

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: Long

Mailing Address: 1003 Timberview Drive

City: Charleston

Country: United States

State or Province: WV

ZIP/Postal Code: 25309

Email Address: christopherlong@gmail.com

Organization Name: null

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

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. 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.

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

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. 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: Nick

Last Name: Garras

Mailing Address: 7334 21st ave me

City: seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98117

Email Address: ncgarras@gmail.com

Organization Name: null

Comment: On behalf of myself and other private citizens of this great country, I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

- 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.
- There is no benefit to the people of this country derived from these changes except for a small number of large corporations.

Please hesitate to make rules just because you are told they are needed by someone with a profit motive.

Nick Garras

On behalf of myself and other private citizens of this great country, I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

- 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.
- There is no benefit to the people of this country derived from these changes except for a small number of large corporations.

Please hesitate to make rules just because you are told they are needed by someone with a profit motive.

Nick Garras

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Booe

Mailing Address: 972 Hunan St. NE

City: Palm Bay

Country: United States

State or Province: FL

ZIP/Postal Code: 32907

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.

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: Andrew

Last Name: King

Mailing Address: One University Hill Drive

City: Buena Vista

Country: United States

State or Province: VA

ZIP/Postal Code: 24416

Email Address:

Organization Name:

Comment: Dear Sir/Madam,

As a person who has always looked at USA as a beacon of freedom, this is of great concern to me that you are trying to implement such a draconian law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Steps and laws like this, when passed one after another, eventually lead to a system as close and authoritarian as those in the Middle East or North Korea.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave ovens. So I find the negative impact on health an unreasonable argument.

Besides, many manufacturers are not updating their firmware fast enough and after a few years they totally abandon their old devices. Having third party open source options that we can rely on is extremely important for us end users.

If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

Sincerely yours, A netizen

Dear Sir/Madam,

As a person who has always looked at USA as a beacon of freedom, this is of great concern to me that you are trying to implement such a draconian law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Steps and laws like this, when passed one after another, eventually lead to a system as close and authoritarian as those in the Middle East or North Korea.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave ovens. So I find the negative impact on health an unreasonable argument.

Besides, many manufacturers are not updating their firmware fast enough and after a few years they totally abandon their old devices. Having third party open source options that we can rely on is extremely important for us end users.

If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

Sincerely yours, A netizen

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: Eickelberger

Mailing Address: 1425 Athens Drive

City: Loveland

Country: United States

State or Province: OH

ZIP/Postal Code: 45140

Email Address:

Organization Name:

Comment: I respectfully request that you do not implement these rules. There are a multiple of reasons for why I believe this idea is misguided. Consumers should be free to choose how they use their devices and the software running on them. Below are several key reasons why this is important:

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.

This would restrict users from any customization of many of the devices they have purchased and own.

I respectfully request that you do not implement these rules. There are a multiple of reasons for why I believe this idea is misguided. Consumers should be free to choose how they use their devices and the software running on them. Below are several key reasons why this is important:

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.

This would restrict users from any customization of many of the devices they have purchased and own.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jessica

Last Name: Litwin

Mailing Address: 1017 South L Street #1

City: Lake Worth

Country: United States

State or Province: FL

ZIP/Postal Code: 33460

Email Address: jessica@litw.in

Organization Name:

Comment: I respectfully submit that this proposed rule would essentially prevent people from installing the operating system and other software on their own computing devices.

As written, it's not outside the realm of possibility that this poorly-scoped regulation would:

- (a) Restrict installation of alternative operating systems like GNU/Linux, OpenBSD, FreeBSD on PC-architecture hardware;
- (b) prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes, since these actions would all require modification;
- (c) prohibit installation of custom firmware on android phones (see A);
- (d) all but destroy the development of alternative free and open source WiFi firmware, like DD-WRT and Tomato;
- (e) technically infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster;
- (f) prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses

Research into improving existing and development of new wireless network technologies often requires modification of testing devices. This proposition would make that impossible.

The open source community will often fix security holes in device firmware where a manufacturer is unable or unwilling to do so. This proposition would prohibit this.

I respectfully submit that this proposed rule would essentially prevent people from installing the operating system and other software on their own computing devices.

As written, it's not outside the realm of possibility that this poorly-scoped regulation would:

- (a) Restrict installation of alternative operating systems like GNU/Linux, OpenBSD, FreeBSD on PC-architecture hardware;
- (b) prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes, since these actions would all require modification;

- (c) prohibit installation of custom firmware on android phones (see A);
- (d) all but destroy the development of alternative free and open source WiFi firmware, like DD-WRT and Tomato;
- (e) technically infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster;
- (f) prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses

Research into improving existing and development of new wireless network technologies often requires modification of testing devices. This proposition would make that impossible.

The open source community will often fix security holes in device firmware where a manufacturer is unable or unwilling to do so. This proposition would prohibit this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matt

Last Name: Turverey

Mailing Address: 150 S Roosevelt Rd

City: Mesa

Country: United States

State or Province: AZ

ZIP/Postal Code: 85202

Email Address:

Organization Name:

Comment: This action will stifle innovation and create 'criminals' out of innocent people.

It also limits ownership of purchased items. If I pay for a thing, the thing is mine to do as I please, as long as it does not harm others.

Inject some common sense into this and stop it before it creates larger problems.

This action will stifle innovation and create 'criminals' out of innocent people.

It also limits ownership of purchased items. If I pay for a thing, the thing is mine to do as I please, as long as it does not harm others.

Inject some common sense into this and stop it before it creates larger problems.

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: Luke

Last Name: Robinson

Mailing Address: PO BOX 557

City: McKinney

Country: United States

State or Province: TX

ZIP/Postal Code: 75070

Email Address: luke@manutransport.com

Organization Name:

Comment: I think the wording here needs a bit more work. Please narrow the scope of your intentions a bit more if a final rule is published. I think most of us understand the merit of such a rule, as long as this rule isn't used to unnecessarily lock down devices that are modified and operate within a legal range.

I think the wording here needs a bit more work. Please narrow the scope of your intentions a bit more if a final rule is published. I think most of us understand the merit of such a rule, as long as this rule isn't used to unnecessarily lock down devices that are modified and operate within a legal range.

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: Ryan

Last Name: Heyser

Mailing Address: 5375 Sugarloaf Pkwy, Apt 9202

City: Lawrenceville

Country: United States

State or Province: GA

ZIP/Postal Code: 30043

Email Address:

Organization Name:

Comment: The rules proposed within could create scenarios where users of defined equipment could become adversely affected by the rules. Where 3rd parties currently create security updates and patches for older hardware, there exist many cases today where using the proposed rules a device would become effectively insecure due to failure by the manufacturer or authorized party to issue needed security updates to these devices. As a customer and software maintainer of several of the products defined within the rules, purposefully creating a scenario where users of these devices become affected by a single entity's inability to issue updates creates a scenario where a large number of users would become effectively using devices where data could be easily stolen. Third parties replace this scenario as a function of porting updates to devices currently dropped for support by their manufacturers. These rules would create further fragmentation of software updates in an era where updates are already rare due do in part to the frequency of hardware refreshes. Rather than focusing on third-parties and open-source developers, perhaps the FCC should be looking closer at the companies that produce the software for these devices and the completely non-standard functionality that most of these devices are shipped with.

The rules proposed within could create scenarios where users of defined equipment could become adversely affected by the rules. Where 3rd parties currently create security updates and patches for older hardware, there exist many cases today where using the proposed rules a device would become effectively insecure due to failure by the manufacturer or authorized party to issue needed security updates to these devices. As a customer and software maintainer of several of the products defined within the rules, purposefully creating a scenario where users of these devices become affected by a single entity's inability to issue updates creates a scenario where a large number of users would become effectively using devices where data could be easily stolen. Third parties replace this scenario as a function of porting updates to devices currently dropped for support by their manufacturers. These rules would create further fragmentation of software updates in an era where updates are already rare due do in part to the frequency of hardware refreshes. Rather than focusing on third-parties and open-source developers, perhaps the FCC should be looking closer at the companies that produce the software for these devices and the completely non-standard functionality that most of these devices are shipped 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: Andrew

Last Name: Donnellan

Mailing Address: 21/4 Jardine St

City: Kingston

Country: Australia

State or Province: ACT

ZIP/Postal Code: 2604

Email Address: andrew@donnellan.id.au

Organization Name:

Comment: I don't want to see FCC regulations prohibit the use of alternative operating systems and firmware on low-power RF devices - this seems an unnecessary restriction on freedom for minimal gain, given the low power at which these devices operate. Even with certified code, many devices have numerous bugs and issues - which don't have a major impact on other devices.

As an Australian I'm concerned that the FCC's moves in this area will impact policymakers in other countries including my own. Please be aware of the international impact of the FCC and the issues this could cause outside the United States.

I don't want to see FCC regulations prohibit the use of alternative operating systems and firmware on low-power RF devices - this seems an unnecessary restriction on freedom for minimal gain, given the low power at which these devices operate. Even with certified code, many devices have numerous bugs and issues - which don't have a major impact on other devices.

As an Australian I'm concerned that the FCC's moves in this area will impact policymakers in other countries including my own. Please be aware of the international impact of the FCC and the issues this could cause outside the United States.

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: M

Mailing Address: 5

City: B

Country: United States

State or Province: WA

ZIP/Postal Code: 98230

Email Address: jacob.morehouse@gmail.com

Organization Name:

Comment: The proposed 2015-18402 is an embarrassment to Americans. Our government should not restrict what the people choose to install on their own devices. There is nothing being "fixed" by doing this, it just limits our choices if we don't like the software on a device.

I purchased an HTC One m7 a few years ago and loved the hardware but disliked all of the fluff that was installed with the carrier's heavily modified version of Android and chose to wipe it out and install Cyanogenmod, which at the time of this comment is more popular than several of the preinstalled operating systems on phones, for just that reason. This rule would have forced me to deal with the hardware manufacturers poor decisions and limited my freedom to act to fix a problem.

I'm writing this from a laptop running Linux, which would also not be possible if hardware manufacturers locked down hardware. I have a home server also running Linux which is an old business server I bought, saving it from a landfill. If I was forced to run and pay for a Windows Server license and necessary CALs to legally run it I would never have afforded it and it would go to a landfill instead.

And what of hobbyists and devices like RaspberryPi? These come with nothing preinstalled at all, would these them be required to? This would completely flatten this market as it completely relies on the ability to install new OSes.

This is embarrassing, and its proposal is clearly that of someone who either doesn't understand the world they live in or is being paid to do this. No sane and moderately educated person would think this is a good idea. We as a people are capable of better.

The proposed 2015-18402 is an embarrassment to Americans. Our government should not restrict what the people choose to install on their own devices. There is nothing being "fixed" by doing this, it just limits our choices if we don't like the software on a device.

I purchased an HTC One m7 a few years ago and loved the hardware but disliked all of the fluff that was installed with the carrier's heavily modified version of Android and chose to wipe it out and install Cyanogenmod, which at the time of this comment is more popular than several of the preinstalled operating systems on phones, for just that reason. This rule would have forced me to deal with the hardware manufacturers poor decisions and limited my freedom to act to fix a problem.

I'm writing this from a laptop running Linux, which would also not be possible if hardware manufacturers locked down hardware. I have a home server also running Linux which is an old business server I bought, saving it from a landfill. If

I was forced to run and pay for a Windows Server license and necessary CALs to legally run it I would never have afforded it and it would go to a landfill instead.

And what of hobbyists and devices like RaspberryPi? These come with nothing preinstalled at all, would these them be required to? This would completely flatten this market as it completely relies on the ability to install new OSes.

This is embarrassing, and its proposal is clearly that of someone who either doesn't understand the world they live in or is being paid to do this. No sane and moderately educated person would think this is a good idea. We as a people are capable of better.

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: Parilla

Mailing Address: 10821 Childs St.

City: Silver Spring

Country: United States

State or Province: MD

ZIP/Postal Code: 20901

Email Address:

Organization Name:

Comment: To whom it may concern,

By not allowing citizens to modify their own computing equipment a level of control is asserted over our lives that chafes against the exploratory and open outlook that is essential for progress or research.

A centralized regulation concerning what the public can or cannot do in regards to our wifi routers demonstrates the monetization of politics and the lobbying of large ISPs. The government would never assert this on their own (generally they listen and respond), this regulation came from the main ISPs. Considering their monopolistic tendencies regarding network coverage and the parceling of the United States leading to stagnating markets devoid of competition beneficial to the consumer, how can they honestly contend their centralized regulation will benefit the public? The quality of their products will continue to act as a drain rather than a boon. Let them fail.

To whom it may concern,

By not allowing citizens to modify their own computing equipment a level of control is asserted over our lives that chafes against the exploratory and open outlook that is essential for progress or research.

A centralized regulation concerning what the public can or cannot do in regards to our wifi routers demonstrates the monetization of politics and the lobbying of large ISPs. The government would never assert this on their own (generally they listen and respond), this regulation came from the main ISPs. Considering their monopolistic tendencies regarding network coverage and the parceling of the United States leading to stagnating markets devoid of competition beneficial to the consumer, how can they honestly contend their centralized regulation will benefit the public? The quality of their products will continue to act as a drain rather than a boon. Let them fail.

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: Dustin

Last Name: Mallonee

Mailing Address: 905 Vandenberg Dr

City: Biloxi

Country: United States

State or Province: MS

ZIP/Postal Code: 39531

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.

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: Douglas

Last Name: Byrd

Mailing Address: 24029 Clyde Cockerham lane

City: Denham Springs

Country: United States

State or Province: LA

ZIP/Postal Code: 70726

Email Address: snoopdougdydug@yahoo.com

Organization Name: null

Comment: There is no reason for you to need to do this. All you are doing is violating the right of consumers to use what they buy for what they choose fit.

There is no reason for you to need to do this. All you are doing is violating the right of consumers to use what they buy for what they choose fit.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brett

Last Name: Faulder

Mailing Address: 5910 Norfolk Drive #305

City: Lincoln

Country: United States

State or Province: NE

ZIP/Postal Code: 68505

Email Address: bafaulder@gmail.com

Organization Name: null

Comment: Please do not pass legislation that would lock down devices with a modular wireless radio or a device with an electronic radio. Modification of these devices through free and open source software drives competition and innovation. Why would anyone want to prevent research into advanced wireless technology or mesh networking?

I can speak specifically in the case of routing firmware WRT. I work as a network administrator and this downloadable modification to routers continues to make my life easier every day.

Manufacturers should not have the final say on what happens to their devices. Once I have purchased the device, if I should choose to modify it and knowingly void the warranty, then that is my choice to do so.

Please do not pass legislation that would lock down devices with a modular wireless radio or a device with an electronic radio. Modification of these devices through free and open source software drives competition and innovation. Why would anyone want to prevent research into advanced wireless technology or mesh networking?

I can speak specifically in the case of routing firmware WRT. I work as a network administrator and this downloadable modification to routers continues to make my life easier every day.

Manufacturers should not have the final say on what happens to their devices. Once I have purchased the device, if I should choose to modify it and knowingly void the warranty, then that is my choice 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: Leonard

Last Name: Payne

Mailing Address: 1457 London Road

City: Sarnia

Country: Canada

State or Province: Ontario

ZIP/Postal Code: N7S 6K4

Email Address:

Organization Name: null

Comment: Please do not limit the ability of users to install the software of their choice onto the hardware that they purchase.

I am a Canadian research professor. Even though my work is not directly regulated by the FCC, any change to FCC regulations will drastically affect the marketplace and availability of open hardware. A portion of my ongoing work through our Enactus program involves working with alternative operating systems and open source software in order to provide cost-effective, highly-performant mesh networks to rural areas in sub-Saharan Africa with donated hardware.

In the proposed policy change, the rules would lock down the devices (laptops, smartphones and wireless access points) that we are trying to optimize. Within a few generations of hardware, my team would quickly find that the market no longer provides the ability to change a commodity device so that it can function in a mesh network capacity. As it is not a highly-desired consumer capability, mesh network configuration and optimization would not be included in stock firmware, even though the hardware is capable. Most firmware and consumer-based operating systems do not support this capability now, so we must install customized software and firmware to open up the capability. The changes to this policy would make modifying the devices prohibitively difficult, even in nations (like Canada and Zambia) where it is not regulated.

So I would implore you to reconsider the requirement for all FCC certified computing devices to be locked down to avoid changes. Perhaps a re-certification system for modified devices, or a method for certifying third-party firmware would fit the needs of the FCC better, while not hobbling research teams like mine. Thank you for considering my comments.

Please do not limit the ability of users to install the software of their choice onto the hardware that they purchase.

I am a Canadian research professor. Even though my work is not directly regulated by the FCC, any change to FCC regulations will drastically affect the marketplace and availability of open hardware. A portion of my ongoing work through our Enactus program involves working with alternative operating systems and open source software in order to provide cost-effective, highly-performant mesh networks to rural areas in sub-Saharan Africa with donated hardware.

In the proposed policy change, the rules would lock down the devices (laptops, smartphones and wireless access points) that we are trying to optimize. Within a few generations of hardware, my team would quickly find that the market no longer provides the ability to change a commodity device so that it can function in a mesh network capacity. As it is not a highly-desired consumer capability, mesh network configuration and optimization would not be included in stock firmware, even though the hardware is capable. Most firmware and consumer-based operating systems do not support

this capability now, so we must install customized software and firmware to open up the capability. The changes to this policy would make modifying the devices prohibitively difficult, even in nations (like Canada and Zambia) where it is not regulated.

So I would implore you to reconsider the requirement for all FCC certified computing devices to be locked down to avoid changes. Perhaps a re-certification system for modified devices, or a method for certifying third-party firmware would fit the needs of the FCC better, while not hobbling research teams like mine. Thank you for considering my comments.

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: Alex

Last Name: Gray

Mailing Address: 2956 Lexington Trace Dr

City: Smyrna

Country: United States

State or Province: GA

ZIP/Postal Code: 30080

Email Address: null

Organization Name: null

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 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: Bryan

Last Name: Welch

Mailing Address: 1213 S 14th St

City: Adel

Country: United States

State or Province: IA

ZIP/Postal Code: 50003

Email Address: bwelch42@yahoo.com

Organization Name: null

Comment: Please do not take away the ability of users such as myself to install the software I choose or create on my own 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.

Sincerely,
Bryan Welch

Please do not take away the ability of users such as myself to install the software I choose or create on my own 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.

Sincerely,
Bryan Welch

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: Anonymous

Last Name: Anonymous

Mailing Address: Anonymous

City: Anonymous

Country: United States

State or Province: TX

ZIP/Postal Code: 78660

Email Address: null

Organization Name: null

Comment:

Dear Sir/Madam,

As a person who has always looked at USA as a beacon of freedom, this is of great concern to me that you are trying to implement such a draconian law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave ovens. So I find the negative impact on health an unreasonable argument.

Along with that the re-installation of router firmware is almost necessary in modern time. Customization of routers doesn't start at overpowering and destroying the 2.4GHz and 5GHz spectrum, instead customization starts when the companies that are supposed to support and help your existing hardware decide to give you no access and leaves the software abandoned, with security holes and hardware crippling issues. We own the hardware at hand and must be able to customize it's limitations and access in order for it to work for citizen's needs and business needs.

If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

Sincerely yours, A Citizen.

Dear Sir/Madam,

As a person who has always looked at USA as a beacon of freedom, this is of great concern to me that you are trying to implement such a draconian law that significantly impacts freedom of choice, stagnates innovation, and severely depresses citizens and instills a feeling of fear, uncertainty, and doubt in their minds.

Health wise, WiFi routers, even when customized using 3rd party firmware are tremendously safer than microwave

ovens. So I find the negative impact on health an unreasonable argument.

Along with that the re-installation of router firmware is almost necessary in modern time. Customization of routers doesn't start at overpowering and destroying the 2.4GHz and 5GHz spectrum, instead customization starts when the companies that are supposed to support and help your existing hardware decide to give you no access and leaves the software abandoned, with security holes and hardware crippling issues. We own the hardware at hand and must be able to customize it's limitations and access in order for it to work for citizen's needs and business needs.

If anything, we need a law that enforces manufacturers to build open systems that their firmware can easily be replaced by third party commercial or open source alternatives.

Please do not implement laws that decreases freedom of people.

Sincerely yours, A Citizen.