

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Richard

Last Name: Mote

Mailing Address: 3217 SW 18th Street

City: Topeka

Country: United States

State or Province: KS

ZIP/Postal Code: 66604

Email Address: r.j.mote@gmail.com

Organization Name:

Comment: This regulation will have two major detriments to American citizens. The first harm will be to the advancement of American technology and research. For example:

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

The second major harm would be to American commerce and rule of law. That is to say, if the FCC forces companies to lock wireless-capable devices (including smart phones and PCs) and essentially ban consumers from modifying their own property to suit their needs, one of two results (or some combination thereof) will occur. Either:

1. Consumers will buy non-American products, and if non-American products must be so modified as to comply with this regulation to be sold in the United States, consumers will buy non-American versions through grey market or black market channels. At best, this damages American companies and harms local and state sales tax revenues. At worst, it erodes respect for the rule of law, similar to the way Prohibition did in the 1920s.
2. Technology-savvy consumers will begin to manufacture or modify non-regulated 'rogue' hot spots, routers and similar devices. Again, this erodes respect for the rule of law. Also, instead of making the FCC more capable of regulating the use of wireless technology, it will eventually strip the FCC of the ability to effectively regulate wireless communication at all, while simultaneously causing it to appear draconian and/or ridiculous in the eyes of the public.

In short, passing this regulation will, in the short term, harm American technology research and sales, while in the long term, it will harm America as a nation and the FCC as an effective regulatory agency.

This regulation will have two major detriments to American citizens. The first harm will be to the advancement of American technology and research. For example:

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

The second major harm would be to American commerce and rule of law. That is to say, if the FCC forces companies to lock wireless-capable devices (including smart phones and PCs) and essentially ban consumers from modifying their own property to suit their needs, one of two results (or some combination thereof) will occur. Either:

1. Consumers will buy non-American products, and if non-American products must be so modified as to comply with this regulation to be sold in the United States, consumers will buy non-American versions through grey market or black market channels. At best, this damages American companies and harms local and state sales tax revenues. At worst, it erodes respect for the rule of law, similar to the way Prohibition did in the 1920s.

2. Technology-savvy consumers will begin to manufacture or modify non-regulated 'rogue' hot spots, routers and similar devices. Again, this erodes respect for the rule of law. Also, instead of making the FCC more capable of regulating the use of wireless technology, it will eventually strip the FCC of the ability to effectively regulate wireless communication at all, while simultaneously causing it to appear draconian and/or ridiculous in the eyes of the public.

In short, passing this regulation will, in the short term, harm American technology research and sales, while in the long term, it will harm America as a nation and the FCC as an effective regulatory agency.

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: Mario Borna

Last Name: Mjertan

Mailing Address: Orljavska 13

City: Pleternica

Country: Croatia

State or Province: Poeko-slavonska

ZIP/Postal Code: 34310

Email Address:

Organization Name:

Comment: Do not implement this.

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.

We need this for computer science to evolve. Please do not implement this.

Do not implement this.

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.

We need this for computer science to evolve. Please do not implement 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: Andrew

Last Name: Rasch

Mailing Address: 31 Arthur St

City: Little Falls

Country: United States

State or Province: NY

ZIP/Postal Code: 13699

Email Address:

Organization Name:

Comment: Please do not implement rules that inhibits users' abilities to install the software of their choice on computing devices. People should be able to fix security holes in their own devices if possible, and in the past people have contributed to fixing serious bugs in wireless drivers which would be impossible under these new rulings. I believe that restricting installation of operating systems only furthers to create more problems than it solves, and this is due to the fact the security through obscurity is not an effective measure. Not to mention billions of dollars of commerce hinges upon the users ability to install their own software on wireless devices. Please be considerate of the tens of thousands of jobs that would instantly cease to exists because of this.

Please do not implement rules that inhibits users' abilities to install the software of their choice on computing devices. People should be able to fix security holes in their own devices if possible, and in the past people have contributed to fixing serious bugs in wireless drivers which would be impossible under these new rulings. I believe that restricting installation of operating systems only furthers to create more problems than it solves, and this is due to the fact the security through obscurity is not an effective measure. Not to mention billions of dollars of commerce hinges upon the users ability to install their own software on wireless devices. Please be considerate of the tens of thousands of jobs that would instantly cease to exists because of 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: Richard

Last Name: Nava

Mailing Address: 239 W. Colorado Blvd. Apt. 102/B

City: Monrovia

Country: United States

State or Province: CA

ZIP/Postal Code: 91016

Email Address: OliviaHNava@gmail.com

Organization Name:

Comment: Question: Did I buy my computer and/or Android phone? I believe I did. Question: Is it legally my property? I am pretty sure it is. Question: If I want to edit something on my legal property, can I do so? I believe I should be able to.

What you want to pass here is a ridiculous rule. It should NOT be allowed to pass. You need to understand what the limits of the Federal Communications Commission are. You, as a whole, need to stop trying to get so far into others' business. This is my device that doesn't even communicate with other devices, and even if it did, nothing of harm would come to those other devices.

Question: Did I buy my computer and/or Android phone? I believe I did. Question: Is it legally my property? I am pretty sure it is. Question: If I want to edit something on my legal property, can I do so? I believe I should be able to.

What you want to pass here is a ridiculous rule. It should NOT be allowed to pass. You need to understand what the limits of the Federal Communications Commission are. You, as a whole, need to stop trying to get so far into others' business. This is my device that doesn't even communicate with other devices, and even if it did, nothing of harm would come to those other 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: Trevor

Last Name: Lucas

Mailing Address: 1423 14th Ave

City: Greeley

Country: United States

State or Province: CO

ZIP/Postal Code: 80631

Email Address:

Organization Name:

Comment: Hi there. I think its a bad idea to limit what people can do with their computing devices in the name of standardization. I get that having a standard is important, so that everyone is on the same playing field and there are no surprises as far as manufacturers go. But having a standard and locking people out from doing what they want to with hardware they've purchased is quite a bit different. Under the new rule, if I bought a HP computer that came with Windows and decided I didn't like it and wanted to try a Linux distribution, I wouldn't be able to do that right? At least, not without getting express consent from HP to modify their hardware. What if I want to put a different ROM on my Android? I can't without getting express permission. That seems a little excessive to me. I feel like once you've bought the hardware, you should be able to modify it to fit your own needs, without needing to ask permission from the person or company you bought it from. On top of that, modifying and trying new things is part of the learning curve and the innovation aspect of computing evolution. People that are free to try new things with their electronic devices will be able to experiment, create, document, and in general DO more. I know the importance of standards, but let them matter only until the finished product is out the door and in my hands. Thank you.

Hi there. I think its a bad idea to limit what people can do with their computing devices in the name of standardization. I get that having a standard is important, so that everyone is on the same playing field and there are no surprises as far as manufacturers go. But having a standard and locking people out from doing what they want to with hardware they've purchased is quite a bit different. Under the new rule, if I bought a HP computer that came with Windows and decided I didn't like it and wanted to try a Linux distribution, I wouldn't be able to do that right? At least, not without getting express consent from HP to modify their hardware. What if I want to put a different ROM on my Android? I can't without getting express permission. That seems a little excessive to me. I feel like once you've bought the hardware, you should be able to modify it to fit your own needs, without needing to ask permission from the person or company you bought it from. On top of that, modifying and trying new things is part of the learning curve and the innovation aspect of computing evolution. People that are free to try new things with their electronic devices will be able to experiment, create, document, and in general DO more. I know the importance of standards, but let them matter only until the finished product is out the door and in my hands. 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: Justin

Last Name: Willcox

Mailing Address: 420 Ponderosa Drive

City: ATHENS

Country: United States

State or Province: GA

ZIP/Postal Code: 30605

Email Address: justin.j.willcox@gmail.com

Organization Name:

Comment: Based on my limited understanding of the proposal, I am concerned that this policy will limit software development on personal computers and mobile devices. Specifically, I am very concerned that I might not be permitted to replace a mobile phone or desktop operating system, or be prohibited from loading third party device drivers.

Every laptop and phone I have ever owned has borne an FCC label; clearly the scope of the regulation could affect my devices. Because of the integrated nature of modern hardware, I may soon be unable to purchase a computing device that does not contain a modular radio. If modification of my computer would require fresh FCC certification, then consumer software enthusiasts, developers and students may find themselves prohibited from legally using the devices they purchased.

Popular new software is very often developed independently, and then loaded onto commodity devices. If consumers cannot legally modify the software, then manufacturers of these devices will receive protection from market pressures that would otherwise have led to alternate operating systems being developed and installed.

It seems clear to me, that the digital revolution leading to the internet as we know it depended entirely on the ability of individual consumers, as well as entrepreneurial companies, to create and install unregistered software on commodity hardware. The popular understanding of this proposal is in direct conflict with the spirit of innovation that led us to the current day. Please consider amending the proposal to clearly protect third party updates to novel or competing software platforms. Alternatively, please provide clarifying language that updating, modifying or replacing software for the purposes of restoring functionality to a device is, itself, a protected form of "repair". At a minimum, the proposal should clarify that changes in software that do not create changes in the function of RF protocols, signal profiles etc., should not be considered changes that require re-certification. The proposal as written is overly broad, and seems to imply that very little software modification may be performed on computers or mobile devices without re-certification by a consumer.

Based on my limited understanding of the proposal, I am concerned that this policy will limit software development on personal computers and mobile devices. Specifically, I am very concerned that I might not be permitted to replace a mobile phone or desktop operating system, or be prohibited from loading third party device drivers.

Every laptop and phone I have ever owned has borne an FCC label; clearly the scope of the regulation could affect my devices. Because of the integrated nature of modern hardware, I may soon be unable to purchase a computing device that does not contain a modular radio. If modification of my computer would require fresh FCC certification, then consumer software enthusiasts, developers and students may find themselves prohibited from legally using the devices they purchased.

Popular new software is very often developed independently, and then loaded onto commodity devices. If consumers cannot legally modify the software, then manufacturers of these devices will receive protection from market pressures that would otherwise have led to alternate operating systems being developed and installed.

It seems clear to me, that the digital revolution leading to the internet as we know it depended entirely on the ability of individual consumers, as well as entrepreneurial companies, to create and install unregistered software on commodity hardware. The popular understanding of this proposal is in direct conflict with the spirit of innovation that led us to the current day. Please consider amending the proposal to clearly protect third party updates to novel or competing software platforms. Alternatively, please provide clarifying language that updating, modifying or replacing software for the purposes of restoring functionality to a device is, itself, a protected form of "repair". At a minimum, the proposal should clarify that changes in software that do not create changes in the function of RF protocols, signal profiles etc., should not be considered changes that require re-certification. The proposal as written is overly broad, and seems to imply that very little software modification may be performed on computers or mobile devices without re-certification by a consumer.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Bengoechea

Mailing Address: 660 E. Princeton

City: Dinuba

Country: United States

State or Province: CA

ZIP/Postal Code: 93618

Email Address:

Organization Name:

Comment: It is simple, I should be able to alter, modify or enhance any thing I legally own. To make it illegal to do so absolutely has no benefit to the consumer. IF\* down the line this begins to actually cause problems at that point we can begin to make specific restrictions, instead of such a broad one that at the very least we don't yet need and quite possibly never will.

It is simple, I should be able to alter, modify or enhance any thing I legally own. To make it illegal to do so absolutely has no benefit to the consumer. IF\* down the line this begins to actually cause problems at that point we can begin to make specific restrictions, instead of such a broad one that at the very least we don't yet need and quite possibly never will.

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: Kilpatrick

Mailing Address: 302 Brockman Ave

City: Greenville

Country: United States

State or Province: SC

ZIP/Postal Code: 29609

Email Address:

Organization Name:

Comment: The proposed rules would be very detrimental to the nature of the American experiment. Clamping down on open source and end user modification/customization is chilling to innovation, prevents rapid deployment of user identified bug fixes, and most importantly is not in keeping with the spirit of free use and first sale.

Many industries have historically relied heavily on the secondary customization and design market for inspiration, innovation, and improvement. Notable are the automotive industry, sporting goods, and audio equipment.

We would not even have the phone operating systems we have today had they not initially sprung up from open source user modified software to begin with.

DD WRT and similar are the best available solution for a reason, they are open source, they produce genuine value for the end user, and the original manufacturer still gets their hardware sale dollars.

It is difficult to find a real reason to enact these rules besides a step towards oligarchy, and expanded government snooping. The activities which the FCC is seeking to control have essentially been nothing but a boon to end users, and have helped developed some of the most reliable, stable communication devices in the world. To stifle this process would be a grave mistake in a society that has climbed to such heights due to being a champion of freedom and innovation.

The proposed rules would be very detrimental to the nature of the American experiment. Clamping down on open source and end user modification/customization is chilling to innovation, prevents rapid deployment of user identified bug fixes, and most importantly is not in keeping with the spirit of free use and first sale.

Many industries have historically relied heavily on the secondary customization and design market for inspiration, innovation, and improvement. Notable are the automotive industry, sporting goods, and audio equipment.

We would not even have the phone operating systems we have today had they not initially sprung up from open source user modified software to begin with.

DD WRT and similar are the best available solution for a reason, they are open source, they produce genuine value for the end user, and the original manufacturer still gets their hardware sale dollars.

It is difficult to find a real reason to enact these rules besides a step towards oligarchy, and expanded government snooping. The activities which the FCC is seeking to control have essentially been nothing but a boon to end users, and

have helped developed some of the most reliable, stable communication devices in the world. To stifle this process would be a grave mistake in a society that has climbed to such heights due to being a champion of freedom and 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: Juho

Last Name: Jaakkola

Mailing Address: 420 W Slaughter Ln #220

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78748

Email Address:

Organization Name:

Comment: First of all, I would like to thank you for trying to resolve this problem with using frequencies that are not allowed. But, at the same time, I believe that you are going about it the wrong way. Limiting it through software is not a reasonable change. It should be done on the hardware level. You need to buckle down on the manufacturer by being more restrictive on the frequencies the hardware will accept, not the software.

Please reconsider this proposal.

First of all, I would like to thank you for trying to resolve this problem with using frequencies that are not allowed. But, at the same time, I believe that you are going about it the wrong way. Limiting it through software is not a reasonable change. It should be done on the hardware level. You need to buckle down on the manufacturer by being more restrictive on the frequencies the hardware will accept, not the software.

Please reconsider this proposal.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Drew

Last Name: Pawlowski

Mailing Address: 205 West Main Street Apt. 206

City: Perham

Country: United States

State or Province: MN

ZIP/Postal Code: 56573

Email Address:

Organization Name:

Comment: I respectfully ask that the FCC reconsider locking down wireless devices. This is still a growing part of communication technology and the sort of restrictions this rule would apply are immature at best. Denying people the ability to fix or upgrade a communications device that they wholly own is a step backward in time. I can only see the nature of this rule as damaging to the people who wish to legally modify and improve their communication devices.

Thank you for what you do, and please take into consideration that this is still a growing part of technology which would only be hampered by this sort of rule.

I respectfully ask that the FCC reconsider locking down wireless devices. This is still a growing part of communication technology and the sort of restrictions this rule would apply are immature at best. Denying people the ability to fix or upgrade a communications device that they wholly own is a step backward in time. I can only see the nature of this rule as damaging to the people who wish to legally modify and improve their communication devices.

Thank you for what you do, and please take into consideration that this is still a growing part of technology which would only be hampered by this sort of 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: Pranshu

Last Name: Bansal

Mailing Address: 123 Do Not Wish To Disclose St

City: knoxville

Country: United States

State or Province: TN

ZIP/Postal Code: 37932

Email Address:

Organization Name:

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

I think this is a terrible idea, it allows for backdoor creation and closing off systems. This means less security over all. It also removes my ability to customize my own systems in ways that make it a better environment for me.

If you close off a system "legally", the people who want to hack it still will, because they are interested in personal gains. The legality of it doesn't bother them.

However, the people who want to make things more secure won't be able to do so in a manner that is legal. So this will create problems for them.

Furthermore, I think it's silly to not allow people to customize their own software. It would be like disallowing people from picking and placing their own furniture in their homes.

I urge you to not implement rules that take away the ability of users to install the software of their choosing on their computing devices

I think this is a terrible idea, it allows for backdoor creation and closing off systems. This means less security over all. It also removes my ability to customize my own systems in ways that make it a better environment for me.

If you close off a system "legally", the people who want to hack it still will, because they are interested in personal gains. The legality of it doesn't bother them.

However, the people who want to make things more secure won't be able to do so in a manner that is legal. So this will create problems for them.

Furthermore, I think it's silly to not allow people to customize their own software. It would be like disallowing people from picking and placing their own furniture in their homes.

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: Garrett

Last Name: Dunbar

Mailing Address: 3159 Berry lane Apt 34

City: Roanoke

Country: United States

State or Province: VA

ZIP/Postal Code: 24018

Email Address:

Organization Name:

Comment: In this time of America's declining technological superiority I find it disturbing that the FCC would look to hamper technologists and developers from pushing the boundaries of current and future wifi technology through the use of custom software and operating systems. Regulating exactly what can and can not be used on a device that has the ability to connect with a wireless network will only degrade our ability to stay technically relevant today and in the future. There is no realistic reason that this regulation needs to be in place except to protect short minded businesses profit margins and lazy government spy organizations at the expense of innovation. I urge the commission to turn down these proposed rules or at least bring in experts that can accurately explain the plus' and minus' of what these rules will do to the future of wireless networking. Thank you.

In this time of America's declining technological superiority I find it disturbing that the FCC would look to hamper technologists and developers from pushing the boundaries of current and future wifi technology through the use of custom software and operating systems. Regulating exactly what can and can not be used on a device that has the ability to connect with a wireless network will only degrade our ability to stay technically relevant today and in the future. There is no realistic reason that this regulation needs to be in place except to protect short minded businesses profit margins and lazy government spy organizations at the expense of innovation. I urge the commission to turn down these proposed rules or at least bring in experts that can accurately explain the plus' and minus' of what these rules will do to the future of wireless networking. 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: Andrew

Last Name: Petrolino

Mailing Address: 1400 Barton Road

City: Redlands

Country: United States

State or Province: CA

ZIP/Postal Code: 92373

Email Address:

Organization Name:

Comment: This proposal will not end modification of firmware, but will effectively hinder volunteer search and rescue workers who use mesh networks to assist emergency personnel.

In today's turbulent world, the very last thing anyone needs is volunteer emergency assets being tied up by a policy that will be rapidly outmoded and swept aside by the ruthless passage of time and the efforts of volunteer experts; experts who, with all due respect, know far more about this technology than any of you.

This proposal will not end modification of firmware, but will effectively hinder volunteer search and rescue workers who use mesh networks to assist emergency personnel.

In today's turbulent world, the very last thing anyone needs is volunteer emergency assets being tied up by a policy that will be rapidly outmoded and swept aside by the ruthless passage of time and the efforts of volunteer experts; experts who, with all due respect, know far more about this technology than any of 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: Timothy

Last Name: Rideout

Mailing Address: 281 Highland Ave

City: Millinocket

Country: United States

State or Province: ME

ZIP/Postal Code: 04462

Email Address:

Organization Name:

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

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.

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

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: Brent

Last Name: Kasel

Mailing Address: 1104 linden st south

City: Northfield

Country: United States

State or Province: MN

ZIP/Postal Code: 55057

Email Address: dingo9055@gmail.com

Organization Name: We the people

Comment: To quote a well written line, to hide something evil insert it in something boring.

You may not understand exactly what you are going to end up creating with this rule. It is a world where only the rich can make devices. I hope you consider that if you do this it will only support monopoly practices.

Stop trying to limit the end consumer and start cracking down on the isp's if you have gotten board.

One of the things that enable the "economically challenged" to keep using technology is Linux, adding restrictions to this is un-American.

To quote a well written line, to hide something evil insert it in something boring.

You may not understand exactly what you are going to end up creating with this rule. It is a world where only the rich can make devices. I hope you consider that if you do this it will only support monopoly practices.

Stop trying to limit the end consumer and start cracking down on the isp's if you have gotten board.

One of the things that enable the "economically challenged" to keep using technology is Linux, adding restrictions to this is un-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: Erle

Last Name: Bridgewater

Mailing Address: 1734 Alps Court

City: Orange Park

Country: United States

State or Province: FL

ZIP/Postal Code: 32003

Email Address: bridgewaterrobbie@gmail.com

Organization Name:

Comment: This is one of the stupider potential decisions of the FCC which is saying something

This is one of the stupider potential decisions of the FCC which is saying something

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: Tyler

Last Name: Momberger

Mailing Address: 1724 McCollum st

City: San Luis obispo

Country: United States

State or Province: CA

ZIP/Postal Code: 93405

Email Address:

Organization Name:

Comment: I believe this proposal should not pass due to a number of reasons.

- \* 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.

I believe this proposal should not pass due to a number of reasons.

- \* 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: Brendan

Last Name: Parrott

Mailing Address: 3724 SW Kelly Ave

City: Portland

Country: United States

State or Province: OH

ZIP/Postal Code: 97239

Email Address: brjopar@gmail.com

Organization Name: null

Comment: Please do not implement rules that take away my right to install software on devices I own. Third party software for these devices exists because of shortcomings of factory-installed software. If these shortcomings impact the security of my financial information online or prevent my hardware from running correctly, I have a right to correct that. In many cases, third-party software is more secure and more reliable.

Please do not implement rules that take away my right to install software on devices I own. Third party software for these devices exists because of shortcomings of factory-installed software. If these shortcomings impact the security of my financial information online or prevent my hardware from running correctly, I have a right to correct that. In many cases, third-party software is more secure and more reliable.

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: Adams

Mailing Address: 2242 Arlington Ct.

City: Auburn

Country: United States

State or Province: AL

ZIP/Postal Code: 36830

Email Address:

Organization Name:

Comment: How about yo go fuck yourself?

How about yo go fuck yourself?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Foster

Mailing Address: 1401 S Walton Blvd #9-141

City: Bentonville

Country: United States

State or Province: AR

ZIP/Postal Code: 72712

Email Address: fcc@matthewanderin.com

Organization Name: null

Comment: As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the user's needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible. I request that the proposed rule be revisited.

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the user's needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible. I request that the proposed rule be revisited.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: O'Brien

Mailing Address: 25 School Road

City: Horsham

Country: United States

State or Province: PA

ZIP/Postal Code: 19044

Email Address:

Organization Name: People for a Less Dumb Congress

Comment: Do you people seriously have nothing better to do with the time that we are paying you for? If that is the case then I think that it is high time that we voted you ALL out and found others that are willing to work for the people! Leave this stuff alone, I'm tired of having to email and submit comments every time you all want to do something dumb. Seriously, work on fixing the wage imbalance or protecting at risk children or something that actually matters. Now cut it out!

Some points:

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.

Do you people seriously have nothing better to do with the time that we are paying you for? If that is the case then I think that it is high time that we voted you ALL out and found others that are willing to work for the people! Leave this stuff alone, I'm tired of having to email and submit comments every time you all want to do something dumb. Seriously, work on fixing the wage imbalance or protecting at risk children or something that actually matters. Now cut it out!

Some points:

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: Jesse

Last Name: Crouch

Mailing Address: 32 Commencement Drive South Village Residence Room 4052

City: Oshawa

Country: Canada

State or Province: Ontario

ZIP/Postal Code: L1G 8G3

Email Address: xycrouchwb@gmail.com

Organization Name: null

Comment: Hello, I would like to start this comment by mentioning the fact that I am not a US Citizen. However, as a Canadian citizen I feel as though this proposal impacts me in a negative fashion. As a long time user, supporter and developer of Android software I would hate to see 10+ years of combined effort wasted. The idea behind custom softwares designed to be installed on phones is not and has never been to undermine any regulations or authorization. Android has long been an open source platform, free to the public to see. Is it so wrong that we would notice code somewhere that could be improved, and do so? This is just one opinion of many I'm sure, but I ask that you reconsider this proposal so that we as Android users can still enjoy the optimized and bug hunted custom software that we have come to love. Thank you.

Hello, I would like to start this comment by mentioning the fact that I am not a US Citizen. However, as a Canadian citizen I feel as though this proposal impacts me in a negative fashion. As a long time user, supporter and developer of Android software I would hate to see 10+ years of combined effort wasted. The idea behind custom softwares designed to be installed on phones is not and has never been to undermine any regulations or authorization. Android has long been an open source platform, free to the public to see. Is it so wrong that we would notice code somewhere that could be improved, and do so? This is just one opinion of many I'm sure, but I ask that you reconsider this proposal so that we as Android users can still enjoy the optimized and bug hunted custom software that we have come to love. 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: Nick

Last Name: Hoskins

Mailing Address: 8578 Roaring Springs Road

City: Gloucester Courthouse

Country: United States

State or Province: VA

ZIP/Postal Code: 23061

Email Address: null

Organization Name: null

Comment: Why would you even consider this

Why would you even consider 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: Amir

Last Name: Kavuchian

Mailing Address: Yerevan 3045 , 60

City: Yerevan

Country: Armenia

State or Province: Yerevan

ZIP/Postal Code: 2012563435

Email Address:

Organization Name:

Comment: A lot is on the line. The freedom to modify devices you own is a concern, but the proposed rules prohibiting new device firmware would do much more damage. The economic impact would be dire, the security implications would be extreme, and emergency preparedness would be greatly hindered by the proposed restrictions on router firmware. Don't do it

A lot is on the line. The freedom to modify devices you own is a concern, but the proposed rules prohibiting new device firmware would do much more damage. The economic impact would be dire, the security implications would be extreme, and emergency preparedness would be greatly hindered by the proposed restrictions on router firmware. Don't do it

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Richard

Last Name: Petithory

Mailing Address: 363 Pleasant St

City: Melrose

Country: United States

State or Province: MA

ZIP/Postal Code: 02176

Email Address: richardpetithory@gmail.com

Organization Name: null

Comment: I am writing to express my concern over the proposed rule. I find the precedent set by this rule to be very disturbing. My right to do what I want with the equipment I purchase and own should not be violated. Destroying this right puts a damper on innovation, education, and freedom. The proposed rule is no different than losing the right to work on or modify my own car, or any other physical devices I purchase.

Being unable to modify equipment I own means I am unable to find and repair software flaws left in by its manufacturer.

I am writing to express my concern over the proposed rule. I find the precedent set by this rule to be very disturbing. My right to do what I want with the equipment I purchase and own should not be violated. Destroying this right puts a damper on innovation, education, and freedom. The proposed rule is no different than losing the right to work on or modify my own car, or any other physical devices I purchase.

Being unable to modify equipment I own means I am unable to find and repair software flaws left in by its 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: Chastity

Last Name: Davis

Mailing Address: 1859 Bonnie Blue Ln

City: Middletown

Country: United States

State or Province: PA

ZIP/Postal Code: 17057

Email Address:

Organization Name:

Comment: This could be extremely damaging to the careers of many individuals as they rely on modifications to routers and PCs to be able to perform the daily tasks that their jobs require.

This could be extremely damaging to the careers of many individuals as they rely on modifications to routers and PCs to be able to perform the daily tasks that their jobs require.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Cody

Last Name: Endries

Mailing Address: W3168 Cornell Ct.

City: Appleton

Country: United States

State or Province: WI

ZIP/Postal Code: 54915

Email Address: cendries1234@gmail.com

Organization Name: N/A

Comment: This proposed bill is anti-consumer and anti-business, and I do not think that it should be passed in the United States. This bill limits my options as a consumer to modify hardware that I have purchased. Once I make a purchase, the company who made that device no longer owns it, and neither do the US government. I should have complete rights to modify my property as I see fit, weather to add functionality, or to aide in ease of use. This is also anti-business, as it limits the use of alternative operating systems, meaning that if they don't come on a computer, they will not be installed. Since many operating systems, such as Linux, very rarely come installed, they would lose a massive amount of business because of this bill. Linux, for example, would be nearly entirely limited to Android, essentially Granting Microsoft a monopoly over computer operating systems.

This proposed bill is anti-consumer and anti-business, and I do not think that it should be passed in the United States. This bill limits my options as a consumer to modify hardware that I have purchased. Once I make a purchase, the company who made that device no longer owns it, and neither do the US government. I should have complete rights to modify my property as I see fit, weather to add functionality, or to aide in ease of use. This is also anti-business, as it limits the use of alternative operating systems, meaning that if they don't come on a computer, they will not be installed. Since many operating systems, such as Linux, very rarely come installed, they would lose a massive amount of business because of this bill. Linux, for example, would be nearly entirely limited to Android, essentially Granting Microsoft a monopoly over computer operating 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: Krystal

Last Name: Cilch-Hannis

Mailing Address: 3004 Ferris Drive

City: Navarre

Country: United States

State or Province: FL

ZIP/Postal Code: 32566

Email Address: kcilch@yahoo.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, here are some points to consider:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and 5. 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, here are some points to consider:

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and 5. 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: Jordan

Last Name: Goldstein

Mailing Address: 143 Albany St

City: Cambridge

Country: United States

State or Province: MA

ZIP/Postal Code: 02139

Email Address: null

Organization Name: null

Comment: I would like to petition the FCC to keep wireless-enabled electronic devices, such as Wifi-enabled computers and smartphones, open for free and unfettered modification by their users. Any restriction in the ability of users to modify their wireless devices would lead to the following negative consequences. First, research in advanced wireless networking technology and protocols obviously requires users to install their own firmware and drivers on wireless devices. Preventing them from doing so would present a serious hamper on innovation which could otherwise lead to faster and more reliable wireless technologies. Second, many wireless technology-related services such as secure Wifi and retail Wifi rely on the ability of users to install wireless software consistent with the requirements of the service provider. Preventing users from installing their own wireless software would thus wipe out billions of dollars of commerce overnight. Finally, there are occasionally serious bugs or security holes in wireless software provided by the manufacturer, and manufacturers are occasionally slow or negligent to fix these. Usually users experiencing such issues will install a 3rd-party fix or software from the wireless chip manufacturer (as opposed to the computer or smartphone manufacturer), as I have done myself on many occasions when the default software has reliability issues. If users cannot modify their own wireless software, many will have to suffer from less than ideal (or even security-sacrificing!) wireless connectivity for longer than otherwise.

All in all, this is an issue which is very important to me and I encourage the FCC to leave wireless devices open for free modification by users.

I would like to petition the FCC to keep wireless-enabled electronic devices, such as Wifi-enabled computers and smartphones, open for free and unfettered modification by their users. Any restriction in the ability of users to modify their wireless devices would lead to the following negative consequences. First, research in advanced wireless networking technology and protocols obviously requires users to install their own firmware and drivers on wireless devices. Preventing them from doing so would present a serious hamper on innovation which could otherwise lead to faster and more reliable wireless technologies. Second, many wireless technology-related services such as secure Wifi and retail Wifi rely on the ability of users to install wireless software consistent with the requirements of the service provider. Preventing users from installing their own wireless software would thus wipe out billions of dollars of commerce overnight. Finally, there are occasionally serious bugs or security holes in wireless software provided by the manufacturer, and manufacturers are occasionally slow or negligent to fix these. Usually users experiencing such issues will install a 3rd-party fix or software from the wireless chip manufacturer (as opposed to the computer or smartphone manufacturer), as I have done myself on many occasions when the default software has reliability issues. If users cannot modify their own wireless software, many will have to suffer from less than ideal (or even security-sacrificing!) wireless connectivity for longer than otherwise.

All in all, this is an issue which is very important to me and I encourage the FCC to leave wireless devices open for free

modification by users.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: DeGenova

Mailing Address: 9224 Struthers Rd

City: New Middletown

Country: United States

State or Province: OH

ZIP/Postal Code: 44442

Email Address: mdege@sbcglobal.net

Organization Name:

Comment: While I understand the want for further security for end users, government uses (such as emergency services) and various other parties, this proposed regulation will not have the desired effect. As various methods of locking down devices has shown (take special note of the smartphone world) that such moves are ultimately ineffective. Modding communities are alive and well even in the closed source and protected world of Apple. As such, I believe that this regulation will be "worthless" in that it will not solve the problem of people modifying firmware in order to do harm (or for any other reason) and will only limit the freedoms of those who modify their firmware for various other reasons (most, if not all, do not create more "harm").

Here's a few reasons on why modifying firmware should be allowed:

- 1) Increased security. Commonly, there are many security flaws in the stock firmware that simply never get patched by the manufacturer.
- 2) Extra features. Security features, VPN support, complex device routing, firewalls, VLANs, and many more.
- 3) Keeping ISPs honest. Being that many ISP's now provide a modem/router for use with their services, I wouldn't surprise me that ISPs might attempt to get around net neutrality by having the stock firmware prioritize different services, arguing that they are not effecting the internet connection, but rather the device itself.
- 4) Development. ASUSWRT is the stock firmware on ASUS routers. It is open source and based upon DD-WRT, a "alternative" firmware that this regulation seeks to ban. From there, someone has taken the source code of ASUSWRT and created ASUSWRT-Merlin, which is built upon the stock firmware with extra features. Currently, he enjoys a good relationship with the Asus developers as they will take some of his features and backport it to the stock firmware. Without free modification of open-source firmware, non of this would have been possible, and in fact, would have halted the development of ASUSWRT which is in my opinion, the best of the consumer-grade router's firmware available in both security and features.

To give a personal example, I currently run ASUSWRT-Merlin on my router. This is not because I seek to cause harm to neighbors, as my router runs in the same manner as it would if I was running the stock firmware, with one exception-access. ASUSWRT-Merlin allows SSH access to the router from a remote source, and in a secure manner, both of which ASUSWRT does not currently allow. From a wireless standpoint, It is the exact same as if I was running the stock firmware.

Please, recognize that this regulation will not solve any issues and only serve to limit the freedoms, development, and security of Americans.

While I understand the want for further security for end users, government uses (such as emergency services) and various other parties, this proposed regulation will not have the desired effect. As various methods of locking down

devices has shown (take special note of the smartphone world) that such moves are ultimately ineffective. Modding communities are alive and well even in the closed source and protected world of Apple. As such, I believe that this regulation will be "worthless" in that it will not solve the problem of people modifying firmware in order to do harm (or for any other reason) and will only limit the freedoms of those who modify their firmware for various other reasons (most, if not all, do not create more "harm").

Here's a few reasons on why modifying firmware should be allowed:

- 1) Increased security. Commonly, there are many security flaws in the stock firmware that simply never get patched by the manufacturer.
- 2) Extra features. Security features, VPN support, complex device routing, firewalls, VLANs, and many more.
- 3) Keeping ISPs honest. Being that many ISP's now provide a modem/router for use with their services, I wouldn't surprise me that ISPs might attempt to get around net neutrality by having the stock firmware prioritize different services, arguing that they are not effecting the internet connection, but rather the device itself.
- 4) Development. ASUSWRT is the stock firmware on ASUS routers. It is open source and based upon DD-WRT, a "alternative" firmware that this regulation seeks to ban. From there, someone has taken the source code of ASUSWRT and created ASUSWRT-Merlin, which is built upon the stock firmware with extra features. Currently, he enjoys a good relationship with the Asus developers as they will take some of his features and backport it to the stock firmware. Without free modification of open-source firmware, non of this would have been possible, and in fact, would have halted the development of ASUSWRT which is in my opinion, the best of the consumer-grade router's firmware available in both security and features.

To give a personal example, I currently run ASUSWRT-Merlin on my router. This is not because I seek to cause harm to neighbors, as my router runs in the same manner as it would if I was running the stock firmware, with one exception-access. ASUSWRT-Merlin allows SSH access to the router from a remote source, and in a secure manner, both of which ASUSWRT does not currently allow. From a wireless standpoint, It is the exact same as if I was running the stock firmware.

Please, recognize that this regulation will not solve any issues and only serve to limit the freedoms, development, and security of Americans.

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: Dave

Last Name: F

Mailing Address: 420 Blaze it street

City: coolville

Country: United States

State or Province: AL

ZIP/Postal Code: 66432

Email Address: master449alt2@yahoo.com

Organization Name: TE

Comment: Please don't add these regulations to routers

Please don't add these regulations to routers

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: Brock

Last Name: Mitchell

Mailing Address: 518 W Kansas St

City: Liberty

Country: United States

State or Province: MO

ZIP/Postal Code: 64068

Email Address:

Organization Name:

Comment: This restricts small business, hobbyist, users with privacy concerns, and a free and open market. This goes against the very principle this same council set in motion with the Title II protections on broadband communications. This proposed rule sets us back toward protecting free and open platforms that we as users operate on. Do not enact this proposed rule.

This restricts small business, hobbyist, users with privacy concerns, and a free and open market. This goes against the very principle this same council set in motion with the Title II protections on broadband communications. This proposed rule sets us back toward protecting free and open platforms that we as users operate on. Do not enact 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: Jacob

Last Name: Dyke

Mailing Address: 20903 Hamlet Ridge Lane

City: Katy

Country: United States

State or Province: TX

ZIP/Postal Code: 77449

Email Address:

Organization Name:

Comment: 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. 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.

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. 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: Jeffrey

Last Name: Ugai

Mailing Address: 455 Eddy St

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94109

Email Address: jeff@ugai.us

Organization Name:

Comment: Restricting the ability of end users to install custom firmware/OS on their wireless devices reduces the value and utility of these devices, presents a significant threat to innovation, and reduces competitiveness in the marketplace. The ability to change, tweak, and ultimately improve electronics has been a crucial catalyst to technological development. Rather than expand security concerns, an open platform benefits from a larger network from which to identify and address vulnerabilities. For these reasons, I strongly encourage you to reject any proposal requiring manufacturers to restrict modification of devices.

Restricting the ability of end users to install custom firmware/OS on their wireless devices reduces the value and utility of these devices, presents a significant threat to innovation, and reduces competitiveness in the marketplace. The ability to change, tweak, and ultimately improve electronics has been a crucial catalyst to technological development. Rather than expand security concerns, an open platform benefits from a larger network from which to identify and address vulnerabilities. For these reasons, I strongly encourage you to reject any proposal requiring manufacturers to restrict modification of 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: Evan

Last Name: Koser

Mailing Address: 2353 Sherbrook Street

City: Pittsburgh

Country: United States

State or Province: PA

ZIP/Postal Code: 15217

Email Address:

Organization Name:

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

The wifi mesh market is still fledgling. I urge the FCC to consider waiting a few more years until the market has had a chance to lay its roots and figure out what works and what does not.

I respectfully ask the FCC not to implement rules that will take away the ability of users to install the software of their choosing on their 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.

The wifi mesh market is still fledgling. I urge the FCC to consider waiting a few more years until the market has had a chance to lay its roots and figure out what works and what does not.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Conrad

Last Name: Wilson

Mailing Address: 119 whispering oaks ln

City: swansea

Country: United States

State or Province: SC

ZIP/Postal Code: 29160

Email Address:

Organization Name:

Comment: Please do not take away the freedom to pick the OS a computer uses.

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

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

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

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

This could potentially allow hackers to use security flaws that won't be fixable, since this proposal will ban it.

Please do not take away the freedom to pick the OS a computer uses.

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

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

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

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

This could potentially allow hackers to use security flaws that won't be fixable, since this proposal will ban it.

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: Jeffrey

Last Name: Ugai

Mailing Address: 455 Eddy St

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94109

Email Address: jeff@ugai.us

Organization Name:

Comment: Restricting the ability of end users to install custom firmware/OS on their wireless devices reduces the value and utility of these devices, presents a significant threat to innovation, and reduces competitiveness in the marketplace. The ability to change, tweak, and ultimately improve electronics has been a crucial catalyst to technological development. Rather than expand security concerns, an open platform benefits from a larger network from which to identify and address vulnerabilities. For these reasons, I strongly encourage you to reject any proposal requiring manufacturers to restrict modification of devices.

Restricting the ability of end users to install custom firmware/OS on their wireless devices reduces the value and utility of these devices, presents a significant threat to innovation, and reduces competitiveness in the marketplace. The ability to change, tweak, and ultimately improve electronics has been a crucial catalyst to technological development. Rather than expand security concerns, an open platform benefits from a larger network from which to identify and address vulnerabilities. For these reasons, I strongly encourage you to reject any proposal requiring manufacturers to restrict modification of 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: Matthew

Last Name: King

Mailing Address: 4015 152nd St

City: Urbandale

Country: United States

State or Province: IA

ZIP/Postal Code: 50323

Email Address: kingdom529@gmail.com

Organization Name:

Comment: Technological innovation, understanding, and leadership are concepts that need to be fostered as much as possible, rather than being suppressed. The United States should be the driving force and can lead by the example of keeping these technologies an open platform. It would be a poor precedent for us to set, where we can no longer challenge ourselves through technological innovation, but that we must feel that we should suppress it through regulations that favor lazy government. We must continue to allow radio based devices the ability to be updated with custom and home developed firmware. We must continue to allow any PC to be installed with an OS that can have a custom kernel installed. these are essential parts of our innovative and discovery process.

Technological innovation, understanding, and leadership are concepts that need to be fostered as much as possible, rather than being suppressed. The United States should be the driving force and can lead by the example of keeping these technologies an open platform. It would be a poor precedent for us to set, where we can no longer challenge ourselves through technological innovation, but that we must feel that we should suppress it through regulations that favor lazy government. We must continue to allow radio based devices the ability to be updated with custom and home developed firmware. We must continue to allow any PC to be installed with an OS that can have a custom kernel installed. these are essential parts of our innovative and discovery process.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Hardcastle

Mailing Address: 8600 McDonogh Road

City: Owings Mills

Country: United States

State or Province: MD

ZIP/Postal Code: 21117

Email Address: jwhardcastle@jwhardcastle.com

Organization Name:

Comment: 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.

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nathan

Last Name: Vaughn

Mailing Address: 1019 Canyon View RD

City: Dripping Springs

Country: United States

State or Province: TX

ZIP/Postal Code: 78620

Email Address:

Organization Name:

Comment: Dear FCC,

Please don't prevent users from installing software of their choosing onto the computing devices they own. Operating systems like Linux and BSD are extremely powerful tools and amazing amounts of work all done by people free of charge. They have their place too such as for people who have really old and slow computers for whom Windows will not run acceptably. Or for those who just like to tinker or customize things. But simply not allowing people to customize their devices makes no sense. It's like you bought a new car, but the government tells you you are not allowed to customize it any. That would annoy a LOT of car fans. It's the same for those who are pro-user and like to tinker with technology. I hope you reconsider your position.

Dear FCC,

Please don't prevent users from installing software of their choosing onto the computing devices they own. Operating systems like Linux and BSD are extremely powerful tools and amazing amounts of work all done by people free of charge. They have their place too such as for people who have really old and slow computers for whom Windows will not run acceptably. Or for those who just like to tinker or customize things. But simply not allowing people to customize their devices makes no sense. It's like you bought a new car, but the government tells you you are not allowed to customize it any. That would annoy a LOT of car fans. It's the same for those who are pro-user and like to tinker with technology. I hope you reconsider your position.

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: Loren

Last Name: Libolt

Mailing Address: 1461 Stewart St

City: Oceanside

Country: United States

State or Province: CA

ZIP/Postal Code: 92054

Email Address:

Organization Name:

Comment: 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.

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: Aaron

Last Name: Krajewski

Mailing Address: 4404 Rue De Bullion

City: Montreal

Country: Canada

State or Province: Quebec

ZIP/Postal Code: h2w2g1

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. I think the choice here is obvious, an lightly regulated wireless realm has lead to innovation, commerce and improved safety. Please do not over-regulate.

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. I think the choice here is obvious, an lightly regulated wireless realm has lead to innovation, commerce and improved safety. Please do not over-regulate.