

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: Karl

Last Name: Andersson

Mailing Address: Lekarydsvgen 11

City: Alvesta

Country: Sweden

State or Province: Smland

ZIP/Postal Code: 34234

Email Address:

Organization Name:

Comment: Greetings, I would like to clarify I am not an US citizen, but I do know that this decision will affect not only the US but also where I am from and over the whole world.

I do not know the fine details of the propositional you are making, however I've gained that there are talks about restricting the the right to "flash" a device (specifically routers) with your own firmware that is not provided by the Corporation.

I can understand if this is from an lobby request or for security concerns, the problem is that first of all if it's is that it's purposed that all router's firmware be restricted, it would greatly impact the freedom over your own device and also on the security threat due to the fact that lots of people who buy routers usually flash them because they know the corporation will sooner or later abandon that product and it's code base, but also out of the need for total control and information with the device, since this in turn gives them the benefit to enhance and control the privacy issues that is present in the software, the hidden and locked away performance the device might be having, the modifications needed to alter the device to run on superior software than what the corporation and the list goes on and on.

I would instead purpose that you create a standard which every company selling routers must follow:

- * Provide a way to flash the device only if the user allows it
- * Make sure that the default configuration prohibits flashing the device, but with the user's consent and choice should be allowed to flash it as necessary.

Greetings, I would like to clarify I am not an US citizen, but I do know that this decision will affect not only the US but also where I am from and over the whole world.

I do not know the fine details of the propositional you are making, however I've gained that there are talks about restricting the the right to "flash" a device (specifically routers) with your own firmware that is not provided by the Corporation.

I can understand if this is from an lobby request or for security concerns, the problem is that first of all if it's is that it's purposed that all router's firmware be restricted, it would greatly impact the freedom over your own device and also on the security threat due to the fact that lots of people who buy routers usually flash them because they know the corporation will sooner or later abandon that product and it's code base, but also out of the need for total control and information with the device, since this in turn gives them the benefit to enhance and control the privacy issues that is

present in the software, the hidden and locked away performance the device might be having, the modifications needed to alter the device to run on superior software than what the corporation and the list goes on and on.

I would instead propose that you create a standard which every company selling routers must follow:

- * Provide a way to flash the device only if the user allows it
- * Make sure that the default configuration prohibits flashing the device, but with the user's consent and choice should be allowed to flash it as necessary.

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: Gibson

Mailing Address: 1036 Hemlock Lane

City: Enola

Country: United States

State or Province: PA

ZIP/Postal Code: 17025

Email Address: jonathangibson02@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Sean

Last Name: Forbes

Mailing Address: 3917 block drive #2299

City: Irving

Country: United States

State or Province: TX

ZIP/Postal Code: 75038

Email Address: forbes.seanr@gmail.com

Organization Name:

Comment: There does not currently exist an adequately elaborated reason as to why the Property OWNER or a technology or communications device should not be able to modify the device as they see fit. There are no current restrictions on the modification of computer and software outside of copyright claims and this is how it needs to stay. I don't much care if the software or firmware that I choose to use on my equipment is different from what the manufacturer wanted. It's my property and I can and shall use my property as I see fit. If this rule is allowed to move forward this would become a serious undermining of the ability of the United States government will have a chilling effect on all of the innovative technology development that's been driving our economy for the last 20 years. If you want the United States of America to remain a relevant and leading competitor on the world stage of technology, the FCC should not be involving itself in property rights issues outside of where someone's property may effect other types of communication. Disallowing me to set up custom firmware for my router or customizing the software of my computer IS NOT SOMETHING THE COMMISSION SHOULD BE REGULATING. Stop punishing advanced users with overt burdens such as asking a large multi-national corporation for permission to modify a device that we already own.

There does not currently exist an adequately elaborated reason as to why the Property OWNER or a technology or communications device should not be able to modify the device as they see fit. There are no current restrictions on the modification of computer and software outside of copyright claims and this is how it needs to stay. I don't much care if the software or firmware that I choose to use on my equipment is different from what the manufacturer wanted. It's my property and I can and shall use my property as I see fit. If this rule is allowed to move forward this would become a serious undermining of the ability of the United States government will have a chilling effect on all of the innovative technology development that's been driving our economy for the last 20 years. If you want the United States of America to remain a relevant and leading competitor on the world stage of technology, the FCC should not be involving itself in property rights issues outside of where someone's property may effect other types of communication. Disallowing me to set up custom firmware for my router or customizing the software of my computer IS NOT SOMETHING THE COMMISSION SHOULD BE REGULATING. Stop punishing advanced users with overt burdens such as asking a large multi-national corporation for permission to modify a device that we already own.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Zack

Last Name: Sonneborn

Mailing Address: 6922 Covington Stone Ave

City: Apollo Beach

Country: United States

State or Province: FL

ZIP/Postal Code: 33572

Email Address: zacksonneborn@msn.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.(*)

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Contreras

Mailing Address: 107 S Mary Ave APT 142

City: Sunnyvale

Country: United States

State or Province: CA

ZIP/Postal Code: 94086-5824

Email Address: robertcontreras@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Timothy J.

Last Name: Wiley

Mailing Address: 2077 Don Juan Ave

City: Eugene

Country: United States

State or Province: OR

ZIP/Postal Code: 97408

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Wesley

Last Name: Kirkland

Mailing Address: 8434 Wade Crest Lane

City: Powell

Country: United States

State or Province: TN

ZIP/Postal Code: 37849

Email Address: wesley@wesleyk.me

Organization Name:

Comment: Please do not pass this as it will inhibit growth and drag down our technological lead and lock down devices in such a way that would make them unusable and unsecure to the average consumer.

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.

Thanks

Please do not pass this as it will inhibit growth and drag down our technological lead and lock down devices in such a way that would make them unusable and unsecure to the average consumer.

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.

Thanks

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: Jose

Last Name: De La Garza

Mailing Address: 1240 E 1ST ST

City: MISSION

Country: United States

State or Province: TX

ZIP/Postal Code: 78572

Email Address: solidemptiness@gmail.com

Organization Name:

Comment: I believe that the proposed rules have been established in error and should not come to pass. I choose to employ a standard, eloquent template to convey my point of view due to time. Below is said template. Thank you.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

I believe that the proposed rules have been established in error and should not come to pass. I choose to employ a standard, eloquent template to convey my point of view due to time. Below is said template. Thank you.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Archie

Last Name: Alegre-Rigsby

Mailing Address: 228 w 25th st apt 1FE

City: NEW YORK

Country: United States

State or Province: NY

ZIP/Postal Code: 10001

Email Address: balanced123@gmail.com

Organization Name:

Comment: If I buy a device as a consumer, I should have the right to give it whatever instructions I want.

As long as it does not infringe on the rights of others.

Software (firmware, custom developed OSes, etc) is just me telling the hardware I purchase to do something.

If I buy a device as a consumer, I should have the right to give it whatever instructions I want.

As long as it does not infringe on the rights of others.

Software (firmware, custom developed OSes, etc) is just me telling the hardware I purchase to do 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: Timothy

Last Name: McCarty

Mailing Address: 1104 SHADETREE LANE

City: ALLEN

Country: United States

State or Province: TX

ZIP/Postal Code: 75013

Email Address: FTC-Comment@mccartyshome.org

Organization Name:

Comment: Blocking the right or ability of consumers to modify hardware, firmware or software on devices that they own is wrong on every conceivable level. I run a customized firmware on several of my own devices, and I always will. It should be noted that VERY often these third party firmwares [sic] are more current and more secure than the crap that the manufacturer provides. Especially where the vendor has chosen to provide the devices with a non-unique 'standard' root or admin password.

Blocking the right or ability of consumers to modify hardware, firmware or software on devices that they own is wrong on every conceivable level. I run a customized firmware on several of my own devices, and I always will. It should be noted that VERY often these third party firmwares [sic] are more current and more secure than the crap that the manufacturer provides. Especially where the vendor has chosen to provide the devices with a non-unique 'standard' root or admin password.

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: Chad

Last Name: Furman

Mailing Address: 80 Damon Rd, Apt 4206

City: Northampton

Country: United States

State or Province: MA

ZIP/Postal Code: 01060

Email Address: chad@chadfurman.com

Organization Name: Chad Furman, Inc.

Comment: As a software developer participating on the international market, a regulation forcing me to use inferior software (i.e. Windows, Mac) will directly limit my ability to perform and remain competitive.

In general, freedom should always be responded to with more freedom.

"If guns are illegal, only criminals will have guns"

As a software developer participating on the international market, a regulation forcing me to use inferior software (i.e. Windows, Mac) will directly limit my ability to perform and remain competitive.

In general, freedom should always be responded to with more freedom.

"If guns are illegal, only criminals will have guns"

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Logan

Last Name: Schuster

Mailing Address: 3171 E 107th Ct

City: Northglenn

Country: United States

State or Province: CO

ZIP/Postal Code: 80233

Email Address:

Organization Name: VectorLit Games Limited

Comment: Please do not take steps to prevent users from altering their own devices with custom code. This is a common and often necessary practice to resolve technical issues and bugs when hardware manufacturers fail to solve the problem themselves. For instance, an estimated 90% of Android devices are currently vulnerable to the stagefright bug with no updates in sight. This proposal would put all of those devices, and all of those Americans, into a situation where they are completely unable to resolve the problem.

In addition, it is essential that Americans should be able to innovate and create new code for many devices. This customization is the birthplace of many American engineers and programmers' skillsets. Taking away the legality of this only hinders American STEM growth while at the same time accomplishing literally nothing to stop "the bad guys", who I can only assume are the target for this proposal.

Please do not take steps to prevent users from altering their own devices with custom code. This is a common and often necessary practice to resolve technical issues and bugs when hardware manufacturers fail to solve the problem themselves. For instance, an estimated 90% of Android devices are currently vulnerable to the stagefright bug with no updates in sight. This proposal would put all of those devices, and all of those Americans, into a situation where they are completely unable to resolve the problem.

In addition, it is essential that Americans should be able to innovate and create new code for many devices. This customization is the birthplace of many American engineers and programmers' skillsets. Taking away the legality of this only hinders American STEM growth while at the same time accomplishing literally nothing to stop "the bad guys", who I can only assume are the target for 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: Miles

Last Name: Gervase

Mailing Address: 720 parkside Ave.

City: buffalo

Country: United States

State or Province: NY

ZIP/Postal Code: 14216

Email Address: Milesgervase123@yahoo.com

Organization Name: null

Comment: Dear FCC, 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 or the NSA chooses to not do so. 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 that they have purchased. These new rules will make it extremely difficult if not illegal, to make an open source baseband for cell phones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems. Thank you for reading this and I hope you consider the points I have made, have a nice rest of the day.

Dear FCC, 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 or the NSA chooses to not do so. 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 that they have purchased. These new rules will make it extremely difficult if not illegal, to make an open source baseband for cell phones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems. Thank you for reading this and I hope you consider the points I have made, have a nice rest of the day.

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: Nabih

Last Name: Iqal

Mailing Address: 218 Yellowhammer Cir

City: Alabaster

Country: United States

State or Province: AL

ZIP/Postal Code: 35007

Email Address: nabihqal@gmail.com

Organization Name:

Comment: The American public should be allowed to install software of their own choosing on their devices. This encourages creativity, education, and makes us a culture of inventors and innovators. A free society is free to modify technology. Locking down devices takes away our freedom to research and even fix potential problems with technology

America was once a country that valued innovators and tinkerers. Our great technologies grew out of people's garages and workshops, put together on shoe-string budgets. If people have no ability to modify, improve upon, and understand their technology, we will only foster a culture of consumers. A ask you, how can a culture of only consumers bring forth any more great ideas and amazing inventions? Lets bring back American ingenuity. Lets make this country a great place for inventors, thinkers, and makers.

Please consider these 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.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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 American public should be allowed to install software of their own choosing on their devices. This encourages creativity, education, and makes us a culture of inventors and innovators. A free society is free to modify technology. Locking down devices takes away our freedom to research and even fix potential problems with technology

America was once a country that valued innovators and tinkerers. Our great technologies grew out of people's garages and workshops, put together on shoe-string budgets. If people have no ability to modify, improve upon, and understand their technology, we will only foster a culture of consumers. A ask you, how can a culture of only consumers bring forth any more great ideas and amazing inventions? Lets bring back American ingenuity. Lets make this country a great place for inventors, thinkers, and makers.

Please consider these 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.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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: Andy

Last Name: Poling

Mailing Address: 1S527 Chase Ave

City: Lombard

Country: United States

State or Province: IL

ZIP/Postal Code: 60148

Email Address:

Organization Name:

Comment: Please don't take away from us the important ability to install the software we choose on our computing devices. Radios are integrated into a wide variety of devices, ranging from WiFi access points and router to smartphones to laptop computers, that merge software computing ability with radio(s) for data and communications.

It is important that we, the owners of these computing devices retain the ability to decide what software we run on our devices. There are many many software changes that could be made to such a hybrid device that would have no impact at all on the connected radio(s) which almost always run separate firmware from the rest of the device.

In this fast-paced modern world, the market is littered with such devices that have inferior or out-of-date software installed, with security vulnerabilities and defects. We need the ability to address these shortcomings if we desire to.

Additionally the continued advance of technology using such hybrid devices is an important benefit to the general citizenry, and should out-weigh concerns about radio firmware modification, which surely is a lesser concern.

Please don't take away from us the important ability to install the software we choose on our computing devices. Radios are integrated into a wide variety of devices, ranging from WiFi access points and router to smartphones to laptop computers, that merge software computing ability with radio(s) for data and communications.

It is important that we, the owners of these computing devices retain the ability to decide what software we run on our devices. There are many many software changes that could be made to such a hybrid device that would have no impact at all on the connected radio(s) which almost always run separate firmware from the rest of the device.

In this fast-paced modern world, the market is littered with such devices that have inferior or out-of-date software installed, with security vulnerabilities and defects. We need the ability to address these shortcomings if we desire to.

Additionally the continued advance of technology using such hybrid devices is an important benefit to the general citizenry, and should out-weigh concerns about radio firmware modification, which surely is a lesser concern.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ben

Last Name: Whittle

Mailing Address: 5615 Southern Oaks

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78261

Email Address: ben.whittle@rackspace.com

Organization Name:

Comment: Dear FCC,

I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Please consider the following 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 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.

Dear FCC,

I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Please consider the following 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.
- Not fixing security holes either feeds cyberthreats or increases electronic waste.
- 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: sashi

Last Name: ono

Mailing Address: 534 magna vista st

City: santa barbara

Country: United States

State or Province: CA

ZIP/Postal Code: 93110

Email Address: sashi@pureengineering.com

Organization Name: www.pureengineering.com

Comment: As an electrical engineer preventing firmware modifications would destroy an number of startups as well and reduce completion and reduce the usefulness of the technology. Less regulation is better for this wireless technology.

As an electrical engineer preventing firmware modifications would destroy an number of startups as well and reduce completion and reduce the usefulness of the technology. Less regulation is better for this wireless technology.

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: JD

Last Name: Ballard

Mailing Address: 121 East Victory Road

City: Meridian

Country: United States

State or Province: ID

ZIP/Postal Code: 83642

Email Address:

Organization Name:

Comment: This is absurd, and a sure way to kill innovation in a part of the technological sector that directly influences our ability to communicate.

Fuck off with opinionated and restricting regulations, FCC.

This is absurd, and a sure way to kill innovation in a part of the technological sector that directly influences our ability to communicate.

Fuck off with opinionated and restricting regulations, FCC.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: scott

Last Name: eustis

Mailing Address: 2317 ursulines

City: new orleans

Country: United States

State or Province: LA

ZIP/Postal Code: 70119

Email Address: scotteustis@gmail.com

Organization Name: public lab

Comment: dear FCC,

Please don't take the freedom of the internet away. Users should be able to install the software of their choosing on their computing devices. Where once, the internet allowed americans freedom to create and distribute important speech, it has been turning more and more into a massive surveillance system, merely for corporate benefit.

The proposed rule is overly broad, including items with an "electronic label." This would seem to disallow older computers to be re-purposed for community use by removing the factory OS (often no longer maintained by the corporation) with linux and open software. I have personally been a part of a few technology cooperatives that re-purposed old machines to give education and access to my fellows that may not have had access to online services. Therefore, this rule seems to contradict the president's initiative to expand internet access to the american people.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Ever since I was a child, the son of an electronics engineer, I have taken apart devices with an electronic label to play and re-solder them, to re mix and re-connect parts. My friends who still work on wireless systems in their professions also take things apart to learn and learn how to invent new devices. There are security problems to fix, and new capabilities to explore. Most of this process involves breaking apart machines built for one purpose and re-engineering them for something quite different.

After the Katrina disaster, portable wifi networks made with flashed routers, enabled us to file FEMA and job application paperwork from community centers. I don't think that would have been possible under this rule.

I now work with a group called Public Lab, a group whose central purpose is the re-imagining and re-purposing consumer grade electronics for low-cost environmental sensing. We are a proud part of the Maker community and have even been a part of maker events on the white house lawn. None of our devices can be standardized, they are experimental by design. They are designed to be "brown boxes" that users must hack to understand and complete. The purpose of this is to build a community of learners as well as users. We have many communities that learn electronics this way, like parts and crafts in Boston. and makers of NO.

Right now, i am working on a system of groundwater monitoring sensors that would communicate with a central server via wireless radio. It would be powered by re-purposed cel phone batteries. The city of new orleans is sinking because of poor groundwater management--we pump too much. the management is poor because monitoring groundwater levels to operate the pumps optimally is too expensive. I hope to be able to engineer a system of simple sensors that would be able to communicate the need to turn on our expensive pumps. I would do this essentially, by using electronics "waste",

devices that are thrown away because they are seen as useless. These devices had to pass FCC compliance to be made, and i fail to see why additional measures of conformity would be required.

Thanks for your review of comments.

Yours,

Scott Eustis
2317 Ursulines, 70119

dear FCC,

Please don't take the freedom of the internet away. Users should be able to install the software of their choosing on their computing devices. Where once, the internet allowed americans freedom to create and distribute important speech, it has been turning more and more into a massive surveillance system, merely for corporate benefit.

The proposed rule is overly broad, including items with an "electronic label." This would seem to disallow older computers to be re-purposed for community use by removing the factory OS (often no longer maintained by the corporation) with linux and open software. I have personally been a part of a few technology cooperatives that re-purposed old machines to give education and access to my fellows that may not have had access to online services. Therefore, this rule seems to contradict the president's initiative to expand internet access to the american people.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Ever since I was a child, the son of an electronics engineer, I have taken apart devices with an electronic label to play and re-solder them, to re mix and re-connect parts. My friends who still work on wireless systems in their professions also take things apart to learn and learn how to invent new devices. There are security problems to fix, and new capabilities to explore. Most of this process involves breaking apart machines built for one purpose and re-engineering them for something quite different.

After the Katrina disaster, portable wifi networks made with flashed routers, enabled us to file FEMA and job application paperwork from community centers. I don't think that would have been possible under this rule.

I now work with a group called Public Lab, a group whose central purpose is the re-imagining and re-purposing consumer grade electronics for low-cost environmental sensing. We are a proud part of the Maker community and have even been a part of maker events on the white house lawn. None of our devices can be standardized, they are experimental by design. They are designed to be "brown boxes" that users must hack to understand and complete. The purpose of this is to build a community of learners as well as users. We have many communities that learn electronics this way, like parts and crafts in Boston. and makers of NO.

Right now, i am working on a system of groundwater monitoring sensors that would communicate with a central server via wireless radio. It would be powered by re-purposed cel phone batteries. The city of new orleans is sinking because of poor groundwater management--we pump too much. the management is poor because monitoring groundwater levels to operate the pumps optimally is too expensive. I hope to be able to engineer a system of simple sensors that would be able to communicate the need to turn on our expensive pumps. I would do this essentially, by using electronics "waste", devices that are thrown away because they are seen as useless. These devices had to pass FCC compliance to be made, and i fail to see why additional measures of conformity would be required.

Thanks for your review of comments.

Yours,

Scott Eustis
2317 Ursulines, 70119

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: George

Last Name: Talbot

Mailing Address: 38 W Hamilton Pl

City: Jersey City

Country: United States

State or Province: NJ

ZIP/Postal Code: 07302

Email Address: georgettalbot@gmail.com

Organization Name:

Comment: Please reconsider this approach. Much device innovation comes from the ability of end users to make modifications to the software of their equipment. Because of the increasing integration of the functions of modern devices like cellphones and WiFi routers, keeping owners of their equipment from flashing their own firmware will have massive unintended effects beyond just the radio portions of the devices.

Pe

Please reconsider this approach. Much device innovation comes from the ability of end users to make modifications to the software of their equipment. Because of the increasing integration of the functions of modern devices like cellphones and WiFi routers, keeping owners of their equipment from flashing their own firmware will have massive unintended effects beyond just the radio portions of the devices.

Pe

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: Zac

Last Name: Tate

Mailing Address: 5230 laurel st

City: new orleans

Country: United States

State or Province: LA

ZIP/Postal Code: 70115

Email Address:

Organization Name:

Comment: Please do not implement unnecessary regulations on the freedom of the people to install software of their choice on their electronic devices. As has already been summarized, wireless networking research depends on the ability of researchers to investigate and modify their devices. The people 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. Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

Please do not implement unnecessary regulations on the freedom of the people to install software of their choice on their electronic devices. As has already been summarized, wireless networking research depends on the ability of researchers to investigate and modify their devices. The people 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. Not fixing security holes either feeds cyberthreats or increases electronic waste.

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: Mark

Last Name: Scopetta

Mailing Address: 337 Bedford Ave 3F

City: Brooklyn

Country: United States

State or Province: NY

ZIP/Postal Code: 11211

Email Address: mark.scopetta@gmail.com

Organization Name:

Comment: The ability to tinker with firmware is important to test new features and to learn. We shouldn't put hurdles in front of hobbyists. There's no better way to understand something than being able to take it apart and rebuild it. Please don't arbitrarily close something that might have unforeseen consequences in the future.

The ability to tinker with firmware is important to test new features and to learn. We shouldn't put hurdles in front of hobbyists. There's no better way to understand something than being able to take it apart and rebuild it. Please don't arbitrarily close something that might have unforeseen consequences in the future.

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: Weiss

Mailing Address: 74 Carol Dr.

City: Hopewell Junc.

Country: United States

State or Province: NY

ZIP/Postal Code: 12533

Email Address: jpwcandidate@yahoo.com

Organization Name: Mr.

Comment: The proposed regulation changes will add no new protections for the public, will interfere with the commerce of WiFi router manufacturers, and worse, will have detrimental effects on the public.

Please permit me to explain.

I have been flashing new firmware onto my home WiFi routers for well over a decade now. (I've used DD-WRT.)

I did so for the following reasons:

Improved Security

Adding network-monitoring capabilities

In the first case, I was able to add VPN-capability and, more importantly, MAC-address filtering. The latter allows you to deny access to any computer, smart-phone, or other WiFi device by its internal, hard-coded hardware-ID.

As for the network-monitoring features, I've used it to diagnose and find more than just problems in my home-network. I've actually found damaged DSL phone wires in my neighborhood through my network-monitoring. My phone-company actually know me now and appreciates my help.

All of this is because of my use of the custom DD-WRT firmware, something you are about to ban.

You should also note that these custom firmwares __already__ don't allow you to modify the radio-hardware. They can't, actually: the radio-hardware has been manufactured at the chip level to prevent this, as required by __existing__ __FCC__ __regulations.

(The only change you can make is to the transmission power, and (A) that is limited to current FCC regulations; (B) it can actually worsen connectivity to the router; (C) you can prematurely age or even burn out the router. All of the custom firmwares warn the user ... __loudly__ ... of these dangers.)

I repeat: Current FCC regulations already prevent modifications to the radio-hardware in WiFi routers, at the manufacturing-level. The proposed regulations therefore add no new benefit to the public.

I want to point out two final, more problematic, issues with this proposal.

WiFi Router manufacturers release new, improved firmwares with security fixes. The proposed regulation change would make it impossible to make these security changes. The major security bugs of last summer would have been impossible to fix under the proposed changes.

Why? Because you cannot ban custom firmwares without preventing ALL firmware changes. That's the only way, as any researcher into security will tell you.

All security measures can be circumvented. Any scheme designed to prevent flashing only certain kinds of firmware will inevitably fail. Therefore, the only way to block certain kinds of firmware is to block all firmware changes and etch the firmware permanently onto the chips.

My final point: Two WiFi router manufacturers, LinkSys and Netgear, sell WiFi routers that advertise the ability to flash a custom firmware as a feature. They provide this feature, however, only on the more expensive models. The proposed changes will, therefore, interfere with commerce, at no benefit to the public.

In summary: The proposed regulation changes will add no new protections for the public, will interfere with the commerce of WiFi router manufacturers, and worse, will have detrimental effects on the public.

The proposed regulation changes will add no new protections for the public, will interfere with the commerce of WiFi router manufacturers, and worse, will have detrimental effects on the public.

Please permit me to explain.

I have been flashing new firmware onto my home WiFi routers for well over a decade now. (I've used DD-WRT.)

I did so for the following reasons:

Improved Security

Adding network-monitoring capabilities

In the first case, I was able to add VPN-capability and, more importantly, MAC-address filtering. The latter allows you to deny access to any computer, smart-phone, or other WiFi device by its internal, hard-coded hardware-ID.

As for the network-monitoring features, I've used it to diagnose and find more than just problems in my home-network. I've actually found damaged DSL phone wires in my neighborhood through my network-monitoring. My phone-company actually know me now and appreciates my help.

All of this is because of my use of the custom DD-WRT firmware, something you are about to ban.

You should also note that these custom firmwares already don't allow you to modify the radio-hardware. They can't, actually: the radio-hardware has been manufactured at the chip level to prevent this, as required by existing FCC regulations.

(The only change you can make is to the transmission power, and (A) that is limited to current FCC regulations; (B) it

can actually worsen connectivity to the router; (C) you can prematurely age or even burn out the router. All of the custom firmwares warn the user ... __loudly__ ... of these dangers.)

I repeat: Current FCC regulations already prevent modifications to the radio-hardware in WiFi routers, at the manufacturing-level. The proposed regulations therefore add no new benefit to the public.

I want to point out two final, more problematic, issues with this proposal.

WiFi Router manufacturers release new, improved firmwares with security fixes. The proposed regulation change would make it impossible to make these security changes. The major security bugs of last summer would have been impossible to fix under the proposed changes.

Why? Because you __cannot__ ban custom firmwares without preventing ALL firmware changes. That's the only way, as any researcher into security will tell you.

All security measures can be circumvented. Any scheme designed to prevent flashing only certain kinds of firmware will inevitably fail. Therefore, the only way to block certain kinds of firmware is to block __all__ firmware changes and etch the firmware permanently onto the chips.

My final point: Two WiFi router manufacturers, LinkSys and Netgear, sell WiFi routers that advertise the ability to flash a custom firmware as a feature. They provide this feature, however, only on the more expensive models. The proposed changes will, therefore, interfere with commerce, at no benefit to the public.

In summary: The proposed regulation changes will add no new protections for the public, will interfere with the commerce of WiFi router manufacturers, and worse, will have detrimental effects on the public.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Austin

Last Name: Capps

Mailing Address: 4606 N Winchester Ave Unit 1A

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60640

Email Address: austincapps@fastmail.fm

Organization Name:

Comment: I am requesting that the FCC not adopt this rule or any other that would impact the ability of users to install the software of their choosing on their devices. Americans should have the ability to patch their own devices when security concerns arise regardless of the manufacturer's seal of approval. Users have a track record of fixing serious bugs in their computing devices. Hijacked routers have already been used in a variety of cyber-attacks, enforcing a regime which would discourage security research to actively fix these holes, as the proposed rule would do, is against the interests of the United States. In addition, the proposed rules would have a negative impact on free software with custom router firmware coming under fire in particular. Custom router firmware is used not only to harden equipment and conduct security research but is actively in use across the US in places where wifi hot spots are offered. The proposed rules would negatively effect commerce at these locations in addition to actively harming the cyber security infrastructure of the United States and should not be adopted.

I am requesting that the FCC not adopt this rule or any other that would impact the ability of users to install the software of their choosing on their devices. Americans should have the ability to patch their own devices when security concerns arise regardless of the manufacturer's seal of approval. Users have a track record of fixing serious bugs in their computing devices. Hijacked routers have already been used in a variety of cyber-attacks, enforcing a regime which would discourage security research to actively fix these holes, as the proposed rule would do, is against the interests of the United States. In addition, the proposed rules would have a negative impact on free software with custom router firmware coming under fire in particular. Custom router firmware is used not only to harden equipment and conduct security research but is actively in use across the US in places where wifi hot spots are offered. The proposed rules would negatively effect commerce at these locations in addition to actively harming the cyber security infrastructure of the United States and should not be adopted.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kyle

Last Name: Smith

Mailing Address: 631 Tower Ridge Ct.

City: Milford

Country: United States

State or Province: MI

ZIP/Postal Code: 48381

Email Address: clipless@gmail.com

Organization Name:

Comment: This would do great harm to opensource software. Please reconsider.

This would do great harm to opensource software. Please reconsider.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anthony

Last Name: Santaferra

Mailing Address: 129 Lockland Ave

City: Framingham

Country: United States

State or Province: MA

ZIP/Postal Code: 01701

Email Address: Santaferra@gmail.com

Organization Name: Drunkenmoba LLC

Comment: This proposal would limit my business ability to secure my connections against intrusion into network.

Ban for security reasons.

This proposal would limit my business ability to secure my connections against intrusion into network.

Ban for security reasons.

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: Denshaw

Mailing Address: 440 N. 38th Street

City: Philadelphia

Country: United States

State or Province: PA

ZIP/Postal Code: 19104-2303

Email Address:

Organization Name:

Comment: I would like to say that I STAND AGAINST the proposed legislation titled "Equipment Authorization and Electronic Labeling for Wireless Devices". Said legislation would create a litany of troublesome scenarios that would serve to limit the creativity of the American people, as well as introduce them and their devices to harm.

In terms of "limit[ing] the creativity of the American people", I am referring specifically to the legislation's effect on the open-source community (both software- and hardware-based). The proposed rule-making would bar modification of electronic devices and leave all innovation in the hands of the device manufacturers. Time and time again, the open-source community has proven to be an invaluable in furthering the technology sector in this country. When people are given the freedom (a principle upon which this country is supposed to stand) to make things better, amazing results follow. I appeal to your standing as a representative of the United States, and want to remind you that the people you represent wish to be free to do as they please.

Furthermore, this legislation, as mentioned above, would expose the American people and their devices to harm. Leaving all updates/modifications up to the manufacturers alone is a risky proposition. Manufacturers are notoriously slow-on-the-draw when it comes to rolling out security patches, and this puts any devices produced by said manufacturer at risk. If people in the community are aware of any security short-comings, they should be able to pursue fixes with the support of other well-versed individuals. In an age where everything that we do (our finances, our work, and our personal means of communication) exists within the framework of wireless communication, it is reprehensible to knowingly put people (and their private information) in a compromising position. Additionally, the inability to modify firmware would limit emergency operators on the HamNet (i.e. amateur radio operators who assist officials during crises), which is heavily relied on in the event of crashed cellphone networks.

I urge you to consider the far-reaching ramifications of the proposed legislation. I'm sure it was drafted with the best of intentions; however, I ultimately believe it would do more harm than good. Being able to tinker with devices has become a sincere passion of mine, and I would be devastated to know that my passion could be stifled with a single set of laws. I thank you for reading this comment, and hope that you'll elect to do the right thing.

I would like to say that I STAND AGAINST the proposed legislation titled "Equipment Authorization and Electronic Labeling for Wireless Devices". Said legislation would create a litany of troublesome scenarios that would serve to limit the creativity of the American people, as well as introduce them and their devices to harm.

In terms of "limit[ing] the creativity of the American people", I am referring specifically to the legislation's effect on the open-source community (both software- and hardware-based). The proposed rule-making would bar modification of electronic devices and leave all innovation in the hands of the device manufacturers. Time and time again, the open-

source community has proven to be an invaluable in furthering the technology sector in this country. When people are given the freedom (a principle upon which this country is supposed to stand) to make things better, amazing results follow. I appeal to your standing as a representative of the United States, and want to remind you that the people you represent wish to be free to do as they please.

Furthermore, this legislation, as mentioned above, would expose the American people and their devices to harm. Leaving all updates/modifications up to the manufacturers alone is a risky proposition. Manufacturers are notoriously slow-on-the-draw when it comes to rolling out security patches, and this puts any devices produced by said manufacturer at risk. If people in the community are aware of any security short-comings, they should be able to pursue fixes with the support of other well-versed individuals. In an age where everything that we do (our finances, our work, and our personal means of communication) exists within the framework of wireless communication, it is reprehensible to knowingly put people (and their private information) in a compromising position. Additionally, the inability to modify firmware would limit emergency operators on the HamNet (i.e. amateur radio operators who assist officials during crises), which is heavily relied on in the event of crashed cellphone networks.

I urge you to consider the far-reaching ramifications of the proposed legislation. I'm sure it was drafted with the best of intentions; however, I ultimately believe it would do more harm than good. Being able to tinker with devices has become a sincere passion of mine, and I would be devastated to know that my passion could be stifled with a single set of laws. I thank you for reading this comment, and hope that you'll elect to do the right thing.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Zatynski

Mailing Address: 1914 Summey Ave

City: Charlotte

Country: United States

State or Province: NC

ZIP/Postal Code: 28205

Email Address: zatynski@yahoo.com

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. If need be, regulate the power output and frequency range allowed with modification of wifi routers, but don't prohibit modifications entirely. This would have devastating effects and is unwanted by the tech community.

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.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

Thank you for your time and consideration. We all appreciate your efforts for net neutrality. Keep up the good work there. Thanks!

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. If need be, regulate the power output and frequency range allowed with modification of wifi routers, but don't prohibit modifications entirely. This would have devastating effects and is unwanted by the tech community.

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.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

Thank you for your time and consideration. We all appreciate your efforts for net neutrality. Keep up the good work there. Thanks!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Crumpler

Mailing Address: 2040 Phillips Mill Road

City: Forest Hill

Country: United States

State or Province: MD

ZIP/Postal Code: 21050

Email Address: Slimjim2234@gmail

Organization Name:

Comment: This is exactly how you hinder ingenuity. Please stop.

Instead of regressing, you should support the efforts of these developers who have created a community driven by progress.

It is clear the motives behind this act by the FCC is purely financial.

As such, I promise there is more money to be made in progressive efforts.

This is exactly how you hinder ingenuity. Please stop.

Instead of regressing, you should support the efforts of these developers who have created a community driven by progress.

It is clear the motives behind this act by the FCC is purely financial.

As such, I promise there is more money to be made in progressive efforts.

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: goff

Mailing Address: 2301 Ridge RD, PO Box 134

City: Pendelton

Country: United States

State or Province: KY

ZIP/Postal Code: 40055

Email Address: null

Organization Name: null

Comment: I would not like the FCC to regulate the software packaged along with radio modules. Software pertaining to a radio is not necessarily the only software that is on the device. However it will likely be contained in a single storage device that would be required to be locked. As such the FCC would be placing restriction on additional software also. My personal example would be that I own a Internet router that has all software placed on one chip, it had been updated with a 3rd party software to patch both security issues not pertaining to the radio and enable ipv6, a new standard that is required for another part that is also not the radio.

Thank you.

I would not like the FCC to regulate the software packaged along with radio modules. Software pertaining to a radio is not necessarily the only software that is on the device. However it will likely be contained in a single storage device that would be required to be locked. As such the FCC would be placing restriction on additional software also. My personal example would be that I own a Internet router that has all software placed on one chip, it had been updated with a 3rd party software to patch both security issues not pertaining to the radio and enable ipv6, a new standard that is required for another part that is also not the radio.

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: Jaren

Last Name: Havell

Mailing Address: 720 East Johnson Ave

City: Cheshire

Country: United States

State or Province: CT

ZIP/Postal Code: 06410

Email Address: jaw174@gmail.com

Organization Name:

Comment: restricting the ability to modify, customize, or otherwise replace the factory provided firmware of a wifi containing device will significantly reduce the usability of the equipment as well as limit the customers choice. Please modify this document to limit these sweeping and ambiguous regulations.

restricting the ability to modify, customize, or otherwise replace the factory provided firmware of a wifi containing device will significantly reduce the usability of the equipment as well as limit the customers choice. Please modify this document to limit these sweeping and ambiguous regulations.

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: Byron

Last Name: Borrer

Mailing Address: 20841 Harlequin Ln

City: Callaway

Country: United States

State or Province: MD

ZIP/Postal Code: 20620

Email Address: bborrer@gmail.com

Organization Name:

Comment: Limiting user modification of software/firmware of devices will surely crush the innovation of wireless communication. Many of the advances of mobile device/home router software features have come from the open source user community. I am an avid open source user and enjoy making changes to my devices firmware/software, extending capabilities and user functionality, while staying within FCC regulations. I would propose that in stead of forcing the manufacturer to limit modification of software, that manufacturers should be made to incorporate a hardware lockout of radio configuration. This could be as simple as a jumper inside of the device that locks the registers for the radio variables in SoC devices, or partitioning flash and encrypting and signing radio firmware separately. I believe the FCC may be unintentionally swinging a large bat at a small ball with these proposed changes.

Limiting user modification of software/firmware of devices will surely crush the innovation of wireless communication. Many of the advances of mobile device/home router software features have come from the open source user community. I am an avid open source user and enjoy making changes to my devices firmware/software, extending capabilities and user functionality, while staying within FCC regulations. I would propose that in stead of forcing the manufacturer to limit modification of software, that manufacturers should be made to incorporate a hardware lockout of radio configuration. This could be as simple as a jumper inside of the device that locks the registers for the radio variables in SoC devices, or partitioning flash and encrypting and signing radio firmware separately. I believe the FCC may be unintentionally swinging a large bat at a small ball with these proposed changes.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Sam

Last Name: Graham

Mailing Address: 5 E 2 N

City: Sugar City

Country: United States

State or Province: ID

ZIP/Postal Code: 83448

Email Address: samgraham@hotmail.com

Organization Name:

Comment: I believe that open source solutions should be allowed. Banning firmware modification is unnecessary.

I believe that open source solutions should be allowed. Banning firmware modification is unnecessary.

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: Angus

Last Name: Putnam

Mailing Address: 17 Hooper

City: Wiscasset

Country: United States

State or Province: ME

ZIP/Postal Code: 04578

Email Address:

Organization Name:

Comment: One of the rights that I believe all Americans have , and should have, is the right to modify their own devices. The NPRM would infringe this right completely. One of the things that keeps Wireless Network research going is the ability to modify those devices and to investigate them. Without that you would be setting back innovation by decades. We also need the ability to be able to fix our own systems when the manufacturer simply won't. Please do not pass NPRM, as it would do all harm and no good.

One of the rights that I believe all Americans have , and should have, is the right to modify their own devices. The NPRM would infringe this right completely. One of the things that keeps Wireless Network research going is the ability to modify those devices and to investigate them. Without that you would be setting back innovation by decades. We also need the ability to be able to fix our own systems when the manufacturer simply won't. Please do not pass NPRM, as it would do all harm and no good.

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: Behrens

Mailing Address: PO Box 8948

City: Emeryville

Country: United States

State or Province: CA

ZIP/Postal Code: 94662

Email Address: david.behrens@gmail.com

Organization Name:

Comment: Hello,

This law would hamper innovation, plain and simple. This is bad for the US and bad for business. This would prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes, which will hamper innovation.

Hello,

This law would hamper innovation, plain and simple. This is bad for the US and bad for business. This would prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes, which will hamper 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: Roger

Last Name: Wong

Mailing Address: 2404 Longview St Apt 104

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78705

Email Address: rogerawong@gmail.com

Organization Name:

Comment: The proposed rules are overly broad. The FCC has valid concerns about software-controlled radios hacked to cause RF interference, but the proposed language would suppress legitimate hobbyist and consumer modifications that do not cause RF interference.

An alternative to this overly-broad proposal would be a "mattress label" approach. "Under penalty of law, modifying this firmware of this device beyond FCC operating parameters is strictly prohibited."

The proposed rules are overly broad. The FCC has valid concerns about software-controlled radios hacked to cause RF interference, but the proposed language would suppress legitimate hobbyist and consumer modifications that do not cause RF interference.

An alternative to this overly-broad proposal would be a "mattress label" approach. "Under penalty of law, modifying this firmware of this device beyond FCC operating parameters is strictly prohibited."

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: Tim

Last Name: Soderstrom

Mailing Address: 3114 Crosby Cove

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78253

Email Address:

Organization Name:

Comment: I respectfully ask that you (the FCC) reconsider implementing rules which take away the ability of users to install the software of their choosing on their computing devices. This should be a universal tenant as secrecy, exclusivity, behemoth Corporations are not to the benefit of the consumer. Consider the benefits users being able to modify their own hardware:

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 (a problem known all too well with WiFi routers already)

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.

At the very least, consider allowing HAMs the ability to modify hardware as has been part of the HAM community since its inception. There at least the Public at large have a path with which to be able to meet the above goals and, in turn, demonstrating to the FCC their ability to do so responsibility.

For the Love of Radio and, importantly, the Love of Liberty, please reconsider your position in this matter.

I respectfully ask that you (the FCC) reconsider implementing rules which take away the ability of users to install the software of their choosing on their computing devices. This should be a universal tenant as secrecy, exclusivity, behemoth Corporations are not to the benefit of the consumer. Consider the benefits users being able to modify their own hardware:

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 (a problem known all too well with WiFi routers already)

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.

At the very least, consider allowing HAMs the ability to modify hardware as has been part of the HAM community since its inception. There at least the Public at large have a path with which to be able to meet the above goals and, in turn, demonstrating to the FCC their ability to do so responsibly.

For the Love of Radio and, importantly, the Love of Liberty, please reconsider your position in this matter.