

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Thomas

Last Name: Moore

Mailing Address: 2314 Capitol Way

City: Olympia

Country: United States

State or Province: WA

ZIP/Postal Code: 98501

Email Address: tmoore1984@gmail.com

Organization Name:

Comment: The notion of locking down new wireless access points (APs) to vendor firmware, just in order to keep unlicensed consumers from misusing the 5GHz bands, is ludicrous. Many people have already pointed out that vendors may not take care of dangerous security vulnerabilities in a timely fashion. Many large software firms have been notoriously lax about patching vulnerabilities, and nowhere is this more critical than in network infrastructure. Setting aside any arguments about who owns the devices in question, it is imperative that software updates are not tied to vendors for security purposes. This could affect more than just end-users: a serious vulnerability could allow nefarious agents to create botnets. Please do not tie the fate of the USA's network infrastructure to the diligence of sometimes lax or short-lived hardware vendors.

The notion of locking down new wireless access points (APs) to vendor firmware, just in order to keep unlicensed consumers from misusing the 5GHz bands, is ludicrous. Many people have already pointed out that vendors may not take care of dangerous security vulnerabilities in a timely fashion. Many large software firms have been notoriously lax about patching vulnerabilities, and nowhere is this more critical than in network infrastructure. Setting aside any arguments about who owns the devices in question, it is imperative that software updates are not tied to vendors for security purposes. This could affect more than just end-users: a serious vulnerability could allow nefarious agents to create botnets. Please do not tie the fate of the USA's network infrastructure to the diligence of sometimes lax or short-lived hardware vendors.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Herman

Mailing Address: 43 Eastern Ave

City: Beverly

Country: United States

State or Province: MA

ZIP/Postal Code: 01915

Email Address: mgherm@gmail.com

Organization Name: CIC Innovation Services

Comment: As an IT professional, any rule which restricted my ability to install a custom or alternative operating system on a device containing a wireless radio (wifi network card) would make my job impossible. I am responsible for a network that contains thousands of wireless devices on hundred of wireless access points, and I need to be able to install custom software to monitor and control the wireless network to ensure that my clients are able to successfully use the wireless infrastructure I have built. At times this means installing esoteric, customized or otherwise non-standard operating systems and software to expand my toolset. In addition, any rule that restricted the ability of consumers or professionals from installing custom software or operating systems on their wifi-enabled hardware would kill a large portion of the startup companies that are my main clients, who are designing the next generation of wireless technologies.

This proposal is dangerous and should not be adopted.

As an IT professional, any rule which restricted my ability to install a custom or alternative operating system on a device containing a wireless radio (wifi network card) would make my job impossible. I am responsible for a network that contains thousands of wireless devices on hundred of wireless access points, and I need to be able to install custom software to monitor and control the wireless network to ensure that my clients are able to successfully use the wireless infrastructure I have built. At times this means installing esoteric, customized or otherwise non-standard operating systems and software to expand my toolset. In addition, any rule that restricted the ability of consumers or professionals from installing custom software or operating systems on their wifi-enabled hardware would kill a large portion of the startup companies that are my main clients, who are designing the next generation of wireless technologies.

This proposal is dangerous 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: Stefan

Last Name: Falls

Mailing Address: PO Box 58404

City: Fairbanks

Country: United States

State or Province: AK

ZIP/Postal Code: 99711

Email Address: sfalls81@gmail.com

Organization Name:

Comment: BLUF: I have no faith in the government. In other words, you (the government), pretty much shouldn't touch anything technology related. Have you ever been on AKO?

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.

BLUF: I have no faith in the government. In other words, you (the government), pretty much shouldn't touch anything technology related. Have you ever been on AKO?

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

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

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

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



Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brandon

Last Name: Witzig

Mailing Address: 10 EVE CRT

City: Bradford

Country: Canada

State or Province: Ontario

ZIP/Postal Code: L3Z3H6

Email Address: Brandon.Witzig2@gmail.com

Organization Name: null

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

as a person who uses modified firmware on devices to fix software bugs, I would have a lot of useless hardware if this law were to go into effect. Therefore I respectfully wish for this regulation to not be approved.

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.

as a person who uses modified firmware on devices to fix software bugs, I would have a lot of useless hardware if this law were to go into effect. Therefore I respectfully wish for this regulation to not be approved.

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: Davos

Mailing Address: 721 S Cedarcrest Dr

City: Schaumburg

Country: United States

State or Province: IL

ZIP/Postal Code: 60193

Email Address: johndavos@hotmail.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: Nicholas

Last Name: Rishel

Mailing Address: 1789 W State Rd 234

City: Fortville

Country: United States

State or Province: IN

ZIP/Postal Code: 46040

Email Address:

Organization Name:

Comment: As a citizen who has used custom firmware to fix hardware security flaws never addressed by the manufacturer: I would request that the FCC does not implement these rules which hinder my ability to protect my home network.

As a citizen who has used custom firmware to fix hardware security flaws never addressed by the manufacturer: I would request that the FCC does not implement these rules which hinder my ability to protect my home network.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Keith

Last Name: Miller

Mailing Address: 3910 Chapel Forge Drive

City: Bowie

Country: United States

State or Province: MD

ZIP/Postal Code: 20715-1312

Email Address: ae3d@graykitty.net

Organization Name: Anne Arundel Radio Club

Comment: As along time licensed Amateur Radio operator with an interest in High Speed Multimedia MESH I fine your proposed rule confusing at best.

I know in my local club, we have a number of 'hams' who use modified routers to learn the skills needed to provide emergency Internet style communications via radio. I would think that regulating the modification of such equipment will essentially stop us from continuation with this endeavor.

Further I have been led to believe it will impact my ability to use non-Microsoft operating systems on many pieces of equipment, because that equipment can no longer be modified to work correctly with things like Linux. Again this stops a great deal of experimentation dead in its tracks. In short I can't see any reason for the federal government to further aid Microsoft in its domination of the home computer market.

Though I am sure it was not your intention to do so, your proposed legislation may turn out to cure one small problem, and create several larger ones. I hope you will consider these issues carefully before deciding on this matter.

As along time licensed Amateur Radio operator with an interest in High Speed Multimedia MESH I fine your proposed rule confusing at best.

I know in my local club, we have a number of 'hams' who use modified routers to learn the skills needed to provide emergency Internet style communications via radio. I would think that regulating the modification of such equipment will essentially stop us from continuation with this endeavor.

Further I have been led to believe it will impact my ability to use non-Microsoft operating systems on many pieces of equipment, because that equipment can no longer be modified to work correctly with things like Linux. Again this stops a great deal of experimentation dead in its tracks. In short I can't see any reason for the federal government to further aid Microsoft in its domination of the home computer market.

Though I am sure it was not your intention to do so, your proposed legislation may turn out to cure one small problem, and create several larger ones. I hope you will consider these issues carefully before deciding on this matter.

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: Rodney

Last Name: McGee

Mailing Address: 139 THE GRN

City: Newark

Country: United States

State or Province: DE

ZIP/Postal Code: 19711

Email Address: tmcgee@udel.edu

Organization Name: University of Delaware

Comment: Regarding proposed rules that would require device makers with Radio Frequency (RF) devices to cryptographically lock down the RF-controlling software on those devices.

As a University of Delaware researcher, I am against these proposed rules. Restricting the technology from being modified is a bad idea because it potentially limits innovation. An alternation is not inherently bad. Choice and freedom are a risk but the upside outweighs the risks. Do not require RF devices be locked down from installing custom software.

Regarding proposed rules that would require device makers with Radio Frequency (RF) devices to cryptographically lock down the RF-controlling software on those devices.

As a University of Delaware researcher, I am against these proposed rules. Restricting the technology from being modified is a bad idea because it potentially limits innovation. An alternation is not inherently bad. Choice and freedom are a risk but the upside outweighs the risks. Do not require RF devices be locked down from installing custom software.

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: Ron

Last Name: Ogle

Mailing Address: 13811 Riverwood Way

City: Carmel

Country: United States

State or Province: IN

ZIP/Postal Code: 46032

Email Address: ronaldo.ogle@gmail.com

Organization Name:

Comment: I am against the FCC requiring manufactures to implement methods to prevent end users from being able to change software in the products that they purchase. At the very least the FCC must differentiate the software regulating frequency modifications from the rest of the software. Therefore the restriction can only be made on that part of the software that strictly regulates frequencies.

I work in the computer security field. We need ways to help protect wireless infrastructure. Manufactures often do not allow security measures that we find prudent. With Open Source, I can modify wireless routers and access points to implement those appropriate and prudent security measures.

If the FCC implements this rule as currently written, you will in essence create security risks.

I am against the FCC requiring manufactures to implement methods to prevent end users from being able to change software in the products that they purchase. At the very least the FCC must differentiate the software regulating frequency modifications from the rest of the software. Therefore the restriction can only be made on that part of the software that strictly regulates frequencies.

I work in the computer security field. We need ways to help protect wireless infrastructure. Manufactures often do not allow security measures that we find prudent. With Open Source, I can modify wireless routers and access points to implement those appropriate and prudent security measures.

If the FCC implements this rule as currently written, you will in essence create security risks.

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: Fusia

Mailing Address: 1511 Howell Highlands

City: Stone Mountain

Country: United States

State or Province: GA

ZIP/Postal Code: 30087

Email Address:

Organization Name:

Comment: This proposal suggests taking away the ability to put open source software on routers because a few people intentionally modified their routers to operate outside of their valid parameters. There are safe guards and region locks inside of both OpenWRT and DD-WRT - a user would have to intentionally select a region/country other than the U.S. These options are available because (surprise!) this software is popular in regions other than the U.S.

This is like banning all dogs because a few dogs have been involved in dog fighting.

As a long-time (4+ years) user of open source software on my routers, this is a horrible idea. I have 4 access points in my house to provide 2.4ghz and 5ghz coverage. I need the open source software in order to configure them to actually work together and allow device roaming. Otherwise I would end up with 4 separate networks with no ability to roam between each access point. Additionally, I get advanced features like QoS and VPN support.

In summary: horrible idea. You already have a legal path to enforce the correct use of unlicensed spectrum.

This proposal suggests taking away the ability to put open source software on routers because a few people intentionally modified their routers to operate outside of their valid parameters. There are safe guards and region locks inside of both OpenWRT and DD-WRT - a user would have to intentionally select a region/country other than the U.S. These options are available because (surprise!) this software is popular in regions other than the U.S.

This is like banning all dogs because a few dogs have been involved in dog fighting.

As a long-time (4+ years) user of open source software on my routers, this is a horrible idea. I have 4 access points in my house to provide 2.4ghz and 5ghz coverage. I need the open source software in order to configure them to actually work together and allow device roaming. Otherwise I would end up with 4 separate networks with no ability to roam between each access point. Additionally, I get advanced features like QoS and VPN support.

In summary: horrible idea. You already have a legal path to enforce the correct use of unlicensed spectrum.

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: Mychaela

Last Name: Falconia

Mailing Address: PO Box 488

City: Oceanside

Country: United States

State or Province: CA

ZIP/Postal Code: 92049

Email Address:

Organization Name:

Comment: Please do not implement the proposed changes. Many end users critically depend on being able to replace flawed firmware from vendors with improved versions, and if this ability is taken away from them, they will no longer be able to live meaningful and productive lives. If the proposed regulations become law in USA, continued life in this country will become intolerable to us, and many of us will vote with our feet by moving to countries with less repressive laws. This development will accelerate the already ongoing exodus of high tech from USA to China and India and other places, and thereby accelerate the loss of American jobs and downturn of the economy.

Please do not implement the proposed changes. Many end users critically depend on being able to replace flawed firmware from vendors with improved versions, and if this ability is taken away from them, they will no longer be able to live meaningful and productive lives. If the proposed regulations become law in USA, continued life in this country will become intolerable to us, and many of us will vote with our feet by moving to countries with less repressive laws. This development will accelerate the already ongoing exodus of high tech from USA to China and India and other places, and thereby accelerate the loss of American jobs and downturn of the economy.

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: Gregory

Last Name: Hice

Mailing Address: 232 East Campus View Drive

City: Riverside

Country: United States

State or Province: CA

ZIP/Postal Code: 92507

Email Address: leonhart231@gmail.com

Organization Name: null

Comment: The proposed rule states that devices with a WiFi spectrum radio transmitter must prevent firmware changes. I understand that the goal of this rule is to enhance security of our devices (which are admittedly very weak to attacks), but I believe that there is a better way of solving the issues of malicious firmware modification.

Instead of completely blocking modification, I would recommend a solution similar to UEFI's "Secure Boot". In brief, the firmware would need to be digitally signed in some way, and the device would prevent firmware with an invalid signature from running. Importantly, this would allow companies and normal people alike to modify the firmware as they saw fit, but would (if done properly) prevent malicious attackers from changing the firmware themselves.

An important aspect to this proposal would be that it would need be simple for an end-user to use and sign their own firmware if they desire. As an electrical engineer, I can say we frequently use very constrained systems. If it was too costly (in terms of software or hardware) to create and run custom firmware, I believe it would hamper our ability to create new systems and learn from existing ones.

Thank you very much for your consideration.

The proposed rule states that devices with a WiFi spectrum radio transmitter must prevent firmware changes. I understand that the goal of this rule is to enhance security of our devices (which are admittedly very weak to attacks), but I believe that there is a better way of solving the issues of malicious firmware modification.

Instead of completely blocking modification, I would recommend a solution similar to UEFI's "Secure Boot". In brief, the firmware would need to be digitally signed in some way, and the device would prevent firmware with an invalid signature from running. Importantly, this would allow companies and normal people alike to modify the firmware as they saw fit, but would (if done properly) prevent malicious attackers from changing the firmware themselves.

An important aspect to this proposal would be that it would need be simple for an end-user to use and sign their own firmware if they desire. As an electrical engineer, I can say we frequently use very constrained systems. If it was too costly (in terms of software or hardware) to create and run custom firmware, I believe it would hamper our ability to create new systems and learn from existing ones.

Thank you very much for your consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Leland

Last Name: Harrell

Mailing Address: 8512 Aventine Ln, Apt 211

City: Fort Worth

Country: United States

State or Province: TX

ZIP/Postal Code: 76244

Email Address: k5gu@k5gu.com

Organization Name:

Comment:

Re: Notice of Proposed Rule Making, ET Docket No. 15-170, FCC 15-92,
"Equipment Authorization and Electronic Labeling for Wireless Devices"

As a consumer and a licensed Amateur Radio Operator involved in providing volunteer wireless communication assistance to agencies such as the American Red Cross, hospitals, local, state and federal agencies during emergencies and communications infrastructure outages, I am concerned about some of the aspects of this NPRM.

In particular, the effect it may have on the amateur radio operator's (as well as the Department of Defense who also use modified COTS devices) the ability to continue to use software to adapt wireless devices to amateur radio use during emergencies.

Any FCC rule that requires manufacturers of RF devices such as routers, access points, etc., to block or prevent software modifications needed to ensure public safety during disasters, acts of terrorism, war, civil unrest, etc., must also include an exception or a method to circumvent this block.

For example, an exception could be proposed to the rule that in case of an official national "declared emergency", a pass code or other decryption method to provide software modifications, be provided by the manufacturer of such devices as routers, access points, and any other devices used to assist in responding to emergencies for the duration of that crisis period. This would be similar to the FCC rules written to accommodate emergency communications during a real emergency.

Please ensure any changes proposed by ET Docket No. 15-170, FCC 15-92 conform to, and are consistent with the goals and priorities published by the U.S. Department of Homeland Security.

As a reference, please see below.

Excerpted from Department of Homeland Security secretary Johnson's "2014 National Emergency Communications Plan"

One of the plan's TOP PRIORITIES: "Enhancing coordination among stakeholders, processes, and planning activities across the emergency response community. "
"Requests for Assistance and Reporting "

"..In addition, amateur radio operators also serve as key contributors in this function as they can be important conduits for relaying information to response agencies and personnel when other forms of communications have failed or have been disrupted...".

"For the purpose of The National Emergency Communications Plan, the terms share information or information sharing refer to the exchange of data, information, or knowledge between various organizations, people, and technologies."

Thank you for your consideration of these comments.

Re: Notice of Proposed Rule Making, ET Docket No. 15-170, FCC 15-92,
"Equipment Authorization and Electronic Labeling for Wireless Devices"

As a consumer and a licensed Amateur Radio Operator involved in providing volunteer wireless communication assistance to agencies such as the American Red Cross, hospitals, local, state and federal agencies during emergencies and communications infrastructure outages, I am concerned about some of the aspects of this NPRM.

In particular, the effect it may have on the amateur radio operator's (as well as the Department of Defense who also use modified COTS devices) the ability to continue to use software to adapt wireless devices to amateur radio use during emergencies.

Any FCC rule that requires manufacturers of RF devices such as routers, access points, etc., to block or prevent software modifications needed to ensure public safety during disasters, acts of terrorism, war, civil unrest, etc., must also include an exception or a method to circumvent this block.

For example, an exception could be proposed to the rule that in case of an official national "declared emergency", a pass code or other decryption method to provide software modifications, be provided by the manufacturer of such devices as routers, access points, and any other devices used to assist in responding to emergencies for the duration of that crisis period. This would be similar to the FCC rules written to accommodate emergency communications during a real emergency.

Please ensure any changes proposed by ET Docket No. 15-170, FCC 15-92 conform to, and are consistent with the goals and priorities published by the U.S. Department of Homeland Security.

As a reference, please see below.

Excerpted from Department of Homeland Security secretary Johnson's "2014 National Emergency Communications Plan"

One of the plan's TOP PRIORITIES: "Enhancing coordination among stakeholders, processes, and planning activities across the emergency response community. "
"Requests for Assistance and Reporting "

"..In addition, amateur radio operators also serve as key contributors in this function as they can be important conduits for relaying information to response agencies and personnel when other forms of communications have failed or have been disrupted...".

"For the purpose of The National Emergency Communications Plan, the terms share information or information sharing refer to the exchange of data, information, or knowledge between various organizations, people, and technologies."

Thank you for your consideration of these comments.

Re: Notice of Proposed Rule Making, ET Docket No. 15-170, FCC 15-92,
"Equipment Authorization and Electronic Labeling for Wireless Devices"

As a consumer and a licensed Amateur Radio Operator involved in providing volunteer wireless communication assistance to agencies such as the American Red Cross, hospitals, local, state and federal agencies during emergencies and communications infrastructure outages, I am concerned about some of the aspects of this NPRM.

In particular, the effect it may have on the amateur radio operator's (as well as the Department of Defense who also use modified COTS devices) the ability to continue to use software to adapt wireless devices to amateur radio use during emergencies.

Any FCC rule that requires manufacturers of RF devices such as routers, access points, etc., to block or prevent software modifications needed to ensure public safety during disasters, acts of terrorism, war, civil unrest, etc., must also include an exception or a method to circumvent this block.

For example, an exception could be proposed to the rule that in case of an official national "declared emergency", a pass code or other decryption method to provide software modifications, be provided by the manufacturer of such devices as routers, access points, and any other devices used to assist in responding to emergencies for the duration of that crisis period. This would be similar to the FCC rules written to accommodate emergency communications during a real emergency.

Please ensure any changes proposed by ET Docket No. 15-170, FCC 15-92 conform to, and are consistent with the goals and priorities published by the U.S. Department of Homeland Security.

As a reference, please see below.

Excerpted from Department of Homeland Security secretary Johnson's "2014 National Emergency Communications Plan"

One of the plan's TOP PRIORITIES: "Enhancing coordination among stakeholders, processes, and planning activities across the emergency response community. "

"Requests for Assistance and Reporting "

"..In addition, amateur radio operators also serve as key contributors in this function as they can be important conduits for relaying information to response agencies and personnel when other forms of communications have failed or have been disrupted...".

"For the purpose of The National Emergency Communications Plan, the terms "share information" or "information sharing" refer to the exchange of data, information, or knowledge between various organizations, people, and technologies."

Thank you for your consideration of these comments.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Steven

Last Name: Hooper

Mailing Address: 5600 Russell Ave

City: Mission

Country: United States

State or Province: KS

ZIP/Postal Code: 66202

Email Address: steven@4ourth.com

Organization Name: 4ourth Mobile

Comment: As you say in the synopsis of this rule, "The telecommunications sector depends on the variety and utility of radiofrequency (RF) devices." This proposed rule would have the effect of restricting innovation and reducing variety, with the end result being a more dangerously homogenous network.

I oppose implementing any rule that restricts the ability of equipment end users from installing software of their choosing on their computing devices.

My opposition to this proposal is not just a personal freedom argument, but one grounded in business, engineering, and science. Networking improves due to the ability of researchers to investigate and modify their devices. There should be no restriction on what a "researcher" is. DMCA is a poor model to follow and permission to research and modify is not working well to innovate and develop products in this space.

End users including consumers need, and should continue to 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 proposed 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.

As you say in the synopsis of this rule, "The telecommunications sector depends on the variety and utility of radiofrequency (RF) devices." This proposed rule would have the effect of restricting innovation and reducing variety, with the end result being a more dangerously homogenous network.

I oppose implementing any rule that restricts the ability of equipment end users from installing software of their choosing on their computing devices.

My opposition to this proposal is not just a personal freedom argument, but one grounded in business, engineering, and science. Networking improves due to the ability of researchers to investigate and modify their devices. There should be no restriction on what a "researcher" is. DMCA is a poor model to follow and permission to research and modify is not working well to innovate and develop products in this space.

End users including consumers need, and should continue to 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 proposed 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: Ashwin

Last Name: Purohit

Mailing Address: 90 Fairview Ave, Bldg 3 Apt 2

City: Kingston

Country: United States

State or Province: NY

ZIP/Postal Code: 12401

Email Address: apurohit8@gmail.com

Organization Name:

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

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software. At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of

industrial espionage.

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

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software. At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

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: Lada

Mailing Address: 1106 W 3RD ST

City: MARION

Country: United States

State or Province: IN

ZIP/Postal Code: 46952-3667

Email Address: rlada@live.com

Organization Name:

Comment: Today, American consumers are already limited in their options for reliable network routers. Most of the easily accessible, reasonably priced options for home-based networks are mediocre at best, and unusable at worst. Virtually all firmware that is included with these devices is unreliable, buggy, and full of security vulnerabilities. In many cases, the manufacturers of these devices are unwilling or unable to provide updates to the firmware in a sufficient time frame for them to be effective. In some cases, device manufacturers neglect to provide updates or patch major security vulnerabilities at all. These devices are critical to the infrastructure of many, many American businesses, and they are being left wide open for any attacker with ill intent to walk right into with minimal effort. (see: http://www.securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php)

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWRT and DD-WRT. End-users often use such firmware because it better fits the users needs, or provides feature updates and patches for security vulnerabilities far sooner than device manufacturers can or will. Each user is also better able to tailor the device to their needs with said alternatives. Users often set up a guest wireless network for their home or business, set up a web server at their home, create hardware based hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWRT as the base of their router software. (see: [1] <http://www.cavium.com/newsevents-Cavium-Delivers-Optimized-OpenWRT-on-OCTEON-III.html> [2]

<https://www.codeaurora.org/xwiki/bin/QSDK/WebHome> [3] <http://mediatek.com/en/news-events/mediatek-news/mediatek-launches-mt7628-industrys-first-80211n-2t2r-ap-soc-for-home-router-smart-router-and-iot-gateway/>)

At the same time, OpenWRT is managed and developed primarily by a community of individuals modifying their own personal routers and installing customized versions of OpenWRT on their own devices. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace the firmware on their router with a customized version of OpenWRT. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could (1) be passed along to customers and employees, and (2) decrease the willingness of hardware manufacturers to invest even more time and money into researching and correcting security vulnerabilities.

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so

chooses. Many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency preparedness would also be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner. (see: <http://www.arrl.org/news/broadband-hamnet-wins-international-association-of-emergency-managers-awards/>)

Today, American consumers are already limited in their options for reliable network routers. Most of the easily accessible, reasonably priced options for home-based networks are mediocre at best, and unusable at worst. Virtually all firmware that is included with these devices is unreliable, buggy, and full of security vulnerabilities. In many cases, the manufacturers of these devices are unwilling or unable to provide updates to the firmware in a sufficient time frame for them to be effective. In some cases, device manufacturers neglect to provide updates or patch major security vulnerabilities at all. These devices are critical to the infrastructure of many, many American businesses, and they are being left wide open for any attacker with ill intent to walk right into with minimal effort. (see: http://www.securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php)

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWRT and DD-WRT. End-users often use such firmware because it better fits the users needs, or provides feature updates and patches for security vulnerabilities far sooner than device manufacturers can or will. Each user is also better able to tailor the device to their needs with said alternatives. Users often set up a guest wireless network for their home or business, set up a web server at their home, create hardware based hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWRT as the base of their router software. (see: [1] <http://www.cavium.com/newsevents-Cavium-Delivers-Optimized-OpenWRT-on-OCTEON-III.html> [2] <https://www.codeaurora.org/xwiki/bin/QSDK/WebHome> [3] <http://mediatek.com/en/news-events/mediatek-news/mediatek-launches-mt7628-industrys-first-80211n-2t2r-ap-soc-for-home-router-smart-router-and-iot-gateway/>) At the same time, OpenWRT is managed and developed primarily by a community of individuals modifying their own personal routers and installing customized versions of OpenWRT on their own devices. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace the firmware on their router with a customized version of OpenWRT. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could (1) be passed along to customers and employees, and (2) decrease the willingness of hardware manufacturers to invest even more time and money into researching and correcting security vulnerabilities.

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses. Many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency preparedness would also be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on

low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner. (see: <http://www.arrl.org/news/broadband-hamnet-wins-international-association-of-emergency-managers-awards/>)

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: Darrell

Last Name: Bradshaw

Mailing Address: 2427 W Kathleen Rd

City: Phoenix

Country: United States

State or Province: AZ

ZIP/Postal Code: 85023

Email Address: miscbs@gmail.com

Organization Name:

Comment: I would like to ask that you reconsider implementing these rules. As a person that has loaded new factory and modified, open-source firmware on many routers, these firmware changes were all for new networking features or fixing a flaw or security hole in the device. Never has the firmware update be used for a malicious abuse of radio spectrum. A few years ago, I got my ham license and now I load modified firmware in wifi routers for legal amateur radio uses.

Security holes happen. I do not want to trash and rebuy a \$120-200 router due to a simple software bug. Recent bugs (Heartbleed and Poodle) in the open source encryption OpenSSL that protects websites caused changes to a vast majority of servers serving up the internet. Many of these routers on the market today use the same Linux based, open source resources in their software. Image the electronic waste that would result if a major exploit was found in one of those resources.

It would be possible that hackers could easily over take and control these flawed routers in massive bot nets to run DDoS attacks. I am an old sysadmin so I remember NIMDA and CodeRed - Windows systems running around happily infecting each other over the internet. These two bugs caused all ISPs to block port 80 to their non-commercial users.

Sure it hasn't happened yet, but OpenSSL had a great track record before it was hit with Heartbleed and Poodle. Could manufacturers keep up with the demand to replace a "vast majority" of flawed routers?

Firmware "hackers" have also driven innovation and built companies. Buffalo Tech owes their success to the fact that they sell routers loaded with version of open source firmware DD-WRT that they improved on.

Requiring protecting firmware changes will increase the cost of these devices and maybe for naught. Remember that DVDs and Blurays would supposedly NEVER be cracked and copied.

Thanks for considering my input.

Darrell Bradshaw

W7ZCK

I would like to ask that you reconsider implementing these rules. As a person that has loaded new factory and modified, open-source firmware on many routers, these firmware changes were all for new networking features or fixing a flaw or security hole in the device. Never has the firmware update be used for a malicious abuse of radio spectrum. A few years ago, I got my ham license and now I load modified firmware in wifi routers for legal amateur radio uses.

Security holes happen. I do not want to trash and rebuy a \$120-200 router due to a simple software bug. Recent bugs (Heartbleed and Poodle) in the open source encryption OpenSSL that protects websites caused changes to a vast majority of servers serving up the internet. Many of these routers on the market today use the same Linux based, open source resources in their software. Image the electronic waste that would result if a major exploit was found in one of those resources.

It would be possible that hackers could easily over take and control these flawed routers in massive bot nets to run DDoS attacks. I am an old sysadmin so I remember NIMDA and CodeRed - Windows systems running around happily infecting each other over the internet. These two bugs caused all ISPs to block port 80 to their non-commercial users.

Sure it hasn't happened yet, but OpenSSL had a great track record before it was hit with Heartbleed and Poodle. Could manufacturers keep up with the demand to replace a "vast majority" of flawed routers?

Firmware "hackers" have also driven innovation and built companies. Buffalo Tech owes their success to the fact that they sell routers loaded with version of open source firmware DD-WRT that they improved on.

Requiring protecting firmware changes will increase the cost of these devices and maybe for naught. Remember that DVDs and Blurays would supposedly NEVER be cracked and copied.

Thanks for considering my input.

Darrell Bradshaw

W7ZCK

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: Judah

Last Name: Towery

Mailing Address: 6902 Coors Blvd

City: Albuquerque

Country: United States

State or Province: NM

ZIP/Postal Code: 87110

Email Address:

Organization Name:

Comment: Please do not take away the ability for users to install software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules. Users should be able to manipulate and control all aspects of their devices. The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

Please do not take away the ability for users to install software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules. Users should be able to manipulate and control all aspects of their devices. The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

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: Alan

Last Name: Richmond

Mailing Address: 1449 Pine St

City: Eureka

Country: United States

State or Province: CA

ZIP/Postal Code: 95501

Email Address: alan@aardwolfweb.com

Organization Name: Aardwolf Networking

Comment: I am own a computer repair and network support business (California licensed electronics repair) and also a licensed amateur radio operator (Technician). As I read these proposed regulations, it would appear they will have a serious negative impact on my ability to provide the safest and most appropriate software for my clients on my business side and the research into mesh networking for emergency communications services that I do on my ham radio personal side.

I run third party firmwares/operating systems on nearly all of my business and personal electronics; GNU/Linux on my PCs, DD-WRT on my routers and Canogen|mod on my tablets and phone.

Don't take those choices and more secure options away.

I am own a computer repair and network support business (California licensed electronics repair) and also a licensed amateur radio operator (Technician). As I read these proposed regulations, it would appear they will have a serious negative impact on my ability to provide the safest and most appropriate software for my clients on my business side and the research into mesh networking for emergency communications services that I do on my ham radio personal side.

I run third party firmwares/operating systems on nearly all of my business and personal electronics; GNU/Linux on my PCs, DD-WRT on my routers and Canogen|mod on my tablets and phone.

Don't take those choices and more secure options away.

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: dan

Last Name: robis

Mailing Address: 237s kolb RD

City: tucson

Country: United States

State or Province: AZ

ZIP/Postal Code: 85710

Email Address:

Organization Name:

Comment: please do not implement this. this law prevents the fixing of issues on devices when the manufactures have stopped supporting devices.

please do not implement this. this law prevents the fixing of issues on devices when the manufactures have stopped supporting devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Citizen

Last Name: Citizen

Mailing Address: one in the US

City: one in the US

Country: United States

State or Province: FL

ZIP/Postal Code: 00000

Email Address:

Organization Name:

Comment: It is not feasible to put restrictions on what software can tell hardware to do without severely limiting peoples rights. Your better off solving the problem this was trying to address some other way.

It is not feasible to put restrictions on what software can tell hardware to do without severely limiting peoples rights. Your better off solving the problem this was trying to address some other way.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Alex

Last Name: Stewart

Mailing Address: 3393 Euclid Ave

City: Concord

Country: United States

State or Province: CA

ZIP/Postal Code: 94519

Email Address: foogod@gmail.com

Organization Name:

Comment: Hello,

I am commenting on behalf of myself as a user of commercial WiFi equipment, professional system administrator, and software developer (I am not associated with any router firmware development projects).

I wish to register my opposition to the currently proposed regulations regarding manufacturers limiting the ability to replace device firmware. While I understand the concern regarding modifying critical radio parameters, I believe the present wording would have substantial unintended negative effects in a variety of other areas.

It is my understanding that it is the FCC's position that these regulations will not prohibit custom firmware on WiFi devices; however, it is my belief that the current vagueness of the exact requirements for access control coupled with suggestions that manufacturers could prevent such "reflashing" will lead to the vast majority of manufacturers choosing to implement such restrictions even if they are not technically mandated by the new rules.

The end result is that these new rules, whether explicitly requiring it or not, will likely in reality mean the end of the ability to use custom firmware on most or all consumer WiFi equipment, and that would in turn harm the consumer in numerous ways:

- (1) Many manufacturers still do not offer security fixes for firmware vulnerabilities discovered months or years ago. In many cases, custom firmware is the only way that users have to make their devices work safely and securely.
- (2) Many alternative firmwares offer (perfectly legal) features and abilities which are simply not available from the manufacturers' stock firmware. Prohibiting such changes would substantially limit many consumers in their abilities to fully use the capabilities of the hardware they have purchased for purposes they should be entitled to.
- (3) To date open-source router firmware projects have been the basis for a large amount of research, innovation, and improvement in the WiFi space, including developments which have actually improved performance and coexistence between devices over what was previously offered by stock firmware. Without the ability to use custom firmware, many critical forms of technical innovation would be stifled.

I understand that the increasing flexibility of these devices coupled with the ability of average users and developers to improve upon their abilities comes with some concerns, but it is critically important to realize that these very same attributes bring with them a much greater potential for good, and have the potential to usher in a burgeoning age of development and innovation of great benefit to everyone involved. It is my belief that because of this newfound

widespread accessibility and configurability, we are only beginning to see what could come to be a golden age of technological advances in this field. I also believe it is very important that we do not "throw the baby out with the bathwater" by inadvertently shutting down such great potential just as it is starting to come to fruition by poorly worded or thought-out legislation. We may not ever know the benefits we end up giving up as a result.

It is also important to note that, despite many people's impressions, replacing router firmware is increasingly common, and is no longer just a niche undertaking for technical people. Many people with limited computer expertise (such as my own parents) now have the ability to perform these upgrades themselves and take advantage of all of the benefits they provide, so this sort of legislative change has the potential to negatively affect a great number of average consumers, not just a few "nerds" or "geeks".

I believe it is critical that the FCC not only consider what the letter of the law actually says, but the ramifications of the likely interpretation of that law by the manufacturers who must attempt to interpret and conform to it, and it is not enough to simply say "we didn't technically say that". Even if not intended, this new rule in its current form has the potential to stifle innovation and substantially harm security and functionality of WiFi hardware across the board, and that will ultimately be harmful to everyone. Please do not do this.

Thank you for your consideration.

Hello,

I am commenting on behalf of myself as a user of commercial WiFi equipment, professional system administrator, and software developer (I am not associated with any router firmware development projects).

I wish to register my opposition to the currently proposed regulations regarding manufacturers limiting the ability to replace device firmware. While I understand the concern regarding modifying critical radio parameters, I believe the present wording would have substantial unintended negative effects in a variety of other areas.

It is my understanding that it is the FCC's position that these regulations will not prohibit custom firmware on WiFi devices; however, it is my belief that the current vagueness of the exact requirements for access control coupled with suggestions that manufacturers could prevent such "reflashing" will lead to the vast majority of manufacturers choosing to implement such restrictions even if they are not technically mandated by the new rules.

The end result is that these new rules, whether explicitly requiring it or not, will likely in reality mean the end of the ability to use custom firmware on most or all consumer WiFi equipment, and that would in turn harm the consumer in numerous ways:

- (1) Many manufacturers still do not offer security fixes for firmware vulnerabilities discovered months or years ago. In many cases, custom firmware is the only way that users have to make their devices work safely and securely.
- (2) Many alternative firmwares offer (perfectly legal) features and abilities which are simply not available from the manufacturers' stock firmware. Prohibiting such changes would substantially limit many consumers in their abilities to fully use the capabilities of the hardware they have purchased for purposes they should be entitled to.
- (3) To date open-source router firmware projects have been the basis for a large amount of research, innovation, and improvement in the WiFi space, including developments which have actually improved performance and coexistence between devices over what was previously offered by stock firmware. Without the ability to use custom firmware, many critical forms of technical innovation would be stifled.

I understand that the increasing flexibility of these devices coupled with the ability of average users and developers to improve upon their abilities comes with some concerns, but it is critically important to realize that these very same attributes bring with them a much greater potential for good, and have the potential to usher in a burgeoning age of development and innovation of great benefit to everyone involved. It is my belief that because of this newfound

widespread accessibility and configurability, we are only beginning to see what could come to be a golden age of technological advances in this field. I also believe it is very important that we do not "throw the baby out with the bathwater" by inadvertently shutting down such great potential just as it is starting to come to fruition by poorly worded or thought-out legislation. We may not ever know the benefits we end up giving up as a result.

It is also important to note that, despite many people's impressions, replacing router firmware is increasingly common, and is no longer just a niche undertaking for technical people. Many people with limited computer expertise (such as my own parents) now have the ability to perform these upgrades themselves and take advantage of all of the benefits they provide, so this sort of legislative change has the potential to negatively affect a great number of average consumers, not just a few "nerds" or "geeks".

I believe it is critical that the FCC not only consider what the letter of the law actually says, but the ramifications of the likely interpretation of that law by the manufacturers who must attempt to interpret and conform to it, and it is not enough to simply say "we didn't technically say that". Even if not intended, this new rule in its current form has the potential to stifle innovation and substantially harm security and functionality of WiFi hardware across the board, and that will ultimately be harmful to everyone. Please do not do this.

Thank you for your consideration.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Ridley

Mailing Address: 14383 Fairway Dr

City: Chelsea

Country: United States

State or Province: MI

ZIP/Postal Code: 48118

Email Address: ridley.john@gmail.com

Organization Name:

Comment: Thank you for the opportunity to comment on this important proposal.

I am a semi-knowledgeable consumer of residential networking equipment and a proponent of open hardware and software.

I have, on many occasions, installed alternative, open source firmware in consumer level routers. I do this for two reasons, the first is for stability, the second is to access additional features that may not be available in factory firmware.

I have had equipment that was basically completely unusable with the factory firmware; one piece of equipment in particular wouldn't run for more than about an hour without crashing. I installed DD-WRT and it's been running for over 5 years with no trouble since then.

Also, there have been NUMEROUS cases in the past of serious vulnerabilities being discovered in manufacturer firmware. Manufacturers are not always willing to fix or even acknowledge these issues, especially on older equipment that may no longer be supported. In my opinion, it's imperative that consumers be allowed to use alternate software to defend the digital "castle" of their home network.

Consumer networking equipment manufacturers that I have had contact with are fully aware of the fact that people are installing aftermarket firmware on their equipment, and I have never talked to one that had any problem with this. More than one manufacturer actually makes models specifically designed and guaranteed to run open source firmware.

I have never used aftermarket firmware to cause the radios in the equipment to operate outside of legal parameters. I feel that this proposal threatens my ability to operate a stable and secure personal network; being forced to just live with whatever firmware the manufacturer cares to provide is unduly limiting.

Finally, the internet has, from the beginning and in an ongoing basis, been built on open standards, technologies and software. Open software provides the basis for everyone down to the level of the individual experimenter playing with a new idea in his home to potentially create the next big thing. Computers, networking and digital radio communications is extremely exciting now and I think we haven't seen anything yet, if we allow the universal human urge to explore and innovate to continue rather than stifling it or making it unduly expensive by imposing too many rules.

Thank you for the opportunity to comment on this important proposal.

I am a semi-knowledgeable consumer of residential networking equipment and a proponent of open hardware and

software.

I have, on many occasions, installed alternative, open source firmware in consumer level routers. I do this for two reasons, the first is for stability, the second is to access additional features that may not be available in factory firmware.

I have had equipment that was basically completely unusable with the factory firmware; one piece of equipment in particular wouldn't run for more than about an hour without crashing. I installed DD-WRT and it's been running for over 5 years with no trouble since then.

Also, there have been NUMEROUS cases in the past of serious vulnerabilities being discovered in manufacturer firmware. Manufacturers are not always willing to fix or even acknowledge these issues, especially on older equipment that may no longer be supported. In my opinion, it's imperative that consumers be allowed to use alternate software to defend the digital "castle" of their home network.

Consumer networking equipment manufacturers that I have had contact with are fully aware of the fact that people are installing aftermarket firmware on their equipment, and I have never talked to one that had any problem with this. More than one manufacturer actually makes models specifically designed and guaranteed to run open source firmware.

I have never used aftermarket firmware to cause the radios in the equipment to operate outside of legal parameters. I feel that this proposal threatens my ability to operate a stable and secure personal network; being forced to just live with whatever firmware the manufacturer cares to provide is unduly limiting.

Finally, the internet has, from the beginning and in an ongoing basis, been built on open standards, technologies and software. Open software provides the basis for everyone down to the level of the individual experimenter playing with a new idea in his home to potentially create the next big thing. Computers, networking and digital radio communications is extremely exciting now and I think we haven't seen anything yet, if we allow the universal human urge to explore and innovate to continue rather than stifling it or making it unduly expensive by imposing too many rules.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brian

Last Name: Weck

Mailing Address: 1413 Mosaic Glen

City: Escondido

Country: United States

State or Province: CA

ZIP/Postal Code: 92029

Email Address: toon@brainwick.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.

That being said, I also understand the FCC's interest in making sure that wireless devices operate within the RF ranges that they are originally certified to use. I believe that this should be an issue directly addressed by the equipment manufacturers to allow for custom code be applied to their hardware while keeping the RF equipment from operating

outside of appropriate ranges.

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.

That being said, I also understand the FCC's interest in making sure that wireless devices operate within the RF ranges that they are originally certified to use. I believe that this should be an issue directly addressed by the equipment manufacturers to allow for custom code be applied to their hardware while keeping the RF equipment from operating outside of appropriate ranges.

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: Nathaniel

Last Name: Emerick

Mailing Address: 1018 Christ Way

City: Wills Point

Country: United States

State or Province: TX

ZIP/Postal Code: 75169

Email Address: npemerick@outlook.com

Organization Name:

Comment: Dear FCC,

I want to respectfully ask you to not implement rules and bans to take away the ability for me or other users to install software of our choosing on our own devices (routers, laptops, desktop, cell phones and other mobile devices, etc.).

The feature of wireless networking depends on the ability for people to investigate, research and modify our devices. Restrictions on this will only hinder innovation. Not only innovation but our ability to secure holes in devices that manufactures chose to no longer support is at risk by imposing rules against modifying devices we own. Users have many times in the past fixed serious flaws and security holes in their wifi devices which would be banned under NPRM. Banning this will create and feed greater cyber-threats then already exist and cause an increase in the waste of electronics.

There is a huge market of commerce that will be severely hindered if not outright gone if these restrictions are imposed on our devices (secure wifi vendors, hotspot vendors etc.).

Thank you for respecting the use of our devices and for listening to my comments.

Sincerely,

Patrick Emerick

Network Administrator

Dear FCC,

I want to respectfully ask you to not implement rules and bans to take away the ability for me or other users to install software of our choosing on our own devices (routers, laptops, desktop, cell phones and other mobile devices, etc.).

The feature of wireless networking depends on the ability for people to investigate, research and modify our devices. Restrictions on this will only hinder innovation. Not only innovation but our ability to secure holes in devices that manufactures chose to no longer support is at risk by imposing rules against modifying devices we own. Users have many times in the past fixed serious flaws and security holes in their wifi devices which would be banned under NPRM. Banning this will create and feed greater cyber-threats then already exist and cause an increase in the waste of electronics.

There is a huge market of commerce that will be severely hindered if not outright gone if these restrictions are imposed on our devices (secure wifi vendors, hotspot vendors etc.).

Thank you for respecting the use of our devices and for listening to my comments.

Sincerely,

Patrick Emerick
Network Administrator

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: Connor

Last Name: Stec

Mailing Address: 32083 11 Mile Rd

City: Farmington Hills

Country: United States

State or Province: MI

ZIP/Postal Code: 48336

Email Address:

Organization Name:

Comment: Rules can help keep society organized, but there are cases when the very same rules become obstacles to new things that just can't follow the strict guidelines.

Innovation is a black box; we never know on what path progress will take, so we need to keep a balance on what to say no to.

Connectivity has this type of potential and the late progress on WLAN modules has boosted the community of makers including small companies creating innovative products. All these sectors rely on getting to the bottom levels of hardware and software to find new ideas and create new value, which may include using a WLAN module for something completely different than what it was designed for. To name a few applications, there are indoor position systems and parallel data transmission links for increased speed.

I don't think it is right to put an end to this potential for innovation by banning custom firmware/radio firmware on WLAN modules. Hardware and software are tools, and we should be free to exploit them as we want, in the name of progress, small steps or large.

Rules can help keep society organized, but there are cases when the very same rules become obstacles to new things that just can't follow the strict guidelines.

Innovation is a black box; we never know on what path progress will take, so we need to keep a balance on what to say no to.

Connectivity has this type of potential and the late progress on WLAN modules has boosted the community of makers including small companies creating innovative products. All these sectors rely on getting to the bottom levels of hardware and software to find new ideas and create new value, which may include using a WLAN module for something completely different than what it was designed for. To name a few applications, there are indoor position systems and parallel data transmission links for increased speed.

I don't think it is right to put an end to this potential for innovation by banning custom firmware/radio firmware on WLAN modules. Hardware and software are tools, and we should be free to exploit them as we want, in the name of progress, small steps or large.

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: Howard

Last Name: Abbey

Mailing Address: 7663 Sleepy Hollow Dr

City: Northville

Country: United States

State or Province: MI

ZIP/Postal Code: 48168-8800

Email Address: hrabbey@yahoo.com

Organization Name:

Comment: Concern has been raised with the rules interfering with the ability to install custom firmware (or to update with not yet officially released firmware) to devices in consumer's possession.

This is a security concern that I could not support.

I think a better alternative to regulation would be to encourage transparency about the limits and abilities of devices, and the responsibilities of device owners.

Concern has been raised with the rules interfering with the ability to install custom firmware (or to update with not yet officially released firmware) to devices in consumer's possession.

This is a security concern that I could not support.

I think a better alternative to regulation would be to encourage transparency about the limits and abilities of devices, and the responsibilities of device owners.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Dave

Last Name: Kalata

Mailing Address: 13530 Linden Ave N Apt 113

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98133-7552

Email Address: Dave@Kalata.net

Organization Name:

Comment: The FCC' proposed restrictions are entirely too broad Third party firmware provides many bug and security fixes to devices that manufacturers are often slow to fix or have abandoned completely in regards to firmware changes!

The FCC' proposed restrictions are entirely too broad Third party firmware provides many bug and security fixes to devices that manufacturers are often slow to fix or have abandoned completely in regards to firmware 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: Arthur

Last Name: Baldwin

Mailing Address: 171 Shamwood Avenue

City: Rialto

Country: United States

State or Province: CA

ZIP/Postal Code: 92377

Email Address: eengnerd@yahoo.com

Organization Name: Mobile PC Clinic

Comment: This proposal is foolish. It will end up creating much more electronic waste, when consumers are forced into early replacement of their wireless routers because the device they own cannot be updated. The proposal also puts restrictions on developers whose aims are to benefit mankind. There will always be those who seek to harm or control the masses, but let's not shackle everybody while taking the "lazy man's way out" of this problem.

Sincerely,

Arthur Baldwin

This proposal is foolish. It will end up creating much more electronic waste, when consumers are forced into early replacement of their wireless routers because the device they own cannot be updated. The proposal also puts restrictions on developers whose aims are to benefit mankind. There will always be those who seek to harm or control the masses, but let's not shackle everybody while taking the "lazy man's way out" of this problem.

Sincerely,

Arthur Baldwin

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: Henriksen

Mailing Address: 2121 San Felipe St Ste 138

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77019

Email Address:

Organization Name:

Comment: Banning the changing or updating of firmware on wireless devices is a terrible idea which will come with all sorts of unintended consequences. I vote NO to this rule.

Banning the changing or updating of firmware on wireless devices is a terrible idea which will come with all sorts of unintended consequences. I vote NO to this rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Harley

Last Name: Gifford

Mailing Address: 108 McCloud Lane

City: Portland

Country: United States

State or Province: TN

ZIP/Postal Code: 37148

Email Address:

Organization Name:

Comment: The ability to modify and install custom software is the heart of the Free Software movement. Should this come to fruition, devices made under this regulation would be unable to be modified. Such modifications may not seem so necessary, but they make possible enhancements such as security which the manufacturer did not implement, so users who use the affected devices would be at greater risk of being compromised in information security.

The ability to modify and install custom software is the heart of the Free Software movement. Should this come to fruition, devices made under this regulation would be unable to be modified. Such modifications may not seem so necessary, but they make possible enhancements such as security which the manufacturer did not implement, so users who use the affected devices would be at greater risk of being compromised in information security.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Fustini

Mailing Address: 4749 N Spaulding Ave

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60625

Email Address: pdp7pdp7@gmail.com

Organization Name: null

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joshua

Last Name: Dumas

Mailing Address: 697 Pine St.

City: Manchester

Country: United States

State or Province: NH

ZIP/Postal Code: 03104

Email Address: josh.dumas@outlook.com

Organization Name:

Comment: Please do not prevent the use of custom or open-source firmware.

Please do not prevent the use of custom or open-source firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Thomas

Mailing Address: 2020 Charleston Oak Circle

City: Lawrenceville

Country: United States

State or Province: GA

ZIP/Postal Code: 30043

Email Address:

Organization Name: J and J Computers

Comment: I do not mind the implementation of rules regarding the changing of the radio transmitters specifically, however it would be a grave loss to everyone if Open Source or third party software could not be loaded onto devices.

Many technologies, bug fixes, concepts, and implementations have been developed and rely on the use of software being loaded onto devices for uses other than what they were originally designed for. Could you imagine computers today if we were told a long time ago that we couldn't hook up an external device like a mouse to it. Could you imagine what phone smartphones would be like if the first ones people were told that you could only make calls (no texting, no email, no internet).

Development is a process, and the use of already manufactured equipment for different reasons than what they were originally intended for is part of that process. If this ruling is too restrictive that the manufacturers make equipment that can not be legally modified, than future development outside of massive companies will be drastically slowed down, if not even halted.

Please consider your words carefully, when creating a ruling that will affect millions due to the few that don't follow appropriate existing laws and guidelines.

I do not mind the implementation of rules regarding the changing of the radio transmitters specifically, however it would be a grave loss to everyone if Open Source or third party software could not be loaded onto devices.

Many technologies, bug fixes, concepts, and implementations have been developed and rely on the use of software being loaded onto devices for uses other than what they were originally designed for. Could you imagine computers today if we were told a long time ago that we couldn't hook up an external device like a mouse to it. Could you imagine what phone smartphones would be like if the first ones people were told that you could only make calls (no texting, no email, no internet).

Development is a process, and the use of already manufactured equipment for different reasons than what they were originally intended for is part of that process. If this ruling is too restrictive that the manufacturers make equipment that can not be legally modified, than future development outside of massive companies will be drastically slowed down, if not even halted.

Please consider your words carefully, when creating a ruling that will affect millions due to the few that don't follow appropriate existing laws and guidelines.