of greater securities).

I hope this joke of an idea is seen for what it is, and you will go about getting real work done.

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: Eckert

Mailing Address: 6111 Winsome Ln, Apt 44

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77057

Email Address: jreckert@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: Riley

Last Name: Moses

Mailing Address: 17866 Lunnonhaus Drive, Apt 3

City: Golden

Country: United States

State or Province: CO

ZIP/Postal Code: 80401

Email Address:

Organization Name:

Comment: I respectfully ask that the FCC not limit my ability to install the software of my own choosing on devices that I own. Not only would it be a fruitless effort (just about anything can act as a modem/router nowadays), but it would be a classic case of "if _____ is outlawed, only outlaws will _____". The people who really care about maliciously broadcasting at unapproved power levels and/or on unapproved frequencies will continue to do so, while law-abiding consumers will no longer have the freedom to configure devices that they have paid for and rightfully own. It makes sense to try and minimize unauthorized wireless interference, but my objections come down to 2 main points:

1. The principle of the matter - I paid for a device, so I should be able to choose how I use it. I'm not paying for a license to use the software, nor accepting terms and conditions. It is mine. If the manufacturer abandons my device and leaves me with security holes or bugs, I should be able to switch to software that fixes those problems. If an alternative firmware allows me to prioritize my traffic or add other features that the stock software lacks, I should have the freedom to use it on a device that I own.
2. The proposed rules are not a solution - As I mentioned before, any hardware that has the capability to broadcast at unapproved power levels and frequencies can be made to do so. DRM/manufacturer limitations are a chicken-and-egg game. Software restrictions can almost always be overcome. And in the rare situations where they can't, people will simply buy other hardware and repurpose it. These rules treat a symptom rather than a cause; limiting the software that can run on these devices ignores the fact that the root cause is hardware. I'm sure it's convenient for manufacturers to make a single hardware platform with all required components and then selectively enable/disable those components for each region where the product is sold. But if this is truly a problem that the FCC cares about, you should enforce rules that require compliant hardware rather than placing blanket restrictions on all consumers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Markus

Last Name: Schulz

Mailing Address: 4218 Englewood Blvd

City: Johnson City

Country: United States

State or Province: TN

ZIP/Postal Code: 37601-1034

Email Address: schulz@alpharesearch.de

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install custom software and or firmware on there personally owned computing devices.

Most commercial manufacturers only support their products for a short time, like 1-2 years in best cases. It would be possible to buy a product where the support for fixing security holes is less than 6 month or no support at all. I specificity select the computing hardware so that I can support these for many more years my self with open source software and firmware. It would be better to work together with the open source projects to install the correct emission outputs and warning messages that it would be illegal to output more in the USA for example. Anyway this new rule would also create a lot more trash faster because consumers would just need to dispose the hardware more often. This would cause CO2 levels to rise while burning the old hardware on a trash piles. With open source software it is possible to recycle some old hardware for some more years of use. The new requirements would also make the new hardware more expensive and that would put another huge burden on all the people of the USA. Most devices are not made in the USA and if I can not see and choose what software is running on this I can never be sure there is not a Chinese spy software running as well. For example Chinese manufacturer Lenovo had a rootkit in their PC firmware to install some extra software that automatically updates itself via the Internet. We need a way for legit and legal open source projects to exist in the future as well. Just making it illegal is not a good solution for the people of the USA.

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: Sam

Last Name: Tkach

Mailing Address: 32 carriage house ln

City: Little silver

Country: United States

State or Province: NJ

ZIP/Postal Code: 07739

Email Address:

Organization Name:

Comment:

Instead of pontificating on the practical reasons due to which this proposal is not a good one (which I'm sure many other comments have done and will do), I'd like to take a look at the philosophical ramifications.

For humans, machines of any sort are "accelerators" of some human attribute. For instance, no one can run as fast as a car's top speed. Automobiles are movement accelerators. This idea applies to everything from coffee machines to garden rakes to computers. Computers are thought and communication accelerators. Whether we like it or not, the widespread nature of computers (and especially the advent of the internet) has irrevocably changed the paradigms by which most humans communicate.

Proposals like this one must be carefully weighed, because if we serve corporate interests with computing laws, we are handing these corporations the idea of human consciousness on a silver platter. If free speech and (much more importantly) free thought are to be protected, laws must not remove freedoms of the user to choose the tools they use to expand their consciousness (I.e.- software).

Would you want to buy a car with a hood that didn't open and tires that can't be changed? I hope not.

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: Keith

Last Name: McPherson

Mailing Address: 2010 Jeffy Trl #212

City: Madison

Country: United States

State or Province: WI

ZIP/Postal Code: 53719

Email Address: Damorian@gmail.com

Organization Name:

Comment: I am a software developer and IT professional who is very concerned about the impact these changes will have on security and usability. On nearly every router/hotspot I've owned I've needed to install DD-WRT in order to properly secure my network and improve performance. Most pre-installed firmware is limited and doesn't give administrators the capability to properly monitor and implement their networks. In my experience this includes unpatched security vulnerabilities, lack of proper dmz/port forwarding settings, and no simple way to monitor connected devices and bandwidth usage. This is necessary for any situation outside a basic home network.

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: Parker

Last Name: Reed

Mailing Address: 160 Holston Mountain Road

City: Elizabethton

Country: United States

State or Province: TN

ZIP/Postal Code: 37643

Email Address: parker.l.reed@gmail.com

Organization Name:

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

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: Leo

Last Name: Delil

Mailing Address: vre Baklandet 23

City: Trondheim

Country: Norway

State or Province: Sr-Trndelag

ZIP/Postal Code: 7013

Email Address:

Organization Name:

Comment: Dear FCC, i would very much like to pick for myself which software i put onto something that i own.

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: Zachary

Last Name: Brown

Mailing Address: 7306 Blanco Peak Street

City: Las Vegas

Country: United States

State or Province: NV

ZIP/Postal Code: 89139

Email Address:

Organization Name:

Comment: This proposal will effectively block open-sourced hardware from being used to better advance our technological boundaries. In doing so you put the power of authority to a small number of large companies. These companies would control and slow the expedition of new study into the working of this technology thus putting the United States as a whole behind it's competitors.

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: Harsh

Mailing Address: 5577 Sunnywoods

City: Cincinnati

Country: United States

State or Province: OH

ZIP/Postal Code: 45239

Email Address:

Organization Name:

Comment: As a consumer, I believe I should be able to modify the device I purchased in any way that I see fit. As such, restricting my ability to load my own software on a device I've purchased ends up hurting me, the consumer, and provides absolutely zero benefit to me whatsoever.

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: Norulak

Mailing Address: 516 Bash Road

City: Toms River

Country: United States

State or Province: NJ

ZIP/Postal Code: 08753

Email Address: midnitte@gmail.com

Organization Name:

Comment: Banning the use of Open Source alternatives would not only harm hobbyists, it would also allow abuse from governments and businesses.

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: Cipriano

Mailing Address: 458 Clipper Street

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94114

Email Address:

Organization Name:

Comment: Please do NOT create rules limiting the software a user can install on their own devices. This is censorship, invasion of privacy, and way out of line with what the FCC should be doing.

This also limits the abilities of users to fix faulty software installed by default on their machines, and makes it harder to adequately evaluate different software options.

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: Anthony

Last Name: Teem

Mailing Address: 2800 Riverview Rd, Apt 926

City: Birmingham

Country: United States

State or Province: AL

ZIP/Postal Code: 35242

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: Brian

Last Name: Phelps

Mailing Address: 4711 Connell Drive

City: Raleigh

Country: United States

State or Province: NC

ZIP/Postal Code: 27612

Email Address: lm317t@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

I am writing you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

I am an embedded hardware engineer. I got my start by experimenting with firmware on Linksys devices. I love to tinker. At no time have I ever broken a law in my tinkering nor do I have any desire to do so. But this rule would assume that tinkerers like me are already guilty by forcing the manufacturer to prevent us from using our equipment as we wish. It is sad that this law implies that I am a would be-criminal in addition to stifling innovation and safe and secure use through my own security patches.

My current router runs DD-WRT because the manufacturer firmware is full of security bugs like the WPA PIN bug and a mysterious open port. This new rule would mean I am at the mercy of a manufacturer to fix the firmware. They do not because they have no incentive to do so. They just sell another newer model that likely has its own new bugs.

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. I just cannot imagine how any engineer or researcher would think this rule is a good 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: Jeff

Last Name: Stainbrook

Mailing Address: 920 Fir Acres Dr.

City: Eugene

Country: United States

State or Province: OR

ZIP/Postal Code: 97401

Email Address: jeff@staindomain.com

Organization Name:

Comment: There is absolutely no benefit to the American people by making the changes as stated. We should be able to unlock the full potential of the hardware we purchase by any means we see fit. By blocking the ability for open source communities to make these changes, you are retarding the nations intelligence by preventing individuals and communities from learning about these technologies through a collaborative effort by people enthralled by technology. The individuals involved are passionate, intelligent, and only want people to be able to use their products to their full potential.

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: Charboneau

Mailing Address: 115 Laurel Branch Ct

City: Roswell

Country: United States

State or Province: GA

ZIP/Postal Code: 30075

Email Address: IanChar13oneau@gmail.com

Organization Name:

Comment: I thin k that this would harm the the consumer and hobbyist community. I enjoy being able to modify my hardware in a legal way that still complies with regulations. There is firmware that lets routers operate on ham bands and this is very convenient to me as a licensed ham operator. If these regulations were to be put in place it would severely limit lots of legal and interesting activities and hobbies.

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: Samuel

Last Name: Foxhill

Mailing Address: 2226 W Elizabeth St

City: Fort Collins

Country: United States

State or Province: CO

ZIP/Postal Code: 80521

Email Address:

Organization Name:

Comment: The FCC should not implement rules that take away the ability of users to install the software of their choosing on their computing devices. In addition:

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: hirsch

Mailing Address: 14 hicks lane

City: sands point

Country: United States

State or Province: NY

ZIP/Postal Code: 11050

Email Address:

Organization Name:

Comment: I do not support this rule. The ability of people to use their own devices in the manner of their choosing is very important to me.

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: a concerned user

Last Name: of technology

Mailing Address: 21 nope ln.

City: no soliciting please

Country: United States

State or Province: CT

ZIP/Postal Code: 06850

Email Address:

Organization Name:

Comment: "software controls" are not the answer to this problem...

for the sake of everyone's digital security, owners(consumers) of a device must be able to freely inspect and have the ability to replace/modify software (including firmware, and/or any device control code that can be modified) that controls the operation of that device. if the fcc is concerned about power levels on certain frequencies, i feel it should then be on the manufacturers part to develop a "hardware control" solution to absolutely regulate these parameters. imposing restrictions on the software that control hardware is not enough to eliminate potential abuse.

i think the best middle ground solution would be to require manufacturers to use a hardware parameter validation module, that can verify parameters are within legal operation, and handle any other regulatory requirements while still allowing security conscious people / businesses / govt facilities / etc to run their own trusted properly audited networking code on routers and other devices.

closed source systems are impossible to secure without a team of dedicated highly talented people looking at that one particular firmware revision. the only way to achieve an acceptable level of security in these devices is to have publicly scrutinized source code, do you really think the managers at company X give a shit about doing a proper security audit when the product is behind schedule and big bossman is getting angry? allowing them to code sign their shitty firmware is most definitely NOT going to help solve this security problem.

another concern that is high on my list are the economic repercussions of this new policy. these new restrictions will push this industry away from american companies when the rest of the world is suddenly unable to run properly audited software on their networking hardware. will some other government agency suddenly start restricting the import of foreign radio devices that do allow software modifications? how can this be seen as a legitimate solution to this AFAICT nonexistent problem? the losses far outweigh the gains, in my opinion.

i think this doesn't actually solve the alleged issue, because the root of the issue lies in the HARDWARE, and any new rules should reflect that. please do not get in to the software regulation business. if it can/will be modified in any way, the owner MUST be able to modify it, or at the absolute minimum, must have access to unencrypted machine code, otherwise it becomes incredibly more difficult to know what the device is actually doing, and i hope you really trust taiwan / china / korea / corrupt local conglomeration X / some random asshole that stumbled over their shitty firmware bugs or backdoors to not turn those devices into hostile nodes some day. oh but wait, that bug they used to gain access was "totally just programmer error", right? please don't cut them a break by allowing them to encrypt firmware and do away with these ambiguous "software controls" in favor of a solution that will actually solve this problem the right way, if it really even is a problem...

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: Andres

Last Name: Schmois

Mailing Address: 4000 SW 37th blvd

City: Gainesville

Country: United States

State or Province: FL

ZIP/Postal Code: 32608

Email Address: andresdroid@gmail.com

Organization Name:

Comment: I hereby ask the FCC to not implement the open source rules that are currently being proposed. DIY products are mostly what keeps products alive; products that should have "just been thrown away" years ago are still kept alive and secure because of open source projects. We already live in a throw-it-away-and-get-a-new-one world, why make matters worse? It's incredible that the FCC is even proposing such a rule, if it's all about security, all about reliability, then why don't you start with the companies that make these products? Before a product can be commercial, open source their software and anyone can audit it. Open sourcing not only helps secure things, it also creates innovation. Can you imagine a world where nothing could be open source? How will anyone learn? How will the newer generations ever create new and amazing things? This rule would be ridiculous to be accepted and a major hit to the security of the internet.

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: Kyle

Last Name: Todoulakis

Mailing Address: 2000 Montego Ave #216

City: Escondido

Country: United States

State or Province: CA

ZIP/Postal Code: 92026

Email Address: Ktodoulakis@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: Daniel

Last Name: Beste

Mailing Address: 12965 Robin Lane

City: Brookfield

Country: United States

State or Province: WI

ZIP/Postal Code: 53005

Email Address: dan.ray.beste@gmail.com

Organization Name: K4-T

Comment: The FCC made the right choice turning the internet into a utility. Now make the right choice again and allow people to innovate with the hardware they purchase. Preventing people from installing their choice of software on a device they own will only harm consumers, and move tech startups that rely on more lenient software rules overseas.

If we want to keep America on the forefront of technological innovation, we need to make sure the rules we enact are not overly restrictive. I'm not an expert on this, but from what I've read if the rules pass in their current form, we may end up with some unintended consequences.