

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.

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: 333575 Georgia Atlanta Station

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30332

Email Address: null

Organization Name: null

Comment: I want to be able to control what software to put on my devices. I do not approve of this proposed rule.

I want to be able to control what software to put on my devices. I do not approve of this proposed rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anthony

Last Name: Coleman

Mailing Address: 2441 Wine Ridge Dr

City: Birmingham

Country: United States

State or Province: AL

ZIP/Postal Code: 35244

Email Address: anthony.coleman@gamil.com

Organization Name:

Comment: Why prevent us from modifying items that WE LEGALLY OWN??

This goes against free property rights and is not american.

Why prevent us from modifying items that WE LEGALLY OWN??

This goes against free property rights and is not american.

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: Walter

Last Name: Seme

Mailing Address: 16 Tower Rd

City: Martinsville

Country: United States

State or Province: NJ

ZIP/Postal Code: 08836

Email Address:

Organization Name:

Comment: Dear FCC,

Please DO NOT pass this proposed rule. This is a terrible rule for the freedom of the Internet and the security of American citizens. By not allowing individuals to install the software they want, American citizens will be restricted and vulnerable to more software exploits. If everyone is using the same software and a bug exists, then more people will be exposed to that bug. This rule is also putting a monopoly on the software that is received. Like Internet Service Providers, monopoly's do not have the interest in the consumer. Lastly, there is no way to enforce this law. If an individual physically controls a device, they will do what ever they want with it and there is no way that this can be changed. Even with security measures in place, if there is a flaw in the router software, then it will be exploited.

A better alternative than this rule would be make router and wifi devices more secure and transparent with what the devices are doing. This also includes exposing the 'super cookies' and tracking that is being done that Internet Services Providers are known to do. One way this could be done is to make the software Open Source so it could be criticized and reviewed by multiple groups and individuals to ensure such devices are secure and not prone to misuse. That is the world that will make American citizens safe and secure from improper use and ensure that these wifi devices and routers are updated and maintained properly. But that is NOT what this rule is proposing.

Please DO NOT pass this rule.

Dear FCC,

Please DO NOT pass this proposed rule. This is a terrible rule for the freedom of the Internet and the security of American citizens. By not allowing individuals to install the software they want, American citizens will be restricted and vulnerable to more software exploits. If everyone is using the same software and a bug exists, then more people will be exposed to that bug. This rule is also putting a monopoly on the software that is received. Like Internet Service Providers, monopoly's do not have the interest in the consumer. Lastly, there is no way to enforce this law. If an individual physically controls a device, they will do what ever they want with it and there is no way that this can be changed. Even with security measures in place, if there is a flaw in the router software, then it will be exploited.

A better alternative than this rule would be make router and wifi devices more secure and transparent with what the devices are doing. This also includes exposing the 'super cookies' and tracking that is being done that Internet Services Providers are known to do. One way this could be done is to make the software Open Source so it could be criticized and reviewed by multiple groups and individuals to ensure such devices are secure and not prone to misuse. That is the world that will make American citizens safe and secure from improper use and ensure that these wifi devices and routers

are updated and maintained properly. But that is NOT what this rule is proposing.

Please DO NOT pass this rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Steve

Last Name: Marks

Mailing Address: Valley Road

City: Waterbury

Country: United States

State or Province: CT

ZIP/Postal Code: 06770

Email Address:

Organization Name:

Comment: If this passes, the FCC could have the ability to...

1. Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.
2. Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes
3. Ban installation of custom firmware on your Android phone
4. Discourage the development of alternative free and open source WiFi firmware, like OpenWrt
5. Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.
6. Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

If this passes, the FCC could have the ability to...

1. Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.
2. Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes
3. Ban installation of custom firmware on your Android phone
4. Discourage the development of alternative free and open source WiFi firmware, like OpenWrt
5. Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.
6. Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

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: Rudy

Last Name: Klecka

Mailing Address: 13210 Madrone Mountain Way

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78737

Email Address: rudy_klecka@email.com

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. I work for a major manufacturer of such devices and even I install my own modified software on them.

The Open Source community has shown time and again its usefulness to both security and general functionality and the passage of this will most certainly kill such communities.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I work for a major manufacturer of such devices and even I install my own modified software on them.

The Open Source community has shown time and again its usefulness to both security and general functionality and the passage of this will most certainly kill such communities.

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: WI

ZIP/Postal Code: Anonymous

Email Address: null

Organization Name: null

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: Chase

Last Name: Weddle

Mailing Address: 10 West Raccoon Ridge

City: Sylva

Country: United States

State or Province: NC

ZIP/Postal Code: 27998

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: Sean

Last Name: Kerr

Mailing Address: 167 S Lexington St

City: St Augustine

Country: United States

State or Province: FL

ZIP/Postal Code: 32084

Email Address: skerr.sa@gmail.com

Organization Name:

Comment: I understand the background reasons for adding rules to govern software on wifi signal devices, however this category is entirely too broad. I am vehemently opposed to the (hopefully) unintended consequences. Such as the prevention of changing operating systems, adding operating systems, and generally modifying software on pc's, phones, and tablets. Please reconsider as this restricts personal freedom and freedom of innovation.

I understand the background reasons for adding rules to govern software on wifi signal devices, however this category is entirely too broad. I am vehemently opposed to the (hopefully) unintended consequences. Such as the prevention of changing operating systems, adding operating systems, and generally modifying software on pc's, phones, and tablets. Please reconsider as this restricts personal freedom and freedom of innovation.

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: Maziar

Mailing Address: 846 W Armitage Ave

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60614

Email Address: jmaziar3@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.

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: Walter

Last Name: Stern

Mailing Address: 320 Smith Ave Apt 3

City: Montevideo

Country: United States

State or Province: MN

ZIP/Postal Code: 56265

Email Address: waldo686@gmail.com

Organization Name:

Comment: I'm here because I read this article:

"The FCC wants to prevent you from installing custom firmware/OSs on routers and other devices with WiFi. This will also prevent you from installing GNU/Linux, BSD, Hackintosh, etc. on PCs"

That is some BS, and this proposed rule is way outta line

I'm here because I read this article:

"The FCC wants to prevent you from installing custom firmware/OSs on routers and other devices with WiFi. This will also prevent you from installing GNU/Linux, BSD, Hackintosh, etc. on PCs"

That is some BS, and this proposed rule is way outta line

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: Nope

City: Christchurch

Country: New Zealand

State or Province: Canterbury

ZIP/Postal Code: 8062

Email Address: null

Organization Name: null

Comment: Please don't do this

Please don't do 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: David

Last Name: Youngquist

Mailing Address: 1214 Clinton Ave.

City: Des Moines

Country: United States

State or Province: IA

ZIP/Postal Code: 50313

Email Address: null

Organization Name: null

Comment: I LOVE my DD-WRT modified router. I run a secure home network that bothers NONE of my neighbors. You regulators should stop needlessly bothering good US citizens and do something useful. You should be working to stop the monopoly of wealthy corporate control of citizen's radio airwaves.

I LOVE my DD-WRT modified router. I run a secure home network that bothers NONE of my neighbors. You regulators should stop needlessly bothering good US citizens and do something useful. You should be working to stop the monopoly of wealthy corporate control of citizen's radio airwaves.

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: Jim

Last Name: Salter

Mailing Address: 1005 Natchez Trail

City: West Columbia

Country: United States

State or Province: SC

ZIP/Postal Code: 29169

Email Address: federalregister@jrs-s.net

Organization Name: JRS Systems LLC

Comment: Please do not implement this regulation as it is described.

Requiring manufacturers to "lock down" devices containing a transceiver would have grave unintended side effects on the marketplace and in the freedom of American citizens.

Manufacturers of routers and wireless bridges frequently leave their devices "abandoned" in terms of software and security updates, very nearly from the moment they are sold. Currently, consumers have the option and ability to fix these issues with open source firmware; this regulation would take away that freedom.

Further, and even more troubling, it would make it legally impossible to install Linux, BSD, or other free and open source operating systems on many if not most general purpose PCs and other computing devices. This would have SEVERE impact on the economy, as these operating systems form the backbone of all internet services, and most internet professionals - and students who will eventually become professionals learn and grow by using these operating systems on their own devices.

Please do not implement this regulation as it is described.

Requiring manufacturers to "lock down" devices containing a transceiver would have grave unintended side effects on the marketplace and in the freedom of American citizens.

Manufacturers of routers and wireless bridges frequently leave their devices "abandoned" in terms of software and security updates, very nearly from the moment they are sold. Currently, consumers have the option and ability to fix these issues with open source firmware; this regulation would take away that freedom.

Further, and even more troubling, it would make it legally impossible to install Linux, BSD, or other free and open source operating systems on many if not most general purpose PCs and other computing devices. This would have SEVERE impact on the economy, as these operating systems form the backbone of all internet services, and most internet professionals - and students who will eventually become professionals learn and grow by using these operating systems on their own 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: Isaiah

Last Name: Soul

Mailing Address: 281 Lexwood Dr

City: Woodville

Country: United States

State or Province: AL

ZIP/Postal Code: 35776

Email Address:

Organization Name:

Comment: The actions proposed in this rule are far too restrictive to American consumers and should not be enacted.

The actions proposed in this rule are far too restrictive to American consumers and should not be enacted.

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: Robert

Last Name: Schwaller

Mailing Address: 3225 W 25th St.

City: Lawrence

Country: United States

State or Province: KS

ZIP/Postal Code: 66047

Email Address:

Organization Name:

Comment: While updating the certification and authorization of transmitting devices is important, changes that would inhibit endusers from modifying their electronics in legitimate ways would be detrimental to consumers. This includes installing new operating systems on to home computers, tablets, cellular phones, routers, etc.

While updating the certification and authorization of transmitting devices is important, changes that would inhibit endusers from modifying their electronics in legitimate ways would be detrimental to consumers. This includes installing new operating systems on to home computers, tablets, cellular phones, routers, etc.

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: Get

Last Name: Rekt

Mailing Address: 1234 rekt rd

City: seattle

Country: United States

State or Province: OR

ZIP/Postal Code: 98101

Email Address:

Organization Name:

Comment: Dont be a dick and dont do this you dummies

Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes

Ban installation of custom firmware on your Android phone

Discourage the development of alternative free and open source WiFi firmware, like OpenWrt

Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

Dont be a dick and dont do this you dummies

Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes

Ban installation of custom firmware on your Android phone

Discourage the development of alternative free and open source WiFi firmware, like OpenWrt

Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

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: Simon

Last Name: Dedman

Mailing Address: 234 Sycamore Street

City: San Carlos

Country: United States

State or Province: CA

ZIP/Postal Code: 94070

Email Address: simondedman@gmail.com

Organization Name:

Comment: Please do not allow this rights-violating law to pass, it's ridiculous. Thank you.

Please do not allow this rights-violating law to pass, it's ridiculous. 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: Austin

Last Name: Savage

Mailing Address: 55 Sea Park Blvd Apt 405

City: Satellite Beach

Country: United States

State or Province: FL

ZIP/Postal Code: 32937-2261

Email Address: finfan321@yahoo.com

Organization Name:

Comment: Please consider the lives this will affect. My personal hobby is installing and tinkering with computers and this will mess that up. Please don't pass this, I beg you.

Please consider the lives this will affect. My personal hobby is installing and tinkering with computers and this will mess that up. Please don't pass this, I beg 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: Jeremy

Last Name: Mill

Mailing Address: 155 west main street, Apt 420

City: vernon

Country: United States

State or Province: CT

ZIP/Postal Code: 06066

Email Address: jeremymill@gmail.com

Organization Name: LivingInSyn

Comment: I believe that this is not a good rule. This action can stifle innovation, and freedom for the sole purpose of preventing something which is at most, a minor problem. Owners of a device should OWN their devices, and be free to do with them as they wish inside of the laws and regulations of the FCC.

I believe that this is not a good rule. This action can stifle innovation, and freedom for the sole purpose of preventing something which is at most, a minor problem. Owners of a device should OWN their devices, and be free to do with them as they wish inside of the laws and regulations of the FCC.

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: Theodore

Last Name: Rolle

Mailing Address: 1298 Old Clyde Rd, Apt E6

City: Clyde

Country: United States

State or Province: NC

ZIP/Postal Code: 28721

Email Address: TheodoreMRolle@students.abtech.edu

Organization Name:

Comment: I would like to respectfully request that the FCC not enact any laws that would prevent end users from installing their own software on wireless devices. The ability of end users to modify software on devices they own is very important for research, and allows end users to update or patch bugs and security holes in firmware that is no longer in active development by the manufacturer.

I would like to respectfully request that the FCC not enact any laws that would prevent end users from installing their own software on wireless devices. The ability of end users to modify software on devices they own is very important for research, and allows end users to update or patch bugs and security holes in firmware that is no longer in active development by the manufacturer.

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: Logan

Last Name: Skrzypczak

Mailing Address: PSC 1 Box 4066

City: APO AE

Country: United States

State or Province: NY

ZIP/Postal Code: 09009

Email Address: LoganDS@Outlook.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.

Bullet Points Below:

- 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.
- The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
- These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

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.

Bullet Points Below:

- 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.
- The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
- These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Santangelo

Mailing Address: 1132 Edpas Road

City: New Brunswick

Country: United States

State or Province: NJ

ZIP/Postal Code: 08901

Email Address: michael.santangelo@gmail.com

Organization Name: n/a

Comment: I respectfully request that the FCC take a good, long look at this before accepting it. These rules would greatly restrict and limit the ability of end users who own hardware to install, tweak, and modify their personal equipment. This is the wrong direction for technology as a whole, but especially so with regard to any sort of communications equipment.

Specific complaints include:

Wireless research depends on our ability to break down, modify, and investigate hardware and the software that runs on that hardware.

We need the ability to examine and fix security holes in our personally owned devices regardless of whether or not the manufacturer has done so. For example with cell phones, there is an exploit called Stagefright. Custom ROMs for phones like the Galaxy S4 have had the fix for the Stagefright exploit for months. I only received an update from Samsung 3 days ago. Custom ROMs for phones could conceivably be outlawed in your wording of this proposal (modular wireless radios found in cell phones).

Please, do not restrict what we can and cannot do with our own equipment in this day and age.

Thank you for your time and consideration.

I respectfully request that the FCC take a good, long look at this before accepting it. These rules would greatly restrict and limit the ability of end users who own hardware to install, tweak, and modify their personal equipment. This is the wrong direction for technology as a whole, but especially so with regard to any sort of communications equipment.

Specific complaints include:

Wireless research depends on our ability to break down, modify, and investigate hardware and the software that runs on that hardware.

We need the ability to examine and fix security holes in our personally owned devices regardless of whether or not the manufacturer has done so. For example with cell phones, there is an exploit called Stagefright. Custom ROMs for phones like the Galaxy S4 have had the fix for the Stagefright exploit for months. I only received an update from Samsung 3 days ago. Custom ROMs for phones could conceivably be outlawed in your wording of this proposal (modular wireless radios found in cell phones).

Please, do not restrict what we can and cannot do with our own equipment in this day and age.

Thank you for your time and consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nathan

Last Name: Johnson

Mailing Address: 1213 NE Green St

City: Lees Summit

Country: United States

State or Province: MO

ZIP/Postal Code: 64086

Email Address:

Organization Name:

Comment: Hello,

Please allow us to continue to install our own firmware on our own personal property. It is a violation of rights for the government to mandate that we free citizens must use a certain product without the ability to choose freely.

Hello,

Please allow us to continue to install our own firmware on our own personal property. It is a violation of rights for the government to mandate that we free citizens must use a certain product without the ability to choose freely.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jesse

Last Name: Larson

Mailing Address: 1665 Hanover At

City: Aurora

Country: United States

State or Province: CO

ZIP/Postal Code: 80010

Email Address: larson.jessem@gmail.com

Organization Name:

Comment: Controlling the way a person uses their devices wither it be browsing facebook, playing games, creating documents, or installing different operating systems isn't right, it isn't constitutional. The government should have no say in what we do with our devices on software or hardware as long as it is not for child pornography or hacking into sysytems. Being able to pit a different OS on a router,phone, or computer is our freedom as a consumer, and a citizen of the United States of America.

Controlling the way a person uses their devices wither it be browsing facebook, playing games, creating documents, or installing different operating systems isn't right, it isn't constitutional. The government should have no say in what we do with our devices on software or hardware as long as it is not for child pornography or hacking into sysytems. Being able to pit a different OS on a router,phone, or computer is our freedom as a consumer, and a citizen of the United States of America.

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: Damian

Last Name: Sosnowski

Mailing Address: Zarudawie

City: Krakw

Country: Poland

State or Province: Maopolskie

ZIP/Postal Code: 30-144

Email Address: sosnowski.damian@gmail.com

Organization Name:

Comment: Accepting these changes means death to huge development communities that better devices available around the world. It's restricting people freedom to do what they choose with their devices. It will affect global community aswell since many software developers are from USA and most countries would see same restrictions because manufacturers would give them the same hardware with the same restrictions.

Accepting these changes means death to huge development communities that better devices available around the world. It's restricting people freedom to do what they choose with their devices. It will affect global community aswell since many software developers are from USA and most countries would see same restrictions because manufacturers would give them the same hardware with the same restrictions.

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: Jordan

Last Name: Beacher

Mailing Address: 132 Main St

City: Parkesburg

Country: United States

State or Province: PA

ZIP/Postal Code: 19365

Email Address: null

Organization Name: null

Comment: "Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety." - Benjamin Franklin

Freedom has always been at the core of this country's belief system. Americans in general believe that their own personal freedom is worth more than the assurance that "nothing will ever be able to hurt them". When federal laws start getting passed limiting our freedoms and privacy in order to try to better protect us from terrorists or anyone wishing to do us harm, in the end limiting these freedoms and privacies only serves to further our enemies' cause. It stifles innovation and the free market, and creates an environment of dangerous false security while imposing less effective, less efficient, and generally less useful technology on the american people.

Firstly, the thinking that one would need a permit or for some reason would be unable to investigate or modify a wifi device is ridiculous. This is supposed to be a free country and we can't even take a look at the inside of a product we buy, to learn how it works or modify it to better suit our goals/intentions? What if there's a small bug/problem with the device? We would have to ship the product in, wait for them to fix it (while they're mid-recall, presumably extremely busy), and ship it back? Wait for a software/firmware update from the manufacturer? If this becomes law, Americans would not have the ability to fix security holes on their own when the manufacturer fails to do so/chooses not to. In effect, that part of the rule alone could open more security holes and cause more potential harm than not restricting our access to wifi devices.

In addition, there is a huge commerce factor, as there are secure wifi vendors and retail hotspot vendors that depend on the ability of users and companies to install the software of their choosing. This is a huge industry worth billions of dollars.

Thank you for your time and for hearing my opinion. Please don't make this rule law.

"Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety." - Benjamin Franklin

Freedom has always been at the core of this country's belief system. Americans in general believe that their own personal freedom is worth more than the assurance that "nothing will ever be able to hurt them". When federal laws start getting passed limiting our freedoms and privacy in order to try to better protect us from terrorists or anyone wishing to do us harm, in the end limiting these freedoms and privacies only serves to further our enemies' cause. It stifles innovation and the free market, and creates an environment of dangerous false security while imposing less effective, less efficient, and generally less useful technology on the american people.

Firstly, the thinking that one would need a permit or for some reason would be unable to investigate or modify a wifi device is ridiculous. This is supposed to be a free country and we can't even take a look at the inside of a product we buy, to learn how it works or modify it to better suit our goals/intentions? What if there's a small bug/problem with the device? We would have to ship the product in, wait for them to fix it (while they're mid-recall, presumably extremely busy), and ship it back? Wait for a software/firmware update from the manufacturer? If this becomes law, Americans would not have the ability to fix security holes on their own when the manufacturer fails to do so/chooses not to. In effect, that part of the rule alone could open more security holes and cause more potential harm than not restricting our access to wifi devices.

In addition, there is a huge commerce factor, as there are secure wifi vendors and retail hotspot vendors that depend on the ability of users and companies to install the software of their choosing. This is a huge industry worth billions of dollars.

Thank you for your time and for hearing my opinion. Please don't make this rule law.

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: Judson

Last Name: Anderson

Mailing Address: 740 E Coolidge Ave.

City: Appleton

Country: United States

State or Province: WI

ZIP/Postal Code: 54915

Email Address: andejp12

Organization Name:

Comment: Please do not take away the legal option of putting software or OS of a consumers choosing on hardware that they have purchased. This is very useful to make a piece of equipment either more secure or to learn more about networking in general. This rule only helps corporations and simply limits consumer choices.

Please do not take away the legal option of putting software or OS of a consumers choosing on hardware that they have purchased. This is very useful to make a piece of equipment either more secure or to learn more about networking in general. This rule only helps corporations and simply limits consumer choices.