

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: Yunseok

Last Name: Choi

Mailing Address: 1760 Broadway St Apt 328

City: Ann Arbor

Country: United States

State or Province: MI

ZIP/Postal Code: 48105

Email Address:

Organization Name:

Comment: Implementing rules that take away the ability of users to install the software of their choosing on their computing devices reduces innovation and security. Wifi drivers often have serious bugs that pose a security threat. By being able to modify the firmware, users are able to defend their network and data from malicious hackers and criminals. Americans should have the right to maintain their security. In addition, allowing modification allows researchers and other inventors to create new innovation that would make computing and wireless data transfer more secure, which would reduce the costs of damages that security issues cause. Not fixing security holes either feeds cyberthreats or increases electronic waste. Meanwhile,there is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. Please do not implement restrictions that hinder progress and security.

Implementing rules that take away the ability of users to install the software of their choosing on their computing devices reduces innovation and security. Wifi drivers often have serious bugs that pose a security threat. By being able to modify the firmware, users are able to defend their network and data from malicious hackers and criminals. Americans should have the right to maintain their security. In addition, allowing modification allows researchers and other inventors to create new innovation that would make computing and wireless data transfer more secure, which would reduce the costs of damages that security issues cause. Not fixing security holes either feeds cyberthreats or increases electronic waste. Meanwhile,there is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. Please do not implement restrictions that hinder progress and 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: Yunseok

Last Name: Choi

Mailing Address: 1760 Broadway St Apt 328

City: Ann Arbor

Country: United States

State or Province: MI

ZIP/Postal Code: 48105

Email Address:

Organization Name:

Comment: Implementing rules that take away the ability of users to install the software of their choosing on their computing devices reduces innovation and security. Wifi drivers often have serious bugs that pose a security threat. By being able to modify the firmware, users are able to defend their network and data from malicious hackers and criminals. Americans should have the right to maintain their security. In addition, allowing modification allows researchers and other inventors to create new innovation that would make computing and wireless data transfer more secure, which would reduce the costs of damages that security issues cause. Not fixing security holes either feeds cyberthreats or increases electronic waste. Meanwhile,there is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. Please do not implement restrictions that hinder progress and security.

Implementing rules that take away the ability of users to install the software of their choosing on their computing devices reduces innovation and security. Wifi drivers often have serious bugs that pose a security threat. By being able to modify the firmware, users are able to defend their network and data from malicious hackers and criminals. Americans should have the right to maintain their security. In addition, allowing modification allows researchers and other inventors to create new innovation that would make computing and wireless data transfer more secure, which would reduce the costs of damages that security issues cause. Not fixing security holes either feeds cyberthreats or increases electronic waste. Meanwhile,there is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. Please do not implement restrictions that hinder progress and 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: Joseph

Last Name: Stephenson

Mailing Address: 10450 East Bankhead Hwy.

City: Aledo

Country: United States

State or Province: TX

ZIP/Postal Code: 76008

Email Address: liroku@gmail.com

Organization Name:

Comment: This is a terrible proposal. This legislation would stifle innovation in terrible but very real ways. The economic impact would be dire, the security implications would be extreme, and emergency preparedness would be greatly hindered by the proposed restrictions on router firmware. I am vehemently opposed to this proposal.

This is a terrible proposal. This legislation would stifle innovation in terrible but very real ways. The economic impact would be dire, the security implications would be extreme, and emergency preparedness would be greatly hindered by the proposed restrictions on router firmware. I am vehemently opposed to this proposal.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: david

Last Name: serck

Mailing Address: avenue charles-quint

City: wavre

Country: Belgium

State or Province: Belgique

ZIP/Postal Code: 1300

Email Address: serckdavid@msn.com

Organization Name:

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

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

We 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.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

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

We 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.

There is no evidence that open-source firmware has caused any more wireless interference than closed-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: Michael

Last Name: Ossmann

Mailing Address: 27902 Meadow Dr. Suite 150

City: Evergreen

Country: United States

State or Province: CO

ZIP/Postal Code: 80439

Email Address: mike@ossmann.com

Organization Name: Great Scott Gadgets

Comment: Thank you for inviting comments on the proposed rules for Equipment Authorization and Electronic Labeling for Wireless Devices.

I am the owner of Great Scott Gadgets, a US company that makes open source test equipment primarily for the information security industry. As a designer and manufacturer of communications equipment, I commend the Commission for seeking to clarify and streamline the rules for equipment authorization. I believe that, on the whole, the updated rules will benefit the electronics industry. However, I am concerned that the rules regarding software control of radio parameters place an undue burden on device manufacturers and unnecessarily restrict the actions of end users.

My concerns arise from rules already in place for Software Defined Radio (SDR) devices. I am encouraged to see that the Commission is eliminating certain special rules for SDR equipment and seeks to treat SDR and non-SDR devices in the same way. However, while the Commission notes that "the existing SDR rules have proven to be insufficiently flexible," the proposed rules broaden the reach of those rules to non-SDR equipment.

The requirement to implement security measures preventing the modification of software has long been unpopular in the SDR community. Software security is difficult, expensive, and unreliable, and it undermines reconfigurability, a principal benefit of SDR. The proposed rules extend this absurd requirement to all radio equipment with any software control, encompassing most radio devices manufactured today.

Under the proposed rules, all radio device manufacturers would be required to devise software security mechanisms that do not exist today, and they would have to prepare for each new device software documentation that is currently not required. Makers of integrated circuits would have to develop entirely new product lines that provide device manufacturers with security mechanisms, killing off existing product lines that lack such controls.

These requirements seem particularly onerous when considering the fact that computer security is largely an unsolved problem. Where manufacturers have had limited success preventing modification of software in electronic devices (e.g. in mobile phones), it has been accomplished only through great effort and expense. The engineering effort required to devise effective security measures (not to mention the cost and power consumption of cryptographic controls) may exceed the effort required to design many digital radio devices made today. A likely outcome is that software security mechanisms implemented in compliance with the proposed rules will prove ineffective and a waste of effort.

Great Scott Gadgets designs and manufactures Open Source Hardware (OSHW). The OSHW community includes a small but rapidly growing segment of the electronics industry that is committed to the ideals that end users have a right to fully control their own equipment and that anyone should be able to study, make, use, modify, and sell devices based

on our published designs. OSHW makers recognize that, just as Open Source Software has resulted in great advances in the software industry, Open Source Hardware will enable future generations of hardware innovation.

As an OSHW designer, I have often been troubled by the Commission's rules for SDR. Great Scott Gadgets manufactures and sells HackRF One, an open source SDR platform popular for research and education. HackRF One is sold as test equipment, making it exempt from equipment authorization. As Open Source Hardware, however, it is a design that may be modified and sold by anyone. If someone were to use HackRF One as the basis for more specialized open source radio equipment that is not subject to the test equipment exemption, this new equipment would require authorization and would be subject to software security requirements that are incompatible with the open source license. We cannot grant open source licenses to users while locking out those same users.

This fundamental incompatibility with open source licensing greatly concerns me. The software security requirements, now that they will apply to non-SDR devices under the proposed rules, will adversely impact not just designers and users of Open Source Hardware but anyone making or using Open Source Software with any radio equipment. Today innovation is stifled by rules that make it difficult or impossible to sell OSHW SDR devices that are anything other than test equipment. Under the proposed rules, even more innovation will be curtailed.

I urge you to eliminate the software security requirements for both SDR and non-SDR equipment.

Additionally I am concerned about the proposal to grant automatic long-term confidentiality to certain types of exhibits. The Commission's Equipment Authorization database is a great public resource that is better protected by the existing rule that grants long-term confidentiality only upon request.

Thank you for inviting comments on the proposed rules for Equipment Authorization and Electronic Labeling for Wireless Devices.

I am the owner of Great Scott Gadgets, a US company that makes open source test equipment primarily for the information security industry. As a designer and manufacturer of communications equipment, I commend the Commission for seeking to clarify and streamline the rules for equipment authorization. I believe that, on the whole, the updated rules will benefit the electronics industry. However, I am concerned that the rules regarding software control of radio parameters place an undue burden on device manufacturers and unnecessarily restrict the actions of end users.

My concerns arise from rules already in place for Software Defined Radio (SDR) devices. I am encouraged to see that the Commission is eliminating certain special rules for SDR equipment and seeks to treat SDR and non-SDR devices in the same way. However, while the Commission notes that "the existing SDR rules have proven to be insufficiently flexible," the proposed rules broaden the reach of those rules to non-SDR equipment.

The requirement to implement security measures preventing the modification of software has long been unpopular in the SDR community. Software security is difficult, expensive, and unreliable, and it undermines reconfigurability, a principal benefit of SDR. The proposed rules extend this absurd requirement to all radio equipment with any software control, encompassing most radio devices manufactured today.

Under the proposed rules, all radio device manufacturers would be required to devise software security mechanisms that do not exist today, and they would have to prepare for each new device software documentation that is currently not required. Makers of integrated circuits would have to develop entirely new product lines that provide device manufacturers with security mechanisms, killing off existing product lines that lack such controls.

These requirements seem particularly onerous when considering the fact that computer security is largely an unsolved problem. Where manufacturers have had limited success preventing modification of software in electronic devices (e.g. in mobile phones), it has been accomplished only through great effort and expense. The engineering effort required to devise effective security measures (not to mention the cost and power consumption of cryptographic controls) may exceed the effort required to design many digital radio devices made today. A likely outcome is that software security mechanisms implemented in compliance with the proposed rules will prove ineffective and a waste of effort.

Great Scott Gadgets designs and manufactures Open Source Hardware (OSHW). The OSHW community includes a small but rapidly growing segment of the electronics industry that is committed to the ideals that end users have a right to fully control their own equipment and that anyone should be able to study, make, use, modify, and sell devices based on our published designs. OSHW makers recognize that, just as Open Source Software has resulted in great advances in the software industry, Open Source Hardware will enable future generations of hardware innovation.

As an OSHW designer, I have often been troubled by the Commission's rules for SDR. Great Scott Gadgets manufactures and sells HackRF One, an open source SDR platform popular for research and education. HackRF One is sold as test equipment, making it exempt from equipment authorization. As Open Source Hardware, however, it is a design that may be modified and sold by anyone. If someone were to use HackRF One as the basis for more specialized open source radio equipment that is not subject to the test equipment exemption, this new equipment would require authorization and would be subject to software security requirements that are incompatible with the open source license. We cannot grant open source licenses to users while locking out those same users.

This fundamental incompatibility with open source licensing greatly concerns me. The software security requirements, now that they will apply to non-SDR devices under the proposed rules, will adversely impact not just designers and users of Open Source Hardware but anyone making or using Open Source Software with any radio equipment. Today innovation is stifled by rules that make it difficult or impossible to sell OSHW SDR devices that are anything other than test equipment. Under the proposed rules, even more innovation will be curtailed.

I urge you to eliminate the software security requirements for both SDR and non-SDR equipment.

Additionally I am concerned about the proposal to grant automatic long-term confidentiality to certain types of exhibits. The Commission's Equipment Authorization database is a great public resource that is better protected by the existing rule that grants long-term confidentiality only upon request.

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: Jarrett

Last Name: bolander

Mailing Address: 329 Bledsoe - TTU

City: Lubbock

Country: United States

State or Province: TX

ZIP/Postal Code: 79406-0016

Email Address:

Organization Name:

Comment: I would like to ask the FCC not to implement the proposal as the ability use alternative software created by other communities should be considered an important freedom

I would like to ask the FCC not to implement the proposal as the ability use alternative software created by other communities should be considered an important freedom

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: Ramsell

Mailing Address: 2450 Airport Rd, Apt A101

City: Longmont

Country: United States

State or Province: CO

ZIP/Postal Code: 80503

Email Address:

Organization Name:

Comment: The FCC proposal is not a free market proposal and does not provide any benefit to users. In fact the proposal makes networking less secure by not allowing updates that are useful. At this time software exists to fix the problems that manufactures refuse to fix. The FCC proposal would make that impossible. The proposal will also make manufactures less likely to fix any broken software.

The FCC proposal is not a free market proposal and does not provide any benefit to users. In fact the proposal makes networking less secure by not allowing updates that are useful. At this time software exists to fix the problems that manufactures refuse to fix. The FCC proposal would make that impossible. The proposal will also make manufactures less likely to fix any broken 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: Nigel

Last Name: Armstrong

Mailing Address: 7 Hunt Wood Dr

City: Poquoson

Country: United States

State or Province: VA

ZIP/Postal Code: 23662

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Rick

Last Name: James

Mailing Address: 14938 Moorpark St

City: Sherman Oaks

Country: United States

State or Province: CA

ZIP/Postal Code: 91403

Email Address:

Organization Name:

Comment: This rulemaking proposal fails the public in a few areas.

The first of which is that it will increase the number of wifi devices in landfills. Hardware makers aren't incentivized in any fashion to patch their devices; they make money on selling customers new hardware, not patching existing devices. So customers will have to buy new to get what should've been a mere software update. (Think: Heartbleed and Shellshock vulnerabilities.)

The second is security. Combined with the above disincentives towards patching, many customers will simply run old firmware because they can't afford to buy a new router every 2 years to ensure the hardware manufacturers' profit margins are sustained. As a result, having millions of out-of-date wifi devices on the internet creates a security nightmare. ((Again, think: Heartbleed and Shellshock vulnerabilities.)

These problems hit lower income families hardest, since less expensive routers typically have worse support problems. Expecting your ISP to "Rent" you a device is also, in the long run, way more expensive for almost no benefit to the consumer.

With like likes of DD-WRT, OpenWRT, Tomato, etc., many of these older routers can get a new lease on life, avoid the land fill, and keep their users more secure. Everyone wins here, and I'm going to hazard a guess that less than 1/10 1% of firmware users are even willing to adjust settings related to radio power and frequency beyond the defaults. (Almost no one clicks "advanced" on any UI.)

As someone who's primary router is an old WRT-54GL made in 2006 (and hasn't seen an update from Linksys since 2008) running DD-WRT (updated earlier this year), I feel this kind of legislation is likely to make me have to buy new hardware where it isn't warranted, or worse, keep old hardware in service long after its useful life has ended, to avoid new DRM.

Please help keep Americans more secure, and keep less waste from going into our landfills (or exporting it to China).

This rulemaking proposal fails the public in a few areas.

The first of which is that it will increase the number of wifi devices in landfills. Hardware makers aren't incentivized in any fashion to patch their devices; they make money on selling customers new hardware, not patching existing devices. So customers will have to buy new to get what should've been a mere software update. (Think: Heartbleed and Shellshock vulnerabilities.)

The second is security. Combined with the above disincentives towards patching, many customers will simply run old firmware because they can't afford to buy a new router every 2 years to ensure the hardware manufacturers' profit margins are sustained. As a result, having millions of out-of-date wifi devices on the internet creates a security nightmare. ((Again, think: Heartbleed and Shellshock vulnerabilities.)

These problems hit lower income families hardest, since less expensive routers typically have worse support problems. Expecting your ISP to "Rent" you a device is also, in the long run, way more expensive for almost no benefit to the consumer.

With like likes of DD-WRT, OpenWRT, Tomato, etc., many of these older routers can get a new lease on life, avoid the land fill, and keep their users more secure. Everyone wins here, and I'm going to hazard a guess that less than 1/10 1% of firmware users are even willing to adjust settings related to radio power and frequency beyond the defaults. (Almost no one clicks "advanced" on any UI.)

As someone who's primary router is an old WRT-54GL made in 2006 (and hasn't seen an update from Linksys since 2008) running DD-WRT (updated earlier this year), I feel this kind of legislation is likely to make me have to buy new hardware where it isn't warranted, or worse, keep old hardware in service long after its useful life has ended, to avoid new DRM.

Please help keep Americans more secure, and keep less waste from going into our landfills (or exporting it to China).

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: Quentin

Last Name: Dai

Mailing Address: impasse gance

City: montpellier

Country: France

State or Province: languedoc roussillon

ZIP/Postal Code: 34000

Email Address: kwentino@gmail.com

Organization Name:

Comment: This is a very wrong idea for our own safety. Firmwares are made to be updated.

What a mess it would be without it!

This is a very wrong idea for our own safety. Firmwares are made to be updated.

What a mess it would be without it!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joshua

Last Name: Titus

Mailing Address: 927 Ocaso Ln Unit 205

City: Rockledge

Country: United States

State or Province: FL

ZIP/Postal Code: 32955

Email Address: jjtitus@umich.edu

Organization Name:

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

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

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

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

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

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Please consider these negative consequences of the current legislation. Security disguised by loss of freedom is not safety.

Thank you,

Joshua

Please do not implement rules that take away the ability of users to install the software of their choosing on their personal computing devices.

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

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

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

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

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Please consider these negative consequences of the current legislation. Security disguised by loss of freedom is not safety.

Thank you,

Joshua

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: Edmonds

Mailing Address: 317 30th Street

City: Springfield

Country: United States

State or Province: OR

ZIP/Postal Code: 97478

Email Address:

Organization Name:

Comment: How is this even up for consideration? Why do we, consumers and creators alike, have to keep reiterating to every part of the technology sector that we want control over the hardware we own?

We shouted about it when the legality of jailbreaking phones was called into question. We shouted about it before that when the legality of reverse engineering was called into question. Now modifying the software controlling radios is on the chopping block. Seriously?

I'm even going to go into how detrimental this will be for free software, open source development, and computer security. Those problems are real, they're severe, and they're infuriatingly obvious. But they're not why I'm angry.

I'm angry because I want to control my own damn computer. How is this a complicated concept?

I want to know that the code running on my router has the fewest security holes possible, especially after the original manufacturer stops releasing firmware updates. I want to know that my phone isn't phoning home to some server in another country with personal information about me. I want to know that my laptop is running the most efficient OS possible, without any extra flashy bits tacked on that I don't need.

I can't do any of that, with hardware I bought and maintain myself in my own home, if you turn all computer radios into black boxes into which I can't peek under penalty of law!

How is this even up for consideration? Why do we, consumers and creators alike, have to keep reiterating to every part of the technology sector that we want control over the hardware we own?

We shouted about it when the legality of jailbreaking phones was called into question. We shouted about it before that when the legality of reverse engineering was called into question. Now modifying the software controlling radios is on the chopping block. Seriously?

I'm even going to go into how detrimental this will be for free software, open source development, and computer security. Those problems are real, they're severe, and they're infuriatingly obvious. But they're not why I'm angry.

I'm angry because I want to control my own damn computer. How is this a complicated concept?

I want to know that the code running on my router has the fewest security holes possible, especially after the original manufacturer stops releasing firmware updates. I want to know that my phone isn't phoning home to some server in

another country with personal information about me. I want to know that my laptop is running the most efficient OS possible, without any extra flashy bits tacked on that I don't need.

I can't do any of that, with hardware I bought and maintain myself in my own home, if you turn all computer radios into black boxes into which I can't peek under penalty of law!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Campbell

Mailing Address: 5552 Beacon St, #2

City: Pittsburgh

Country: United States

State or Province: PA

ZIP/Postal Code: 15217

Email Address: jdc_fcccomment@introrse.com

Organization Name: Microak Systems

Comment: Notice of Proposed Rulemaking 15-92 describes proposed changes to wireless device certification procedures intended to streamline approvals while locking down modular and software-defined-radios in devices.

Locking down modular radios is a mistake, even though device approval rules do need streamlining. The proposed rules should undergo further revision.

1. Current device certification is onerous. The costs for certifying a new device, even one based on previously certified reference designs or a previously certified older model, can run to \$20,000 or more. Developers of new devices, especially small businesses and those serving niche and nascent markets, are at a disadvantage in marking those devices in the US. US innovators find it costly to bring new types of devices to market. US consumers suffer reduced device availability because of device certification costs. Even at the risk of limited additional unwanted interference the device certification process should be simplified and streamlined.

2. Software innovation should be unlocked from hardware: To ensure a free market, device owners must have a right to use a purchased piece of hardware in any compliant way they wish, including reflashing or updating the device's software. Prohibiting such software changes, or requiring vendor control of them, has long been a tool monopolists have used to inhibit innovation and control device ecosystems. Consider mainframe and minicomputer systems, which were rapidly eclipsed by the incredibly fast development of open-standards-based computing where many software vendors could supply operating systems and applications for a wide variety of devices. Separating software from hardware has served far more people and created far more jobs than binding them together would have.

Therefore:

* The commission should not mandate mechanisms which lead to de-facto monopolies.

* The commission should not mandate mechanisms which tie hardware to software.

* The commission should recognize the importance of competition and innovation for device software per se and require device hardware manufacturers to publically document necessary interfaces and features so that 3rd parties can build rules-compliant alternative software loads for ALL devices. This would lead to competitive software markets for currently evolving types of hardware and devices such as the Internet of Things and smart phones, as well as accelerate innovation overall.

3. Open Source development should be encouraged: Free and open-source software development has been at the core of the incredibly rapid innovation of Internet services, and provides essential pieces for companies and individuals creating secure, performant, interoperable systems today. This is only logical because as device complexity and interoperability requirements grow, no single entity can afford to create a software stack from scratch. Vendor software is also frequently buggy, nonperformant, noncompliant, or non-interoperable and needs replacement.

Open source alternatives have frequently proven able to fix such issues with existing wireless devices (see OpenWRT, Tomato, DD-WRT, etc). The commission should explicitly encourage open source software development. Only by doing so will our bold new world of internet devices not open a vast can of new vulnerabilities, privacy disasters, siloed innovation, and catastrophic hacks.

Notice of Proposed Rulemaking 15-92 describes proposed changes to wireless device certification procedures intended to streamline approvals while locking down modular and software-defined-radios in devices.

Locking down modular radios is a mistake, even though device approval rules do need streamlining. The proposed rules should undergo further revision.

1. Current device certification is onerous. The costs for certifying a new device, even one based on previously certified reference designs or a previously certified older model, can run to \$20,000 or more. Developers of new devices, especially small businesses and those serving niche and nascent markets, are at a disadvantage in marking those devices in the US. US innovators find it costly to bring new types of devices to market. US consumers suffer reduced device availability because of device certification costs. Even at the risk of limited additional unwanted interference the device certification process should be simplified and streamlined.

2. Software innovation should be unlocked from hardware: To ensure a free market, device owners must have a right to use a purchased piece of hardware in any compliant way they wish, including reflashing or updating the device's software. Prohibiting such software changes, or requiring vendor control of them, has long been a tool monopolists have used to inhibit innovation and control device ecosystems. Consider mainframe and minicomputer systems, which were rapidly eclipsed by the incredibly fast development of open-standards-based computing where many software vendors could supply operating systems and applications for a wide variety of devices. Separating software from hardware has served far more people and created far more jobs than binding them together would have.

Therefore:

* The commission should not mandate mechanisms which lead to de-facto monopolies.

* The commission should not mandate mechanisms which tie hardware to software.

* The commission should recognize the importance of competition and innovation for device software per se and require device hardware manufacturers to publically document necessary interfaces and features so that 3rd parties can build rules-compliant alternative software loads for ALL devices. This would lead to competitive software markets for currently evolving types of hardware and devices such as the Internet of Things and smart phones, as well as accelerate innovation overall.

3. Open Source development should be encouraged: Free and open-source software development has been at the core of the incredibly rapid innovation of Internet services, and provides essential pieces for companies and individuals creating secure, performant, interoperable systems today. This is only logical because as device complexity and interoperability requirements grow, no single entity can afford to create a software stack from scratch. Vendor software is also frequently buggy, nonperformant, noncompliant, or non-interoperable and needs replacement.

Open source alternatives have frequently proven able to fix such issues with existing wireless devices (see OpenWRT,

Tomato, DD-WRT, etc). The commission should explicitly encourage open source software development. Only by doing so will our bold new world of internet devices not open a vast can of new vulnerabilities, privacy disasters, siloed innovation, and catastrophic hacks.

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: William

Last Name: Fischer

Mailing Address: 1055 Kelwyn Ln.

City: Lewisville

Country: United States

State or Province: NC

ZIP/Postal Code: 27023

Email Address:

Organization Name:

Comment: I understand the need to make sure software defined radios do not have the firmware changed in a way that could create interference. The current wording makes it sound like the firmware for any device that has a radio will need to be locked down. This goes against the FCC comments that recognizes that users should own the devices they pay for. For example, users should be able to unlock their cell phones. There are also many reasons to change the firmware of wireless routers which can increase user control over quality of service functions, monitoring functions, and other things that increase usability without making changes to the transmission power of the radio. If you absolutely need something in addition to current laws against causing interference, I would prefer you put that responsibility on the user who actually owns the device. If this has to be controlled at the time on manufacture, then you should require that software defined radios have their own firmware stored in memory that is in a separate device from the rest of the system firmware. This could add some complexity to the design (assuming the manufacture isn't already using a module for the RF sections), but it allows users to control the devices firmware while still allowing the radio firmware to be locked down. This still isn't preferred since it would prevent users from updating firmware that fixes bugs in a radios software.

I understand the need to make sure software defined radios do not have the firmware changed in a way that could create interference. The current wording makes it sound like the firmware for any device that has a radio will need to be locked down. This goes against the FCC comments that recognizes that users should own the devices they pay for. For example, users should be able to unlock their cell phones. There are also many reasons to change the firmware of wireless routers which can increase user control over quality of service functions, monitoring functions, and other things that increase usability without making changes to the transmission power of the radio. If you absolutely need something in addition to current laws against causing interference, I would prefer you put that responsibility on the user who actually owns the device. If this has to be controlled at the time on manufacture, then you should require that software defined radios have their own firmware stored in memory that is in a separate device from the rest of the system firmware. This could add some complexity to the design (assuming the manufacture isn't already using a module for the RF sections), but it allows users to control the devices firmware while still allowing the radio firmware to be locked down. This still isn't preferred since it would prevent users from updating firmware that fixes bugs in a radios 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: Kress

Last Name: Franzen

Mailing Address: 4 Witham Farm Rd

City: Greenland

Country: United States

State or Province: NH

ZIP/Postal Code: 03840

Email Address:

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on computing devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses not to do so. Even in the last 12 months, there have been major security flaws with consumer-grade devices, and there is no economic incentive for these manufacturers to correct such issues; in fact, the incentives are strong for them NOT to fix such issues. Government-mandated DRM will likely exacerbate the challenges facing consumers, and the cost of implementing and enforcing such a law will be excessive. Additionally, wireless networking research depends on the ability of researchers to investigate and modify their devices. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Please do not implement rules that take away the ability of users to install the software of their choosing on computing devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses not to do so. Even in the last 12 months, there have been major security flaws with consumer-grade devices, and there is no economic incentive for these manufacturers to correct such issues; in fact, the incentives are strong for them NOT to fix such issues. Government-mandated DRM will likely exacerbate the challenges facing consumers, and the cost of implementing and enforcing such a law will be excessive. Additionally, wireless networking research depends on the ability of researchers to investigate and modify their devices. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

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: Dominic

Last Name: Corriveau

Mailing Address: 9233 E. Neville Ave.

City: Mesa

Country: United States

State or Province: AZ

ZIP/Postal Code: 85209

Email Address:

Organization Name:

Comment: This proposed rule should be blocked from proceeding. Manufacturers of router firmware for consumer products are woefully insecure and rarely maintained by the manufacturer. Allowing consumers to modify the firmware using open-source tools available. Tools such as IPFire, PFSense, DD-WRT, Gargoyle and Tomato are essential for enthusiasts and small businesses to maintain consistent, safe connections to the internet and keeping the security for their network in their hands.

Additionally, many small businesses have formed around offering these open-source tools for consumers on networking equipment. This regulation will chill the growing market of offering secure networking for those who do not have enterprise budgets, but would like enterprise tools.

This regulation will not kill the market for open-source firmware, but will require users to take more drastic action to obtain the firmware. We cannot rely on the manufacturers to keep consumers best interest in mind. They have proven over the last decade that the firmware provided on their networking equipment is an embarrassment for the security conscience consumer and small business owner.

Please block this proposed rule.

This proposed rule should be blocked from proceeding. Manufacturers of router firmware for consumer products are woefully insecure and rarely maintained by the manufacturer. Allowing consumers to modify the firmware using open-source tools available. Tools such as IPFire, PFSense, DD-WRT, Gargoyle and Tomato are essential for enthusiasts and small businesses to maintain consistent, safe connections to the internet and keeping the security for their network in their hands.

Additionally, many small businesses have formed around offering these open-source tools for consumers on networking equipment. This regulation will chill the growing market of offering secure networking for those who do not have enterprise budgets, but would like enterprise tools.

This regulation will not kill the market for open-source firmware, but will require users to take more drastic action to obtain the firmware. We cannot rely on the manufacturers to keep consumers best interest in mind. They have proven over the last decade that the firmware provided on their networking equipment is an embarrassment for the security conscience consumer and small business owner.

Please block this proposed rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Blake

Last Name: VandeMerwe

Mailing Address: 438 West 1360 North

City: American Fork

Country: United States

State or Province: UT

ZIP/Postal Code: 84003

Email Address: blakev@null.net

Organization Name: Blake VandeMerwe

Comment: I do not support locking in firmware/software for devices I've purchased.

I think this is a bad idea and cannot support it.

I do not support locking in firmware/software for devices I've purchased.

I think this is a bad idea and cannot support it.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Cole

Last Name: Renard

Mailing Address: 11133 189th St. N.

City: Marine on St. Croix

Country: United States

State or Province: MN

ZIP/Postal Code: 55047

Email Address: crenard55@gmail.com

Organization Name:

Comment: Locking down wireless technology prevents users from investigating security holes in their wireless devices.

Having the manufacturer have control over a wireless device can pose a security threat just as high as the reasons for this fcc proposal by allowing them to put monitoring or hacking software into their devices.

Keeping the ability to have these devices be open source is what high security and innovation thrive on. Without modification to these devices, loopholes could be undetected for longer.

Locking down wireless technology prevents users from investigating security holes in their wireless devices.

Having the manufacturer have control over a wireless device can pose a security threat just as high as the reasons for this fcc proposal by allowing them to put monitoring or hacking software into their devices.

Keeping the ability to have these devices be open source is what high security and innovation thrive on. Without modification to these devices, loopholes could be undetected for longer.

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: Brandyn

Last Name: Aldag

Mailing Address: 52188 30th Ave

City: Bangor

Country: United States

State or Province: MI

ZIP/Postal Code: 49013

Email Address: djofba@gmail.com

Organization Name:

Comment: This is respectful request, asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices, which will ultimately aid the FCC in keeping users within radio frequency regulation.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so, as this protects their right to liberty and security of person.

Private sers 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.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

In conclusion, this regulation would stifle innovation, make us less secure, and set back innovation in the United States decades, and would likely do little to deter or prevent cybercrime or the violation of Federal regulations.

This is respectful request, asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices, which will ultimately aid the FCC in keeping users within radio frequency regulation.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so, as this protects their right to liberty and security of person.

Private sers 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.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

In conclusion, this regulation would stifle innovation, make us less secure, and set back innovation in the United States decades, and would likely do little to deter or prevent cybercrime or the violation of Federal regulations.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Thomas

Last Name: Loredo

Mailing Address: 1030 Coddington Rd

City: Ithaca

Country: United States

State or Province: NY

ZIP/Postal Code: 14850

Email Address: loredo@museweb.com

Organization Name:

Comment: I urge the FCC not to implement rules that prevent consumers from installing software of their own choosing on computing equipment they have purchased.

For the specific area targeted here, the rules will unnecessarily and harmfully limit research and innovation regarding WiFi technology.

In addition, when manufacturers choose to stop updating equipment, or go out of business, the rules will prevent consumers from keeping purchased equipment from operating safely. This is particularly important regarding security updates, which can impact not only the owner of a computing device, but also the networked public that may be targeted by individuals or groups exploiting out-of-date software and firmware.

I am also deeply concerned about the precedent these rules would set regarding consumer control of computing products they have purchased in settings more general than wireless devices.

I urge the FCC not to implement rules that prevent consumers from installing software of their own choosing on computing equipment they have purchased.

For the specific area targeted here, the rules will unnecessarily and harmfully limit research and innovation regarding WiFi technology.

In addition, when manufacturers choose to stop updating equipment, or go out of business, the rules will prevent consumers from keeping purchased equipment from operating safely. This is particularly important regarding security updates, which can impact not only the owner of a computing device, but also the networked public that may be targeted by individuals or groups exploiting out-of-date software and firmware.

I am also deeply concerned about the precedent these rules would set regarding consumer control of computing products they have purchased in settings more general than wireless 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: Russell

Last Name: Senior

Mailing Address: P.O. Box 12314

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97212

Email Address: president@personaltelco.net

Organization Name: Personal Telco Project

Comment: I use alternative software on commodity wifi routers every day. My work, both paid and volunteer depends on my ability to build and install my own custom and shared software on these devices. From building manageable wifi hot spots, to research-enabling telemetry systems, to community mesh networks, to model train controllers. Others, like me, non-authorized modifiers, are actually developing and building the software that increasingly manufacturers ship to makes these devices useful. This proposed rule, unreasonably dichotomizes people and organizations into "producers" and "consumers". This in not a tenable position any longer. People will need to adapt the software on devices to their needs, because the market place of manufacturers is incapable of satisfying these needs.

No one, in my experience, builds these non-authorized softwares in order to violate FCC rules. They build non-authorized software to solve their particular practical problems. In the attempt to foreclose the infinitesimal possibility of FCC rule violation, you cut off the rather prominent and significant nose that makes wifi routers useful to many, many people.

The rule, insofar as it obstructs users from building solutions on devices they buy, is nonsensical and needs a complete rethink in light of these realities.

I use alternative software on commodity wifi routers every day. My work, both paid and volunteer depends on my ability to build and install my own custom and shared software on these devices. From building manageable wifi hot spots, to research-enabling telemetry systems, to community mesh networks, to model train controllers. Others, like me, non-authorized modifiers, are actually developing and building the software that increasingly manufacturers ship to makes these devices useful. This proposed rule, unreasonably dichotomizes people and organizations into "producers" and "consumers". This in not a tenable position any longer. People will need to adapt the software on devices to their needs, because the market place of manufacturers is incapable of satisfying these needs.

No one, in my experience, builds these non-authorized softwares in order to violate FCC rules. They build non-authorized software to solve their particular practical problems. In the attempt to foreclose the infinitesimal possibility of FCC rule violation, you cut off the rather prominent and significant nose that makes wifi routers useful to many, many people.

The rule, insofar as it obstructs users from building solutions on devices they buy, is nonsensical and needs a complete rethink in light of these realities.

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: lutz

Last Name: rak

Mailing Address: lutz-th@gmx.de

City: gera

Country: Germany

State or Province: Thringen

ZIP/Postal Code: 07549

Email Address: lutz-th@gmx.de

Organization Name: null

Comment: Hallo, was sie hiermit vorhaben ist ein Angriff auf die freie Software!! Ich werde mich deshalb auch an die Parteien in Deutschland und an das EU Parlament wenden, um dieses in Europa zu verhindern. Weiterhin werde ich in Deutschland dieses auch an die Presse und das Fernsehen weiterleiten.

MfG

Lutz Rak

Hallo, was sie hiermit vorhaben ist ein Angriff auf die freie Software!! Ich werde mich deshalb auch an die Parteien in Deutschland und an das EU Parlament wenden, um dieses in Europa zu verhindern. Weiterhin werde ich in Deutschland dieses auch an die Presse und das Fernsehen weiterleiten.

MfG

Lutz Rak

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matt

Last Name: Price

Mailing Address: 111 Clifford Terrace

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94117

Email Address: matt.price@utoronto.ca

Organization Name:

Comment: This is a terrible idea. I have reflashed all my wireless routers for the last 8 years or so, overcoming deficits in the stock firmware and producing a much more stable home network than the original firmware provided. This regulation would make that impossible!

This is a terrible idea. I have reflashed all my wireless routers for the last 8 years or so, overcoming deficits in the stock firmware and producing a much more stable home network than the original firmware provided. This regulation would make that impossible!

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: Derek

Last Name: Escue

Mailing Address: 2262 Commerce Dr, , AR 72401

City: Jonesboro

Country: United States

State or Province: AR

ZIP/Postal Code: 72401

Email Address: descue@techfriends.com

Organization Name: Software Company

Comment: Respectfully,

The company I work for, Tech Friends, Inc., provides services to correctional institutions around the nation. Security is an extremely high concern for these facilities. We use a custom firmware for our routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

Respectfully,

The company I work for, Tech Friends, Inc., provides services to correctional institutions around the nation. Security is an extremely high concern for these facilities. We use a custom firmware for our routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

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: Gwendhal

Last Name: CLAUDEL

Mailing Address: gwendhalclaudel@gmail.com

City: La Saline Les Bains

Country: France

State or Province: RUNION

ZIP/Postal Code: 97434

Email Address: gwendhalclaudel@gmail.com

Organization Name:

Comment: DON'T DO THAT!!! How many leaks did we find on official devices? Too much.

Plus when I buy something, I like to think that it's completely MINE. And if I want an opensource firmware on my android? I downloaded Cyanogenmode on my GT I93000 because my phone was too slow after a month of use. A year after, my android is still fast. I've got plenty examples of devices which works better after a flash, just ask me (in french please, as you can see, my English is not so good...).

Have a good day and PLEASE don't do that, it's stupid.

P.S: Here is an article (in french sorry) of the wireless hard drive seagate which has a critical leak.

<http://korben.info/grosse-faille-dans-les-disques-durs-sans-fil-seagate.html>

DON'T DO THAT!!! How many leaks did we find on official devices? Too much.

Plus when I buy something, I like to think that it's completely MINE. And if I want an opensource firmware on my android? I downloaded Cyanogenmode on my GT I93000 because my phone was too slow after a month of use. A year after, my android is still fast. I've got plenty examples of devices which works better after a flash, just ask me (in french please, as you can see, my English is not so good...).

Have a good day and PLEASE don't do that, it's stupid.

P.S: Here is an article (in french sorry) of the wireless hard drive seagate which has a critical leak.

<http://korben.info/grosse-faille-dans-les-disques-durs-sans-fil-seagate.html>

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: Marc

Last Name: Lefebvre

Mailing Address: 79 Sauerman Rd

City: Doylestown

Country: United States

State or Province: PA

ZIP/Postal Code: 18901

Email Address:

Organization Name:

Comment: As an IT Professional I think this is a very bad idea for the following reasons:

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

As an IT Professional I think this is a very bad idea for the following reasons:

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

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: Brown

Mailing Address: 741 N 3rd St.

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95112

Email Address:

Organization Name:

Comment: Prohibiting individuals from install open source and free software on their own hardware, including retail wifi routers and access points, is completely unacceptable. The solution is **not** to limit vendors from permitting new firmware to be burned into their hardware, including individuals installing custom firmware. Rather, the solution is to limit the power of the radio signals, if necessary -- nothing more.

Stopping individuals from installing or customizing or programming their own software will only open the floodgates to custom "routers" which are even more powerful and even more intrusive. Preventing people from playing around only with over-the-counter hardware is definitely not the answer.

Prohibiting individuals from install open source and free software on their own hardware, including retail wifi routers and access points, is completely unacceptable. The solution is **not** to limit vendors from permitting new firmware to be burned into their hardware, including individuals installing custom firmware. Rather, the solution is to limit the power of the radio signals, if necessary -- nothing more.

Stopping individuals from installing or customizing or programming their own software will only open the floodgates to custom "routers" which are even more powerful and even more intrusive. Preventing people from playing around only with over-the-counter hardware is definitely not the answer.

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: Eric

Last Name: Brown

Mailing Address: 13810 Sutton Park Drive #929

City: Jacksonville

Country: United States

State or Province: FL

ZIP/Postal Code: 32224

Email Address: ericsb@live.com

Organization Name:

Comment: After reading the proposed rules, my biggest concern is this has the real ability to completely change how the free market works. A real nasty potentially unforeseen impact this could have is it could go as far as to render an operating system like Linux illegal as users have the ability to alter it in such a way that it crosses into grey areas of this rule. This also has the potential to impact users of device that allow deep levels of customization (For example Google Android devices).

This new rule is deeply concerning and I believe it needs to be better defined and the public needs to be more engaged and made aware of possible implications this rule has on them.

After reading the proposed rules, my biggest concern is this has the real ability to completely change how the free market works. A real nasty potentially unforeseen impact this could have is it could go as far as to render an operating system like Linux illegal as users have the ability to alter it in such a way that it crosses into grey areas of this rule. This also has the potential to impact users of device that allow deep levels of customization (For example Google Android devices).

This new rule is deeply concerning and I believe it needs to be better defined and the public needs to be more engaged and made aware of possible implications this rule has on them.

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: Julien-Benjamin

Last Name: RUIZ

Mailing Address: 40 Chemin de la Salade Ponsan

City: Toulouse

Country: France

State or Province: Midi-Pyrnes

ZIP/Postal Code: 31400

Email Address: julienbenjamin.ruiz@gmail.com

Organization Name: CNES

Comment: Good afternoon,

It seems you would like to lock every WiFi device down ? Have you really a deep understandings of the consequences for the future, for the hardware and software industry ? By nature, you are forbidding opensource hardware and software as soon as it is linked to WiFi. And this example was just one among a lot of others... As, nowadays, every single and simple device embedded a WiFi chip, basically, you are involving the whole current and future high-technology devices.

Your motivations seem to be quite useless, and much more, as soon as you compare these to their consequences.

I would like you to think a little more about it before trying to regulate this type of subject.

I also would happily hear from you about what you think.

Best regards,

Julien-Benjamin RUIZ

Good afternoon,

It seems you would like to lock every WiFi device down ? Have you really a deep understandings of the consequences for the future, for the hardware and software industry ? By nature, you are forbidding opensource hardware and software as soon as it is linked to WiFi. And this example was just one among a lot of others... As, nowadays, every single and simple device embedded a WiFi chip, basically, you are involving the whole current and future high-technology devices.

Your motivations seem to be quite useless, and much more, as soon as you compare these to their consequences.

I would like you to think a little more about it before trying to regulate this type of subject.

I also would happily hear from you about what you think.

Best regards,

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matthew

Last Name: Lorence

Mailing Address: 474 Route 7 South

City: Milton

Country: United States

State or Province: VT

ZIP/Postal Code: 05468

Email Address: mlorence@gmail.com

Organization Name:

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

By restricting access to the software contained within our wireless devices, the FCC would be restricting the ability of users to patch security risks that manufacturers choose not to address which may increase our risk of cyber threats.

Additionally, the FCC will be stifling innovation coming from the open source world.

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

By restricting access to the software contained within our wireless devices, the FCC would be restricting the ability of users to patch security risks that manufacturers choose not to address which may increase our risk of cyber threats.

Additionally, the FCC will be stifling innovation coming from the open source world.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Matt

Last Name: Ciderby

Mailing Address: [N/A]

City: [N/A]

Country: United States

State or Province: MA

ZIP/Postal Code: [N/A]

Email Address: mat.cider@gmail.com

Organization Name: Project Ascension

Comment: This is an actual affront to consumer liberty. As someone who works with budget projects for schools in under-funded areas, I rely on turning cheap routers into ones that can support a network by physical and software modification.

By disallowing people to flash new software to routers, not only are you asking to have it worked around which works backwards for your goal, but also you are depriving people of the right to use a product as they see fit.

Hypothetically, manufacturers have the right to do this on their own, but most know that this is a PR suicide. Users who don't care would not notice anyway, but those who do care about it are the ones doing the flashing.

I have read through this proposal and would have to say that if brought before a court, I believe it would be found to be vastly unconstitutional. Regulations about use of products is a hard thing to pass through the eyes of the court, especially with the current set of rather originalist-leaning justices.

I have to say I am strongly opposed to this proposal, and hope that those who are the determining factor see the same.

This is an actual affront to consumer liberty. As someone who works with budget projects for schools in under-funded areas, I rely on turning cheap routers into ones that can support a network by physical and software modification.

By disallowing people to flash new software to routers, not only are you asking to have it worked around which works backwards for your goal, but also you are depriving people of the right to use a product as they see fit.

Hypothetically, manufacturers have the right to do this on their own, but most know that this is a PR suicide. Users who don't care would not notice anyway, but those who do care about it are the ones doing the flashing.

I have read through this proposal and would have to say that if brought before a court, I believe it would be found to be vastly unconstitutional. Regulations about use of products is a hard thing to pass through the eyes of the court, especially with the current set of rather originalist-leaning justices.

I have to say I am strongly opposed to this proposal, and hope that those who are the determining factor see the same.

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: Zach

Last Name: Villers

Mailing Address: 5597 Santiago Dr

City: Westerville

Country: United States

State or Province: OH

ZIP/Postal Code: 43081

Email Address: zachvatwork@gmail.com

Organization Name:

Comment: While controlling modification to equipment that broadcasts and communicates via RF is extremely important for public safety, limiting end-user and commercial ability to create, modify, and use custom firmware/software for small, low-power wifi devices is a significant threat to the security of our personal data and the ability for businesses to protect their financial and intellectual assests. Please consider re-wording this ruling so it does not impinge upon my personal digital freedom and security.

While controlling modification to equipment that broadcasts and communicates via RF is extremely important for public safety, limiting end-user and commercial ability to create, modify, and use custom firmware/software for small, low-power wifi devices is a significant threat to the security of our personal data and the ability for businesses to protect their financial and intellectual assests. Please consider re-wording this ruling so it does not impinge upon my personal digital freedom and 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: Drew

Last Name: Wings

Mailing Address: PO Box 503

City: Denver

Country: United States

State or Province: CO

ZIP/Postal Code: 80222

Email Address: champagnetony@gmail.com

Organization Name: null

Comment: I respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. 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. Additionally, it is completely insane to restrict what someone can do with items that they own. The whole nature of ownership has been attacked by corporate raiders who care nothing about our nation and only about their profits. This is a bad idea. Please do not restrict consumer rights.

I respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. 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. Additionally, it is completely insane to restrict what someone can do with items that they own. The whole nature of ownership has been attacked by corporate raiders who care nothing about our nation and only about their profits. This is a bad idea. Please do not restrict consumer rights.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jose

Last Name: Grullon

Mailing Address: 8737 NW 146th Lane

City: Miami Lakes

Country: United States

State or Province: FL

ZIP/Postal Code: 33018

Email Address: josefgrullon@gmail.com

Organization Name:

Comment: I hope you find it in your wisdom to not infringe upon our ability to modify hardware we already purchased.

Those technically inclined should not be stifled if they can find a better way for a device to work.

I hope you find it in your wisdom to not infringe upon our ability to modify hardware we already purchased. Those technically inclined should not be stifled if they can find a better way for a device to work.

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: Michaelson

Mailing Address: 112 Belmont Road

City: Apple Valley

Country: United States

State or Province: MN

ZIP/Postal Code: 55124-9713

Email Address: jasondmichaelson@gmail.com

Organization Name:

Comment: See attached file(s)

See attached file(s)

Regarding ET Docket No. 15-170; RM-11673

I was recently made aware of the proposed rule referenced in the above docket. This letter is a formal comment on that proposed rule, and due to the accessibility of the FCC IT infrastructure will be submitted both by mail and electronically as soon as the ability is restored.

Firstly, allow me to provide a little background information about myself. I received degrees in both Computer Science and Electrical Engineering from the University of Minnesota in 1999. I received an M.S. degree in Software Engineering in 2008, and am currently pursuing a PhD in Computer Science with an emphasis on security.

Given both my background, as well as personal reasons, the proposed rule is deeply concerning to me, for reasons to be described below. I certainly agree that the Federal Communications Commission has a legitimate interest in ensuring that the radios in wireless networking equipment operate within the parameters the Commission has authorized. However, I believe that the legitimate interest of the Commission can be served without measures such as disallowing the updating of the operating system, as the proposed rule has called out, namely by requiring the radio, either through its own standalone firmware or by settings embedded in the hardware.

The first concern I have is in fact from the perspective of security vulnerabilities. As vulnerabilities are found in the software that runs on wireless routers and access points, the manufacturers of those devices generally correct them by issuing new updates to the firmware. This is not, however always the case, particularly with older devices. Take for example the Linksys model WRT54G wireless router. Over the course of its lifetime, it has been through 12 different hardware revisions according to its support page on the Linksys web site. However, none of those versions has any updates available to the firmware anymore. At one point they did; I owned one at one time and kept the firmware updated regularly. These devices are incredibly resilient with the first versions being released in December 2002. My parents still have one of these devices.

The problem here seems apparent; this particular model is no longer supported, so although it still works great and serves its purpose, if a vulnerability is found with it, the only recourse to protect the network it serves is to replace the router. We know that the TJX breach that allowed millions of payment card numbers to be compromised in 2007 was a result of insecurities in the WiFi systems their payment terminals were connected to. While the 2013 data breach at Target was more the result of bad network security practices than WiFi insecurities, it could have just as easily been a result of WiFi problems.

For large retailers such as Target and TJX, this isn't a problem. If an insecure device isn't supported there's always a capital budget expenditure to be made to upgrade the hardware (no doubt to the cheering of the manufacturers). However, for the mom and pop Chinese restaurant down the street with the off-the-shelf router they bought to hook up to their cable modem or DSL line, the budget is probably not there.

Because of a lack of manufacturer support for older hardware, third-party firmware packages, such as DD-WRT (which was explicitly called out in the proposed rulemaking information, and which I am a widespread user of), are often the only choice for security updates to the router software¹. As worded, the proposed rule would prohibit users from maintaining good security practices on their networks.

Secondly, on devices for which the manufacturer does in fact provide firmware updates, it may take weeks or months for those vulnerability fixes to be released to the public. On the other hand, the version of DD-WRT I employ in my home network has fresh builds available typically weekly or more frequent if needed. While the Netgears and Ciscos of the world may take a couple of weeks to patch all their firmware against a vulnerability such as the 2014 Shellshock breach in the Unix Bash shell program (CVE-2014-6271), the third-party firmware community (as a result of being a subset of the open source software community) typically has the fix in place within hours, if not before it can even become an issue. The ability to mitigate broad security problems quickly would be outlawed if this proposed rule is adopted as is.

Third, manufacturer-provided firmware is designed to be as easy to use as possible. Since their typical user isn't necessarily a tech-savvy network administrator, this is understandable. The mom and pop Chinese restaurant wants to be able to plug in their computer, credit card terminal, maybe a Voice over IP phone or two, and other hardware and have it all just work. Maybe they want to provide free WiFi services to their customers while they dine. The typical firmware on off-the-shelf routers, for example, typically comes with a piece of software called UPnP enabled. UPnP enables programs running on the local network to open up network ports on an as-needed basis to communicate with the outside world. According to Netgear's page on UPnP and its routers, "Security risk associated with enabling UPnP on the router, technically a worm or malware program could use this function to compromise security for the entire LAN".

One of the fundamental tenets of computer security is at the attack surface should be as small as possible. This means only enabling pieces of the software that are necessary to meet the needs of the installation. While there may be a need for UPnP for some users, that's certainly not the case for all, and definitely not the mom and pop Chinese restaurant. The typical manufacturer firmware is the antithesis of this principle, enabling everything the end user may need, opening the router up to both the good users and the malicious ones. Third-party firmware distributions typically have distinct packages: a minimal build with just the necessary packages installed, a build which has everything installed, and something somewhere in between. Many even allow a user to install the minimal build and install only the explicit packages they need (although arguably this is not the route the mom and pop Chinese restaurant would use).

Fourth, third-party firmware enables features in commodity routers that are frequently only available in higher-priced "commercial-grade" models. One example of this is the ability to present multiple distinct

¹ It should be noted that the firmware installed on any given router is not typically a monolithic piece of software. There is an operating system kernel, a web server to facilitate external communication, an application which processes the requests the user makes via the web server, software drivers for the various networking devices (wireless radios, Ethernet ports, etc.), various services (e.g., a Network Time Protocol client to keep the router's internal clock in sync with the world). Any one of these pieces can result in a security vulnerability with the router.

networks (both wired and wireless). The mom and pop Chinese restaurant can (and if we're perfectly honest should) have a wireless network for use by its customers (if it wants to offer free wifi) that is distinct from the network it is using for business purposes. They can't do that with an off the shelf device using the manufacturer supplied firmware, but with a third-party solution like OpenWRT or DD-WRT, they open themselves to a more secure world. The customer wi-fi network can be isolated from the business wi-fi network while using a single inexpensive device rather than one costing hundreds or even a couple thousand dollars.

As another example, small offices or restaurants, and even home users use these devices as active security devices (firewalls). In reality, the manufacturer firmware seldom provides more of a firewalling capability than what can be provided with simple Network Address Translation². Third-party firmware solutions enable more complex firewalling abilities, even allowing these devices to serve as Virtual Private Network end points which enable employees to work remotely while having access to the internal network. Such users are unlikely to spend the thousands of dollars necessary for a high-end solution that for which they really have no need. In the end, these users rely on the security provided by NAT, which is little more than security through obscurity, which is inherently insecure.

As a final example of features available in third-party firmware versus manufacturer firmware, I offer up my own home as an example. It is large enough that if I have a single centrally-located access point, the signal is weaker than I'd like it to be, particularly on the 5GHz band that is the subject of this proposed rule. Because of this I actually have a pair of higher-end consumer-grade NetGear R7000 routers, both running the DD-WRT firmware, stationed at each end of the house to provide complete coverage. Our home phone service comes in as Voice over IP, and we have several WiFi-based cordless phones, as well as soft-phone applications on our iPhones. DD-WRT allows me to broadcast two distinct network names, which are attached to different VLANs³ on their uplink connections. One network is for laptops and other wireless devices to use and for guest access. The other is for the Voice over IP network. In fact I actually have a third VLAN available at the R7000's, as they are both located near our DirecTV receivers and Blu-Ray players, both of which plug into the wired Ethernet ports on the routers as a media-specific network.

Breaking my home network down into distinct VLANs allows me to prioritize the network traffic on the uplink ports so that the voice traffic gets the highest priority, followed by the laptop network, followed by the media network. With DD-WRT I have seamless integration and handoff between the two routers when a phone moves between their zones of coverage. In fact one of the advantages of using DD-WRT is that I can actually turn the transmit power down on the routers, to balance out the signal strengths better where the broadcast ranges overlap. If I were only able to use the manufacturer's firmware on these routers, I'd

² Network Address Translation is a mechanism by which multiple computers on one side of a translator (in this case the consumer router) can access resources on the other side of the translator (i.e., the Internet), while appearing to share a single IP address (the public side of the router). It was developed as a stopgap method of dealing with the dwindling supply of IPv4 addresses available to end users. While it provides minimal security, as the deployment of IPv6 increases, it will become unnecessary, and that security will disappear.

³ A VLAN, also known as a Virtual LAN, is a method by which network switching equipment can divide its ports into separate networks, or broadcast domains without using multiple network switches. Typically a given network port is connected to a single VLAN, however multiple VLANs can be assigned to a single network port and aggregated over a "trunk" line between different switches.

either lose a significant amount of control over my own network, or I'd be forced to spend several thousand dollars on an enterprise-grade system. I know this is something that's a lot more complex than a typical home user would do, but there's a legitimate case for it in the case of the mom and pop Chinese restaurant I've been mentioning, and literally millions of other small businesses across the country. Yes, these advanced networking features won't "just work" out of the box, even with a third-party firmware, but they aren't even in the box with manufacturer firmware, and they don't "just work" out of the box with an expensive solution. The difference between the expensive solution and the third-party solution being that the features are easy to configure through a web-based GUI with the third party firmware.

As a final argument against this proposed rule, a significant number of manufacturers are relying on the Linux operating system and many other open source tools that are licensed under the GNU General Public License. The reasons for this are vast, but just like the reasons customers with relatively simple needs choose off the shelf hardware instead of expensive commercial software, GNU/Linux is the software of choice because it just works. However one of the conditions of the software is that when a manufacturer customizes it and redistributes it, they are required to make their source code changes available to the end users, so that they can further customize it (this also has a side benefit of the source code being available for peer review to find security vulnerabilities). Many of these packages are licensed under version 3 of the GPL, which not only requires that the source code be made available to the consumer, but also any facilities necessary to actually use that software along with the hardware. Without changing many underlying software packages, manufacturers may not even be able to comply with the proposed rule as written because the end-user would be prohibited from using the modified software on the router. Such a rule would impose undue burdens on the device manufacturers who would now have to find different software, or write their own to replace the functionality they could no longer legally deliver due to copyright law.

In closing, I'd like to point out that the Supreme Court standard of strict scrutiny, *United States v. Carolene Products Company*, 304 U.S. at 155 (1938)⁴, may be relevant here, as there is a potential first amendment liberty at stake. As I'm sure the Commission is already aware, strict scrutiny is a three pronged test: there must exist a compelling governmental interest, the policy must be

⁴ There may be narrower scope for operation of the presumption of constitutionality when legislation appears on its face to be within a specific prohibition of the Constitution, such as those of the first ten amendments, which are deemed equally specific when held to be embraced within the Fourteenth. See *Stromberg v. California*, [283 U. S. 359](#), [283 U. S. 369-370](#); *Lovell v. Griffin*, [303 U. S. 444](#), [303 U. S. 452](#).

It is unnecessary to consider now whether legislation which restricts those political processes which can ordinarily be expected to bring about repeal of undesirable legislation is to be subjected to more exacting judicial scrutiny under the general prohibitions of the Fourteenth Amendment than are most other types of legislation. On restrictions upon the right to vote, see *Nixon v. Herndon*, [273 U. S. 536](#); *Nixon v. Condon*, [286 U. S. 73](#); on restraints upon the dissemination of information, see *Near v. Minnesota ex rel. Olson*, [283 U. S. 697](#), [283 U. S. 713-714](#), [283 U. S. 718-720](#), [283 U. S. 722](#); *Grosjean v. American Press Co.*, [297 U. S. 233](#); *Lovell v. Griffin*, *supra*; on interferences with political organizations, see *Stromberg v. California*, *supra*, [283 U. S. 369](#); *Fiske v. Kansas*, [274 U. S. 380](#); *Whitney v. California*, [274 U. S. 357](#), [274 U. S. 373-378](#); *Herndon v. Lowry*, [301 U. S. 242](#), and see Holmes, J., in *Gitlow v. New York*, [268 U. S. 652](#), [268 U. S. 673](#); as to prohibition of peaceable assembly, see *De Jonge v. Oregon*, [299 U. S. 353](#), [299 U. S. 365](#).

Nor need we enquire whether similar considerations enter into the review of statutes directed at particular religious, *Pierce v. Society of Sisters*, [268 U. S. 510](#), or national, *Meyer v. Nebraska*, [262 U. S. 390](#); *Bartels v. Iowa*, [262 U. S. 404](#); *Farrington v. Tokushige*, [273 U. S. 284](#), or racial minorities, *Nixon v. Herndon*, *supra*; *Nixon v. Condon*, *supra*: whether prejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities, and which may call for a correspondingly more searching judicial inquiry. Compare [17 U. S. Maryland](#), 4 Wheat. 316, [17 U. S. 428](#); *South Carolina v. Barnwell Bros.*, [303 U. S. 177](#), [303 U. S. 184](#), n 2, and cases cited.

narrowly tailored to meet that interest, and the least restrictive means of meeting that interest must be used. There is no argument that the Commission has a compelling interest in implementing this proposed rule; the RF spectrum is a limited resource, and radios which transmit at a higher power than lawfully allowed interfere with other radios. I would argue that restricting the ability of the software in consumer routers to increase the transmitter power beyond what is legally allowed is sufficiently narrowly tailored to solve the problem the rule is trying to solve. The problem with the rule, as I see it, is that outright prohibiting third-party firmware is not the least restrictive means for achieving the desired end result.

The firmware which controls the radio, and that which provides the operating system of the router, while often packaged together, end up in distinctly different locations on the hardware, and are in fact two distinct pieces of software. The radio firmware is incredibly specific to the hardware, and is typically provided as a binary blob to the manufacturer from the supplier of the actual radio hardware. Usually, the source code for this firmware is in a form proprietary to the manufacturer of the radio hardware, and useless to the end consumer of the product. It can, in fact, be deployed to the radio separate from the firmware that provides the general operating system for the device. As an example, Apple's iPhone devices receive both distinct radio firmware updates and more generic iOS updates (although on belief, the former is often contained in the latter). Router firmware updates which contain radio firmware updates update the radio firmware separately from the operating system. There is no compelling reason to prohibit consumers from installing a third party firmware in the name of limiting the radio power to that which is lawfully allowed, when that goal can be achieved through hardware means that would prevent the radio from transmitting with too high of a power level, while allowing the operating system to be modified by the user.

Relying on software to limit the output power of radio-frequency devices has a history of being problematic. Take as an example the case of the Therac 25. The hardware interlocks of the predecessor which restricted the radiation doses delivered to safe levels were replaced by software interlocks, which failed at least a half-dozen times, resulting in severe injuries and 3 deaths. Arguably that isn't a risk here given that these routers typically have a 25W power supply at best and the radios aren't physically capable of emitting that much power. But it is far from inconceivable that they could produce unwanted interference (hence the government's legitimate interest in controlling the output power). But as the proposed rule itself states there is an expectation that there will be distinct hardware produced for the US market and distinct hardware produced for the rest of the world. Under such circumstances, there is no reason that the transmit power cannot be limited physically with hardware that would otherwise be unmodifiable by the user (without explicitly triggering existing rules about transmitter medication).

As an aside, my passion for engineering grew in part because the facilities existed for me to tinker with electronic devices, such as model railroad throttles, when I was younger. Sadly, the advancing miniaturization of electronics over the past two decades has made this tinkering a lost art, not for lack of desire but because such tinkering requires such specialized tools. While I lament its loss, that loss is a contributing factor to why a hardware limitation on the transmit power is actually feasible; the average user doesn't have the tools that would be necessary to rewire a surface-mount based circuit board. There are volumes of research that have been published in the field of computer science that would not have

been possible without the ability to modify the software on consumer-grade routers, unnecessarily resulting in even more innovation leaving the country for foreign lands.

While I can appreciate the goals the Commission has in mind in making this rule, I strongly encourage the Commissioners to consider reducing the scope of the prohibition on third party firmware in consumer routers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Thierry

Last Name: Arbault

Mailing Address: 14 rue Balzac

City: Croix

Country: France

State or Province: Nord

ZIP/Postal Code: 59170

Email Address:

Organization Name:

Comment: This idea is not only abysmally stupid but also very dangerous for the freedom of users.

If passed this law will also affect people throughout the world which is unacceptable.

One of the obvious consequences will be that consumers worldwide will keep away from such devices, making the day of numerous non-US manufacturers.

When I buy a device, it is mine and I decided when, if, and how it can be used and modified. Keep out of MY property !

This idea is not only abysmally stupid but also very dangerous for the freedom of users.

If passed this law will also affect people throughout the world which is unacceptable.

One of the obvious consequences will be that consumers worldwide will keep away from such devices, making the day of numerous non-US manufacturers.

When I buy a device, it is mine and I decided when, if, and how it can be used and modified. Keep out of MY property !

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: r

Last Name: s

Mailing Address: 51 rue legendre

City: paris

Country: France

State or Province: Ile de France

ZIP/Postal Code: 75017

Email Address:

Organization Name:

Comment: You cannot make this ammend. To remove from us the right to modify our own wireless devices is the same as removing the right of free talk. It is completely against the policy of a country of freedom like the United States of America.

You cannot do this to us and you shouldn't do this to yourselves.

You cannot make this ammend. To remove from us the right to modify our own wireless devices is the same as removing the right of free talk. It is completely against the policy of a country of freedom like the United States of America.

You cannot do this to us and you shouldn't do this to yourselves.

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 Peter

Last Name: Berquist

Mailing Address: 1736 Stove Prairie Circle

City: Loveland

Country: United States

State or Province: CO

ZIP/Postal Code: 80538

Email Address: pete_berquist@netzero.net

Organization Name: Emissions Test Consulting, LLC

Comment: I commend the Commission on their decision. This is a positive way to limit the bureaucracy involved in placing a product on the market. Good work!!!

I commend the Commission on their decision. This is a positive way to limit the bureaucracy involved in placing a product on the market. Good work!!!

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: Marek

Last Name: Milbar

Mailing Address: 351 Pheasant Drive

City: Huntingdon Valley

Country: United States

State or Province: PA

ZIP/Postal Code: 19006

Email Address:

Organization Name:

Comment: The proposal is likely to put a stop on improvements and creativity in the very same area (Wi-Fi equipment) that it is attempting to protect. As such, it may turn to be damaging instead of helpful.

The early days of Linksys routers, where nearly anyone could modify readily available source code, and significantly improve functionality and performance, are the best proof that open access equals open mind.

Looking at small things such as the ability of a third party to develop and provide improved access software (drivers and beyond), or looking at big things such as the evolution of the Android world, should be enough for substantiating the advantage 'open' as opposed to 'locked'.

Please stop this process and remove the proposed rule.

The proposal is likely to put a stop on improvements and creativity in the very same area (Wi-Fi equipment) that it is attempting to protect. As such, it may turn to be damaging instead of helpful.

The early days of Linksys routers, where nearly anyone could modify readily available source code, and significantly improve functionality and performance, are the best proof that open access equals open mind.

Looking at small things such as the ability of a third party to develop and provide improved access software (drivers and beyond), or looking at big things such as the evolution of the Android world, should be enough for substantiating the advantage 'open' as opposed to 'locked'.

Please stop this process and remove the proposed rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ricardo

Last Name: Feliciano

Mailing Address: 701 N. Surrey Ave

City: Ventnor

Country: United States

State or Province: NJ

ZIP/Postal Code: 08406

Email Address: FelicianoTech@gmail.com

Organization Name:

Comment: Wireless routers have been prone to many security vulnerabilities over the years. The only secure ones have been the routers we've been able to install alternative software on such as DD-WRT. It's the 1st-party software that's a security concern. Not the 3rd-party software that we CHOOSE to install on the hardware we bought.

I ask that the FCC please do not:

- 1) Restrict the software routers can run in the name of security as this will have the opposite effect.
- 2) Restrict my freedom to run software of my choosing on a device I paid for and own.

Thank you.

Wireless routers have been prone to many security vulnerabilities over the years. The only secure ones have been the routers we've been able to install alternative software on such as DD-WRT. It's the 1st-party software that's a security concern. Not the 3rd-party software that we CHOOSE to install on the hardware we bought.

I ask that the FCC please do not:

- 1) Restrict the software routers can run in the name of security as this will have the opposite effect.
- 2) Restrict my freedom to run software of my choosing on a device I paid for and own.

Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Riley

Last Name: Abbe

Mailing Address: 2812 SW 28th Ave

City: Amarillo

Country: United States

State or Province: TX

ZIP/Postal Code: 79109

Email Address: macodin@gmail.com

Organization Name:

Comment: I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168> The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt> The result of this multi-year effort was a major advance in performance for all routers. The fq_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as

test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) I would incorporate all the other talking points listed on the Save WiFi page at:
https://libreplanet.org/wiki/Save_WiFi

5) Finally, I want to address the FCC's original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve America's airwaves.

I copied this because I agree with it and it's laid out better than I could ever do myself. Thank you for your time.

Riley Abbe

I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168>. The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt>. The result of this multi-year effort was a major advance in performance for all routers. The fq_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it

more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) I would incorporate all the other talking points listed on the Save WiFi page at:

https://libreplanet.org/wiki/Save_WiFi

5) Finally, I want to address the FCC's original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve America's airwaves.

I copied this because I agree with it and it's laid out better than I could ever do myself. Thank you for your time.

Riley Abbe

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: Robin

Last Name: Tauxe

Mailing Address: Route d'Avouillons 9

City: Leysin

Country: Switzerland

State or Province: Vaud

ZIP/Postal Code: 1854

Email Address: rtauxe@gmail.com

Organization Name:

Comment: I want to be able to customize my computing devices.

I want to be able to customize my computing 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: Emilio

Last Name: Parisca

Mailing Address: 250 Pharr Rd

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30305

Email Address: vladdrak@hotmail.com

Organization Name:

Comment: Please keep router and software open source. Do not stifle innovation and security by restricting such software to proprietary manufacturers. Peer review and transparency push both open source and private companies to compete for better products, which benefit consumers and business alike.

Please keep router and software open source. Do not stifle innovation and security by restricting such software to proprietary manufacturers. Peer review and transparency push both open source and private companies to compete for better products, which benefit consumers and business alike.

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: Emil

Last Name: Alasgarov

Mailing Address: Mir Calal Street

City: Baku

Country: Azerbaijan

State or Province: Baku

ZIP/Postal Code: AZ0001

Email Address: debianmik@gmail.com

Organization Name:

Comment: This project is contrary to the freedom to use my device. It seems that the United States - it's a free country. But apparently it is not. By adopting this project, you will begin to slow technological progress. But apparently, the American government just wants more to monitor citizens.

This project is contrary to the freedom to use my device. It seems that the United States - it's a free country. But apparently it is not. By adopting this project, you will begin to slow technological progress. But apparently, the American government just wants more to monitor citizens.

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: Ricardo

Last Name: Velazquez

Mailing Address: 602 Brigita ave

City: la puente

Country: United States

State or Province: CA

ZIP/Postal Code: 91744

Email Address:

Organization Name:

Comment: this new law/bill will not fix anything. it will only hold back the industry and all new development. please for the love of god do not implement this for receivers. you should force manufactures to encrypt there signals or add an extra layer of security. why would you kill/hurt the hardware simply because nobody was smart enough to make the signal secure.

this new law/bill will not fix anything. it will only hold back the industry and all new development. please for the love of god do not implement this for receivers. you should force manufactures to encrypt there signals or add an extra layer of security. why would you kill/hurt the hardware simply because nobody was smart enough to make the signal secure.

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: Yehonatan

Last Name: Davidi

Mailing Address: Alenby 22

City: Tel-Aviv

Country: Israel

State or Province: Center

ZIP/Postal Code: 6330111

Email Address:

Organization Name:

Comment: My understanding is that the proposed law aims to put in place security measures against tampering with the broadcast capabilities of wireless devices (power or frequency), since these actions could allow the devices to operate outside the specifications allowed by local regulations.

While this in itself is a reasonable thing to do, the means by which it can be achieved vary greatly in side effects.

Requiring devices to prevent any kind of modification of the firmware altogether, would do great damage to users of such devices, everywhere, since custom firmwares are routinely used to implement useful features in devices (routers, cellular phones, etc.), or fix bugs in the original firmware, which have absolutely nothing to do with the wireless radio itself.

For example, a user may want to install custom firmware on the router, to add FTP server capabilities. This has nothing to do with the wireless capabilities that the proposed law wishes to regulate, and yet if the law requires broad restrictions on firmware modifications, this useful ability may be taken away from the users.

My fear is that if the law is implemented as is, it may greatly and unnecessarily restrict the freedom of users to modify their devices in ways which do not violate any existing laws.

If a device vendor chooses to allow firmware customization for its users, we should not limit by law these freedoms, just because some modifications may be illegal. That would be like throwing the baby out with the bath water.

I would suggest instead, that the law, if it wishes to achieve the stated goal, specifically isolates the wireless radio component, and requires that the component itself will be locked, in hardware, in a way that prevents broadcasting outside the allowed specifications. This way no firmware modification can unlock what is locked in hardware, and yet the crucial freedom of modifying the firmware for other useful features is not taken away from the users.

My understanding is that the proposed law aims to put in place security measures against tampering with the broadcast capabilities of wireless devices (power or frequency), since these actions could allow the devices to operate outside the specifications allowed by local regulations.

While this in itself is a reasonable thing to do, the means by which it can be achieved vary greatly in side effects.

Requiring devices to prevent any kind of modification of the firmware altogether, would do great damage to users of

such devices, everywhere, since custom firmwares are routinely used to implement useful features in devices (routers, cellular phones, etc.), or fix bugs in the original firmware, which have absolutely nothing to do with the wireless radio itself.

For example, a user may want to install custom firmware on the router, to add FTP server capabilities. This has nothing to do with the wireless capabilities that the proposed law wishes to regulate, and yet if the law requires broad restrictions on firmware modifications, this useful ability may be taken away from the users.

My fear is that if the law is implemented as is, it may greatly and unnecessarily restrict the freedom of users to modify their devices in ways which do not violate any existing laws.

If a device vendor chooses to allow firmware customization for its users, we should not limit by law these freedoms, just because some modifications may be illegal. That would be like throwing the baby out with the bath water.

I would suggest instead, that the law, if it wishes to achieve the stated goal, specifically isolates the wireless radio component, and requires that the component itself will be locked, in hardware, in a way that prevents broadcasting outside the allowed specifications. This way no firmware modification can unlock what is locked in hardware, and yet the crucial freedom of modifying the firmware for other useful features is not taken away from the users.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Mosby

Mailing Address: 320 Saint Paul St.

City: Brookline

Country: United States

State or Province: MA

ZIP/Postal Code: 02446

Email Address:

Organization Name:

Comment: The proposed changes in regulations governing firmware updates on routers and other devices creates legal grey zones that can be exploited to the detriment of the consumer and citizen. I urge you to take the time and review what will be looked back upon as a hasty and potentially dangerous precedent.

The proposed changes in regulations governing firmware updates on routers and other devices creates legal grey zones that can be exploited to the detriment of the consumer and citizen. I urge you to take the time and review what will be looked back upon as a hasty and potentially dangerous precedent.

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: Every

Last Name: One

Mailing Address: The White House?

City: America

Country: United States

State or Province: AS

ZIP/Postal Code: 90210

Email Address: Fuckyou@thegov.doo

Organization Name: Government? No.

Comment: Seriously? Ban firmware changes? Is everyone in the FCC 90 years old and slightly slow now? Fuck outta here.

Seriously? Ban firmware changes? Is everyone in the FCC 90 years old and slightly slow now? Fuck outta here.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jesse

Last Name: Partridge

Mailing Address: 1127 W Marie Ave

City: Coeur d'Alene

Country: United States

State or Province: ID

ZIP/Postal Code: 83815

Email Address: jessedp009@gmail.com

Organization Name:

Comment: It is my belief, based on what parts of this document I have read, and the widely reported stories about it, that it would harm countless influential consumers and creative entities. I mean this in that it would introduce legal complications into the work of firmware modification hobbyists, HAM radio operators, and the like. Additionally, this proposal would place unnecessary restriction on a practice, which is already more difficult than it should be: Installation of unofficial or unsupported software and firmware. For some members of the tech community, installation of things like custom WiFi router firmware, Custom ROMs for smartphones running Android, and, most importantly, Linux-based operating systems for computers, is extremely important. In some cases, it is even part of one's business. Restricting firmware on devices with software-defined radios will do more harm to creative and enterprising groups like the Free Software Foundation and CyanogenMod, than it would help manufacturers keep their devices safe from malicious exploits.

It is my belief, based on what parts of this document I have read, and the widely reported stories about it, that it would harm countless influential consumers and creative entities. I mean this in that it would introduce legal complications into the work of firmware modification hobbyists, HAM radio operators, and the like. Additionally, this proposal would place unnecessary restriction on a practice, which is already more difficult than it should be: Installation of unofficial or unsupported software and firmware. For some members of the tech community, installation of things like custom WiFi router firmware, Custom ROMs for smartphones running Android, and, most importantly, Linux-based operating systems for computers, is extremely important. In some cases, it is even part of one's business. Restricting firmware on devices with software-defined radios will do more harm to creative and enterprising groups like the Free Software Foundation and CyanogenMod, than it would help manufacturers keep their devices safe from malicious exploits.

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: Gerald

Last Name: White

Mailing Address: 12908 Cactus Berry Dr

City: Riverton

Country: United States

State or Province: UT

ZIP/Postal Code: 84096

Email Address:

Organization Name:

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: clint

Last Name: merkley

Mailing Address: 2474 west 1500 north

City: vernal

Country: United States

State or Province: UT

ZIP/Postal Code: 84078

Email Address:

Organization Name:

Comment: I believe regulations like this and others not only stifle creativity and innovation but are the seeds from which rebellion grows.

I do not endorse this.

I very much oppose this.

No. Much no.

I believe regulations like this and others not only stifle creativity and innovation but are the seeds from which rebellion grows.

I do not endorse this.

I very much oppose this.

No. Much no.

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: L

Last Name: Harrington

Mailing Address: 4324 Winners Circle Unit 3023

City: Sarasota

Country: United States

State or Province: FL

ZIP/Postal Code: 34238

Email Address: lharrington@gmail.com

Organization Name:

Comment: Removing functionality that enterprising consumers and business technicians use as value-add is not the answer to clamping down on spectrum abuse by the handfuls of abusers committing such acts. Radio firmwares can offer reduced APIs, certain aspects of radio operation could be made unmodifiable (via software), etc. There are many solutions much more tactical that do not throw the baby out with the bath water. As a 20+ year user of custom router firmwares (never once have I modified my radio settings to anything but spec, nor has a single peer of mine that I know) I am fearful you will be killing a cottage industry, a hobbyists dream and an independent freelancer's revenue stream.

Please consider the ramifications of overbroad regulation.

Removing functionality that enterprising consumers and business technicians use as value-add is not the answer to clamping down on spectrum abuse by the handfuls of abusers committing such acts. Radio firmwares can offer reduced APIs, certain aspects of radio operation could be made unmodifiable (via software), etc. There are many solutions much more tactical that do not throw the baby out with the bath water. As a 20+ year user of custom router firmwares (never once have I modified my radio settings to anything but spec, nor has a single peer of mine that I know) I am fearful you will be killing a cottage industry, a hobbyists dream and an independent freelancer's revenue stream.

Please consider the ramifications of overbroad regulation.

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: Kai

Last Name: Schulte

Mailing Address: descipar@gmail.com

City: Duesseldorf

Country: Germany

State or Province: NRW

ZIP/Postal Code: 40211

Email Address:

Organization Name:

Comment: I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans and Non-Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US and worldwide, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168> The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt> The result of this multi-year effort was a major advance in performance for all routers. The fq_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans and Non-Americans to improve their knowledge and become more competitive.

4) I would incorporate all the other talking points listed on the Save WiFi page at:
https://libreplanet.org/wiki/Save_WiFi

5) Finally, I want to address the FCC's original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve regulated airwaves.

I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans and Non-Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US and worldwide, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168>. The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturers seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt> The result of this multi-year effort was a major advance in performance for all routers. The fq_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would likely not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans and Non-Americans to improve their knowledge and become more

competitive.

4) I would incorporate all the other talking points listed on the Save WiFi page at:

https://libreplanet.org/wiki/Save_WiFi

5) Finally, I want to address the FCC's original concern that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve regulated airwaves.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: Franaszek

Mailing Address: PO Box 3133

City: Santa Rosa

Country: United States

State or Province: CA

ZIP/Postal Code: 95402

Email Address:

Organization Name:

Comment: Re: Notice of Proposed Rule Making, ET Docket No. 15-170, FCC 15-92

I am concerned that the FCC proposed rules will have the unintended consequences of restricting the installation of alternative operating systems such as Linux and BSD on devices with wireless capability. Furthermore, the new rule could be used to ban the installation of custom firmware on Android phones -- which is something hundreds of thousands of Americans do each year. Finally, the proposed rule may cripple the development of highly useful router firmwares such as OpenWRT & Tomato.

With all this at stake it makes no sense to approve this rule. I am asking the commission to reject it. This nation's success in computer/wireless technology was created by allowing open standards and technology. This rule would be a step backwards.

Re: Notice of Proposed Rule Making, ET Docket No. 15-170, FCC 15-92

I am concerned that the FCC proposed rules will have the unintended consequences of restricting the installation of alternative operating systems such as Linux and BSD on devices with wireless capability. Furthermore, the new rule could be used to ban the installation of custom firmware on Android phones -- which is something hundreds of thousands of Americans do each year. Finally, the proposed rule may cripple the development of highly useful router firmwares such as OpenWRT & Tomato.

With all this at stake it makes no sense to approve this rule. I am asking the commission to reject it. This nation's success in computer/wireless technology was created by allowing open standards and technology. This rule would be a step backwards.

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: Eric

Last Name: Donaldson

Mailing Address: 417 8th Ave SE

City: Rochester

Country: United States

State or Province: MN

ZIP/Postal Code: 55904

Email Address: eric.donaldson

Organization Name: none

Comment: Thank you for allowing comments on an issue as important as citizens having the ability to run their software of choice on the computing devices that they own. I run DD-WRT on my router because I believe that open source software is more secure than proprietary software. I understand and appreciate the work you've done in keeping the radio spectrum free from interference. Please look for a way to continue this good work without taking away the rights of users to run the software they need to develop and use secure wifi routers and other products.

Thank you for allowing comments on an issue as important as citizens having the ability to run their software of choice on the computing devices that they own. I run DD-WRT on my router because I believe that open source software is more secure than proprietary software. I understand and appreciate the work you've done in keeping the radio spectrum free from interference. Please look for a way to continue this good work without taking away the rights of users to run the software they need to develop and use secure wifi routers and other products.

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: Kautz

Mailing Address: 31 Camp St

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94110-1101

Email Address: jkautz@gmail.com

Organization Name:

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

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

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

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

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: Triplet

Mailing Address: P.O. Box 2303

City: South Padre Island

Country: United States

State or Province: TX

ZIP/Postal Code: 78597

Email Address: sgamer@gmail.com

Organization Name:

Comment: As a user of alternative router firmware, I have been blessed to be able to operate my devices to their peak functionality by using them however I want. This legislation will stop that completely. Why? Am I harming anyone by modifying my own equipment? This is akin to not allowing people to perform engine swaps on their car with engines from a different manufacturer! It makes no sense, harms innovation, and will literally shut down years of advanced networking development.

As a user of alternative router firmware, I have been blessed to be able to operate my devices to their peak functionality by using them however I want. This legislation will stop that completely. Why? Am I harming anyone by modifying my own equipment? This is akin to not allowing people to perform engine swaps on their car with engines from a different manufacturer! It makes no sense, harms innovation, and will literally shut down years of advanced networking development.

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: Josh

Last Name: Renaud

Mailing Address: 624 Forest Ave.

City: Ferguson

Country: United States

State or Province: MO

ZIP/Postal Code: 63135

Email Address:

Organization Name:

Comment: Until recently, I hadn't realized it was possible to install open-source firmware on my WiFi router. But once I did, it vastly improved my household internet connection, and enabled many new features that weren't possible before.

I was dismayed to learn about the proposed rules and recommendations that would prevent the installation of open-source wireless firmware such as OpenWrt or dd-wrt.

Home users like me install this replacement firmware because gives _US_ the power. We can make the device suit our needs.

The proposed changes would take away our ability to administer and customize hardware that we bought and paid for. That is unacceptable to me.

Until recently, I hadn't realized it was possible to install open-source firmware on my WiFi router. But once I did, it vastly improved my household internet connection, and enabled many new features that weren't possible before.

I was dismayed to learn about the proposed rules and recommendations that would prevent the installation of open-source wireless firmware such as OpenWrt or dd-wrt.

Home users like me install this replacement firmware because gives _US_ the power. We can make the device suit our needs.

The proposed changes would take away our ability to administer and customize hardware that we bought and paid for. That is unacceptable to me.

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: corey

Last Name: waldrum

Mailing Address: 1420 moss rose circle

City: Irving

Country: United States

State or Province: TX

ZIP/Postal Code: 75061

Email Address:

Organization Name:

Comment: please dont pass the new rules for wifi because they implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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 choose 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 dont pass the new rules for wifi because they implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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 choose 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: Shay

Last Name: Sackett

Mailing Address: 1264 Alameda Ave.

City: Glendale

Country: United States

State or Province: CA

ZIP/Postal Code: 91201

Email Address: shaysacketttek@gmail.com

Organization Name:

Comment: I, Shay Sackett, would like to respectfully request that the FCC not implement any rules that take away the freedom of the user to install the software of their choosing. I value my privacy and security, as most Americans do, and often times companies will not fix gaping holes in router, computer, or smartphone security software. When this occurs I, and my fellow citizens, need to be able to modify/and or upload new software to ensure our privacy and security. Additionally, adding restrictions that keep the user from installing different firmware will severely damage the open source community that often time provides better, more secure software than the manufacturer, for free. Researchers need to be able to modify their equipment to carry out the work they do, and limiting their ability to work effectively would slow down innovation and erode America's technological edge over the rest of the world. America stands for freedom, and that applies to the world of software and electronics as well. Thank you for your time.

I, Shay Sackett, would like to respectfully request that the FCC not implement any rules that take away the freedom of the user to install the software of their choosing. I value my privacy and security, as most Americans do, and often times companies will not fix gaping holes in router, computer, or smartphone security software. When this occurs I, and my fellow citizens, need to be able to modify/and or upload new software to ensure our privacy and security. Additionally, adding restrictions that keep the user from installing different firmware will severely damage the open source community that often time provides better, more secure software than the manufacturer, for free. Researchers need to be able to modify their equipment to carry out the work they do, and limiting their ability to work effectively would slow down innovation and erode America's technological edge over the rest of the world. America stands for freedom, and that applies to the world of software and electronics as well. Thank you for your time.

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: Marc

Last Name: Brooks

Mailing Address: 938 Morrison Ave

City: St. Louis

Country: United States

State or Province: MO

ZIP/Postal Code: 63104

Email Address: idisposable@gmail.com

Organization Name: Self

Comment: While in principle this is a good idea, the net effect will be to prevent consumers from protecting themselves from back-doors, security flaws and bugs (intentional or not) that manufacturers often ship in production devices. These devices, under the relentless economic pressures of shipping NEWER models are usually immediately abandoned, leaving the consumer vulnerable to all kinds of problems including security flaws and unintended functioning. By making it illegal for a consumer to fix these issues, you are basically guaranteeing decades of bad hardware and software in this generation of the Internet of (broken, hacked) Things.

Please (re)consider the cost of this unintended side effect and stop this ruling dead.

While in principle this is a good idea, the net effect will be to prevent consumers from protecting themselves from back-doors, security flaws and bugs (intentional or not) that manufacturers often ship in production devices. These devices, under the relentless economic pressures of shipping NEWER models are usually immediately abandoned, leaving the consumer vulnerable to all kinds of problems including security flaws and unintended functioning. By making it illegal for a consumer to fix these issues, you are basically guaranteeing decades of bad hardware and software in this generation of the Internet of (broken, hacked) Things.

Please (re)consider the cost of this unintended side effect and stop this ruling dead.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jacob

Last Name: Mueller

Mailing Address: 2075 Bridge Port Ct. Apt. 9

City: De PEre

Country: United States

State or Province: WI

ZIP/Postal Code: 54115

Email Address: jakem@spamcop.net

Organization Name:

Comment: This rule will completely destroy any experimentation and innovation by technically-minded citizens as pertains to

Decades ago, the United States led the world in grassroots technological advancement in the electricity and electronics fields. The Amateur Radio Service created unique solutions to unique problems, some of which became the basis for commercial technologies that were later in use. RF circuits used to blank out noise from LORAN-A transmitters on the 160 meter band, developed by amateurs in the 1950's, were later adapted for noise-blanking circuits in commercially-available amateur radios.

In more recent times, the Amateur Radio community began experimenting in the 2.4 and 5Ghz bands by launching the Broadband-HAMNET project, providing high-speed data, voice, and telephony over a mesh network. This was accomplished by operators MODIFYING their own wi-fi routers. A resilient communications networking model borne of experimentation with outdated equipment, while no threat to a Telecom, could lead to greater things in the future.

The "hacking" community (by this I mean computer hackers, yes) is so often vilified by a misinformed public. The ability to inspect and modify devices or source code is critical for experimenters in the following ways: First, many security vulnerabilities, some very serious, are detected by "white hat" hackers who experiment with these technologies.

The distributed model of security and vulnerability research among independent parties is instrumental for IT professionals who need to keep their assets secure. If the reader does not believe me, Microsoft, RedHat, Secunia, the MITRE corporation, etc., all post credit for discovery of their vulnerabilities after security patches are released. Often these come from independent security research firms and individuals that are in essence, "hackers". Second, it is important to promote learning and experimentation among all technically minded citizens if the Commission believes that the United States should continue to lead the world in technological development. Preventing such by implementing the proposed regulation will discourage honest citizens from experimentation, and will help to drive a monopoly on technological development held by multi-national corporations or the Federal Government, and also "black hat" hackers. It is the opinion of the writer that the Government's first obligation is to ensure the Liberty of the citizens, as well as promote activities that develop the citizens individually for the good of the Nation.

In conclusion, it is the opinion of the writer that removing the ability to modify or "flash" new firmware onto 5Ghz WIFI devices will harm the interest in technology among citizens, hurt important security research efforts, and cause the United States to fall further behind in technology. The liberty of a Nations' citizens to experiment with and develop technology is a cornerstone of civilization itself.

To whomever reads this, thank you for your patience with this "wall of text"

Jacob C. Mueller
IT professional 10 years running
Amateur Radio Operator Callsign KD9CLF

This rule will completely destroy any experimentation and innovation by technically-minded citizens as pertains to

Decades ago, the United States led the world in grassroots technological advancement in the electricity and electronics fields. The Amateur Radio Service created unique solutions to unique problems, some of which became the basis for commercial technologies that were later in use. RF circuits used to blank out noise from LORAN-A transmitters on the 160 meter band, developed by amateurs in the 1950's, were later adapted for noise-blanking circuits in commercially-available amateur radios.

In more recent times, the Amateur Radio community began experimenting in the 2.4 and 5Ghz bands by launching the Broadband-HAMNET project, providing high-speed data, voice, and telephony over a mesh network. This was accomplished by operators MODIFYING their own wi-fi routers. A resilient communications networking model borne of experimentation with outdated equipment, while no threat to a Telecom, could lead to greater things in the future.

The "hacking" community (by this I mean computer hackers, yes) is so often vilified by a misinformed public. The ability to inspect and modify devices or source code is critical for experimenters in the following ways: First, many security vulnerabilities, some very serious, are detected by "white hat" hackers who experiment with these technologies.

The distributed model of security and vulnerability research among independent parties is instrumental for IT professionals who need to keep their assets secure. If the reader does not believe me, Microsoft, RedHat, Secunia, the MITRE corporation, etc., all post credit for discovery of their vulnerabilities after security patches are released. Often these come from independent security research firms and individuals that are in essence, "hackers". Second, it is important to promote learning and experimentation among all technically minded citizens if the Commission believes that the United States should continue to lead the world in technological development. Preventing such by implementing the proposed regulation will discourage honest citizens from experimentation, and will help to drive a monopoly on technological development held by multi-national corporations or the Federal Government, and also "black hat" hackers. It is the opinion of the writer that the Government's first obligation is to ensure the Liberty of the citizens, as well as promote activities that develop the citizens individually for the good of the Nation.

In conclusion, it is the opinion of the writer that removing the ability to modify or "flash" new firmware onto 5Ghz WIFI devices will harm the interest in technology among citizens, hurt important security research efforts, and cause the United States to fall further behind in technology. The liberty of a Nations' citizens to experiment with and develop technology is a cornerstone of civilization itself.

To whomever reads this, thank you for your patience with this "wall of text"

Jacob C. Mueller
IT professional 10 years running
Amateur Radio Operator Callsign KD9CLF

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: ABAMA

Last Name: MONKEY

Mailing Address: CICILAN

City: FUCKCITY

Country: Afghanistan

State or Province: ABAMKA FUCK YOU

ZIP/Postal Code: 664477

Email Address: biyanosa@wickmail.net

Organization Name: biyanosa

Comment: FUCK YOU ABAMA! ABAMA IS MONKEY!

FUCK YOU ABAMA! ABAMA IS MONKEY!

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: Paul

Last Name: Marks

Mailing Address: 505 Cypress Point Dr Unit 132

City: Mountain View

Country: United States

State or Province: CA

ZIP/Postal Code: 94043

Email Address:

Organization Name:

Comment: For the past decade, I've been using wireless routers as general-purpose computers to run open source software like OpenWRT and DD-WRT. I disagree with any new regulation that would limit my right to do so with new hardware. The ability to flash custom software onto wireless devices has been instrumental in the development of new Internet technologies like IPv6, CoDel, and mesh networking.

Additionally, I think it would be a bad idea to give Chinese companies an incentive to make their software non-modifiable, because then it becomes completely trivial to include backdoors which cannot be removed.

For the past decade, I've been using wireless routers as general-purpose computers to run open source software like OpenWRT and DD-WRT. I disagree with any new regulation that would limit my right to do so with new hardware. The ability to flash custom software onto wireless devices has been instrumental in the development of new Internet technologies like IPv6, CoDel, and mesh networking.

Additionally, I think it would be a bad idea to give Chinese companies an incentive to make their software non-modifiable, because then it becomes completely trivial to include backdoors which cannot be removed.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jacob

Last Name: Killelea

Mailing Address: 861 Cambridge Ave

City: Menlo Park

Country: United States

State or Province: CA

ZIP/Postal Code: 94025

Email Address: jkillelea344@gmail.com

Organization Name:

Comment: Restrictions on radio software would lead to issues with free and open software, which is a critical component of the US technology industry, would dangerously limit the consumer's ability to upgrade obsolete or insecure software, and kill burgeoning movements in custom software and improvised networks.

Restrictions on radio software would lead to issues with free and open software, which is a critical component of the US technology industry, would dangerously limit the consumer's ability to upgrade obsolete or insecure software, and kill burgeoning movements in custom software and improvised networks.

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: Je'Don

Last Name: Lopez

Mailing Address: 1347 W. Moon Vista St.

City: Apache Junction

Country: United States

State or Province: AZ

ZIP/Postal Code: 85120

Email Address:

Organization Name:

Comment: To the FCC, I respectfully ask you do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. The NPRM will negatively affect the lives of everyday people. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so, and users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. It's also important to not implement the NPRM because it will negatively affect businesses and research institutions. 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.

To the FCC, I respectfully ask you do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. The NPRM will negatively affect the lives of everyday people. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so, and users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. It's also important to not implement the NPRM because it will negatively affect businesses and research institutions. 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.

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: Reazul

Last Name: Islam

Mailing Address: reazulswe@gmail.com

City: Dhaka

Country: Bangladesh

State or Province: Dhaka

ZIP/Postal Code: 0088

Email Address: reazulswe@gmail.com

Organization Name: Daffodil International Univresity

Comment: I object this because security and privacy is important to me.

I object this because security and privacy is important to me.

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: Jules

Last Name: Guidry

Mailing Address: 1095 edinboro dr

City: boulder

Country: United States

State or Province: CO

ZIP/Postal Code: 80305

Email Address:

Organization Name:

Comment: Though I cannot speak to the intent of this regulation, the increasing integration of wireless capabilities into devices means it would unjustly limit the ability of consumers to modify their legally purchased devices. As such, I cannot support it.

Though I cannot speak to the intent of this regulation, the increasing integration of wireless capabilities into devices means it would unjustly limit the ability of consumers to modify their legally purchased devices. As such, I cannot support it.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Connor

Last Name: Waltman

Mailing Address: 9118 Pennfield Rd

City: Battle Creek

Country: United States

State or Province: MI

ZIP/Postal Code: 49014

Email Address:

Organization Name:

Comment: I may not be a computer expert or a genius, but I know unnecessary bureaucracy when I see it. FCC, stop treating us like children, we can take risks and make our own decisions and we don't need you constantly watching over our every move.

I may not be a computer expert or a genius, but I know unnecessary bureaucracy when I see it. FCC, stop treating us like children, we can take risks and make our own decisions and we don't need you constantly watching over our every move.

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: White-Robinson

Mailing Address: 36 Maybank St

City: Dunedin

Country: New Zealand

State or Province: Otago

ZIP/Postal Code: 9010

Email Address: alexwr@gmail.com

Organization Name:

Comment: Hello,

I'm concerned that the "b. Modification of Certified Equipment by Third Parties" section precludes the modification and updating of software on an RF device such as an 802.11 wireless access device or client.

This would potentially prevent the development of novel applications of these technologies (For example, emergency response networks powered by mesh networking) by people without the resources to go through FCC certification. It may also prevent device users from improving on open-source RF-controlling software and deny people the ability to develop or apply fixes for security issues on wireless appliances when the vendor of an appliance has chosen to not provide one.

While the airwaves must be respected for the benefit of all RF users, forcing people to not use their equipment in a safe, secure manner seems detrimental to the development of future RF usage and to the security of RF users.

Regards,
Alex White-Robinson.

Hello,

I'm concerned that the "b. Modification of Certified Equipment by Third Parties" section precludes the modification and updating of software on an RF device such as an 802.11 wireless access device or client.

This would potentially prevent the development of novel applications of these technologies (For example, emergency response networks powered by mesh networking) by people without the resources to go through FCC certification. It may also prevent device users from improving on open-source RF-controlling software and deny people the ability to develop or apply fixes for security issues on wireless appliances when the vendor of an appliance has chosen to not provide one.

While the airwaves must be respected for the benefit of all RF users, forcing people to not use their equipment in a safe, secure manner seems detrimental to the development of future RF usage and to the security of RF users.

Regards,
Alex White-Robinson.

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: sagar

Last Name: kabor

Mailing Address: shukrabad

City: dhaka

Country: Bangladesh

State or Province: dhanmondi

ZIP/Postal Code: 1207

Email Address:

Organization Name:

Comment: "I object this because security and privacy is important to me."

"I object this because security and privacy is important to me."

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: Richardson

Mailing Address: 470 DAWSON AVE

City: Ottawa

Country: Canada

State or Province: Ontario

ZIP/Postal Code: K1Z5V7

Email Address: mcr@sandelman.ca

Organization Name: SANDELMAN SOFTWARE WORKS

Comment: I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

The security of vendor provided router software has been abysmal. It represents a very significant threat to national security as home router number in the hundreds of millions, and are presently used in malicious ways to attack the network infrastructure. A major reason why the code is old and does not get updated is precisely because of previous claims my manufacturers that they could not reveal how their radios work due to FCC rules. This has prevented or significantly slowed parties that care about the network (such as major ISPs: Verizon and Comcast for instance) from creating managing their own devices based upon open source frameworks.

If this ruling is not rescinded, then the small progress that has been made to secure the home network against malicious code will be lost as the open source projects will be forced to stop. Furthermore, the presence of security flaws in the routers themselves represents an avenue by which a malicious party could have access to the software defined radio present in the router. So, if one assumes that there is a malicious party out that that wishes to do bad things to the radio spectrum, this ruling makes it *easier* not harder, while at the same time driving the price up for everyone.

If I were with the FCC, I would go the other way: I would consider rescinding the license of any manufacturer who refuses to cooperate with open source groups. They are making the Internet significantly less safe, and the FCC certainly has interests in an open and neutral Internet.

I will also point at all the other talking points listed on the Save WiFi page at:
https://libreplanet.org/wiki/Save_WiFi

Please note that I am Canadian: but what happens in the US affects the entire world.

Further, my company relies on access to devices (processors, systems on a chip) that contain 802.11 and 802.15.4 radios in order to do basic research and produce products in the IoT space. If my company can not access the radio, then efforts to secure Internet Of Things devices will fail, and we will have a major disaster on our hands.

I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for consumer routers.

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This lock down would prevent modification to the radios power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

The security of vendor provided router software has been abysmal. It represents a very significant threat to national security as home router number in the hundreds of millions, and are presently used in malicious ways to attack the network infrastructure. A major reason why the code is old and does not get updated is precisely because of previous claims my manufacturers that they could not reveal how their radios work due to FCC rules. This has prevented or significantly slowed parties that care about the network (such as major ISPs: Verizon and Comcast for instance) from creating managing their own devices based upon open source frameworks.

If this ruling is not rescinded, then the small progress that has been made to secure the home network against malicious code will be lost as the open source projects will be forced to stop. Furthermore, the presence of security flaws in the routers themselves represents an avenue by which a malicious party could have access to the software defined radio present in the router. So, if one assumes that there is a malicious party out that that wishes to do bad things to the radio spectrum, this ruling makes it *easier* not harder, while at the same time driving the price up for everyone.

If I were with the FCC, I would go the other way: I would consider rescinding the license of any manufacturer who refuses to cooperate with open source groups. They are making the Internet significantly less safe, and the FCC certainly has interests in an open and neutral Internet.

I will also point at all the other talking points listed on the Save WiFi page at:
https://libreplanet.org/wiki/Save_WiFi

Please note that I am Canadian: but what happens in the US affects the entire world.

Further, my company relies on access to devices (processors, systems on a chip) that contain 802.11 and 802.15.4 radios in order to do basic research and produce products in the IoT space. If my company can not access the radio, then efforts to secure Internet Of Things devices will fail, and we will have a major disaster on our hands.

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: Brom

Mailing Address: 8445 SW Brentwood St.

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97225

Email Address: squarebird@hotmail.com

Organization Name: USAF, Retired

Comment: No, please do not implement this rule. It will stifle innovation by garage tinkerers in a still young and evolving technology.

Thank you,

Robert Brom

Major, USAF, Ret.

Portland Oregon

No, please do not implement this rule. It will stifle innovation by garage tinkerers in a still young and evolving technology.

Thank you,

Robert Brom

Major, USAF, Ret.

Portland Oregon

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: Rick

Last Name: Rickington

Mailing Address: 123 Main Street

City: Rick Town

Country: United States

State or Province: PA

ZIP/Postal Code: 12345

Email Address: I don't want you having my info to mail and people will send bombs

Organization Name: Rick

Comment: You really shouldn't do this, the ability to tweak and edit existing technologies is what gave us the car, phone, etc. We should not halt the entire human race for the sake of a little security, which won't happen anyway because those that want to hack, will hack.

You really shouldn't do this, the ability to tweak and edit existing technologies is what gave us the car, phone, etc. We should not halt the entire human race for the sake of a little security, which won't happen anyway because those that want to hack, will hack.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Dustin

Last Name: Lloyd

Mailing Address: 651 Westover Hills Blvd

City: Richmond

Country: United States

State or Province: VA

ZIP/Postal Code: 23225

Email Address:

Organization Name:

Comment: This equipment authorization and electronic labeling for wireless devices proposal opposes liberties that should be enforced, rather than prohibited.

This proposal is insulting to end users (RF product consumers) by disrespecting our liberties on the basis of ownership of a RF product. Not allowing the modifications of RF products such as flashing the ROM on embedded devices, leaves it questionable as to who owns the the RF product once purchased by the consumer; whereas if the consumer cannot modify their purchased product to fit their needs whilst respecting frequency allocations, then how would one quantify ownership of a RF product other than possession of a RF device?

This notion of not being able to modify RF products for the sake of productivity is counter intuitive to the RF technology itself.

Thank you for your considerations.

This equipment authorization and electronic labeling for wireless devices proposal opposes liberties that should be enforced, rather than prohibited.

This proposal is insulting to end users (RF product consumers) by disrespecting our liberties on the basis of ownership of a RF product. Not allowing the modifications of RF products such as flashing the ROM on embedded devices, leaves it questionable as to who owns the the RF product once purchased by the consumer; whereas if the consumer cannot modify their purchased product to fit their needs whilst respecting frequency allocations, then how would one quantify ownership of a RF product other than possession of a RF device?

This notion of not being able to modify RF products for the sake of productivity is counter intuitive to the RF technology itself.

Thank you for your considerations.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jordan

Last Name: Calo

Mailing Address: 1519 Sherman Ave

City: Chico

Country: United States

State or Province: CA

ZIP/Postal Code: 95926

Email Address: jspam3@yahoo.com

Organization Name:

Comment: I use a special router firmware called Tomato (similar to DD-WRT). From what I have been reading, this bill would prevent me from modifying my own devices to install the tomato firmware. Passing this bill sounds like a horrible idea. Not only would this limit the functionality of a device I have purchased with my own money (tomato expands the feature set on my router), but it would also make this same device less secure, as the Custom Tomato firmware includes security enhancements that are not included on the device's stock (non-custom) firmware.

I use a special router firmware called Tomato (similar to DD-WRT). From what I have been reading, this bill would prevent me from modifying my own devices to install the tomato firmware. Passing this bill sounds like a horrible idea. Not only would this limit the functionality of a device I have purchased with my own money (tomato expands the feature set on my router), but it would also make this same device less secure, as the Custom Tomato firmware includes security enhancements that are not included on the device's stock (non-custom) 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: Bryce

Last Name: McNab

Mailing Address: 140 N 9th street Apt A

City: San Jose

Country: United States

State or Province: CA

ZIP/Postal Code: 95112

Email Address: bmcnab80@gmail.com

Organization Name: null

Comment: I would like to request that the FCC not implement rules that 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.

I would like to request that the FCC not implement rules that 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.

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: Aleksandr

Last Name: Shekhter

Mailing Address: 29 Hunters Pointe

City: Middletown

Country: United States

State or Province: NJ

ZIP/Postal Code: 07748

Email Address:

Organization Name:

Comment: Before making this document an official document please consider the following:

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

In a short owrds I believe that this regulation should not be used as it is because of the reasons outlined above.

Thank you very much,

--- Alex Shekhter

Before making this document an official document please consider the following:

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

In a short owrds I believe that this regulation should not be used as it is because of the reasons outlined above.

Thank you very much,

--- Alex Shekhter

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: reza

Last Name: naima

Mailing Address: 229 Steiner St

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94117

Email Address:

Organization Name:

Comment: as it's impossible to separate out the firmware that controls the radio from the firmware that operates a wifi router, by locking down the firmware you are preventing many custom modifications which enhance functionality of the hardware. also, even if lock downs are attempted, ways to circumvent will always be found. the current set of rules is sufficient and attempts at locking down firmwares will probably backfire. i strongly suggest you do not try to impose further lock-downs of what is currently open source software running on routers.

as it's impossible to separate out the firmware that controls the radio from the firmware that operates a wifi router, by locking down the firmware you are preventing many custom modifications which enhance functionality of the hardware. also, even if lock downs are attempted, ways to circumvent will always be found. the current set of rules is sufficient and attempts at locking down firmwares will probably backfire. i strongly suggest you do not try to impose further lock-downs of what is currently open source software running on routers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jonathan

Last Name: Morton

Mailing Address: Ryttyntie 1 A 14

City: Forssa

Country: Finland

State or Province: Kanta-Hme

ZIP/Postal Code: 30300

Email Address: chromatix99@gmail.com

Organization Name:

Comment: See attached file(s)

See attached file(s)

Comment re: Proposed Rulemaking on Software Defined Radios

=====

I am an EU resident and citizen, and a software engineer involved in cutting-edge networking research. I wish to make certain that the FCC is aware that their regulations have global effects, not merely local to the United States.

I and others firmly believe that these newly proposed certification rules:

- will likely have deeply harmful effects,
- address a theoretical harm which has not been clearly demonstrated to exist in practice,
- will also be ineffective at achieving their stated goal.

I would like to take this opportunity to briefly outline alternative rules which would more carefully address the problem, avoiding the disadvantages listed above.

Global Reach

=====

It is a sad fact that most electronic device manufacture no longer takes place in the Western Hemisphere. Reduced labour costs and less restrictive regulations in the Far East mean that most consumer devices are designed and made there, and only reach America and Europe by export. If faced with tight regulations for imported devices, these manufacturers have few choices:

- Abandon the restrictive market entirely. North America is a large market, so this would be considered undesirable for the manufacturer, not just due to reduced choice for the consumer.
- Produce a separate, specially adapted product for the restrictive market. For large, durable goods such as road vehicles, it is possible to make such adaptations without much impact on final prices. However, this would unacceptably increase design and manufacturing costs for small, relatively cheap consumer electronics devices, due to disruption of the economies of scale that these manufacturers rely on.
- Produce a single product adapted for the most restrictive market the device is sold to. This effectively imposes these restrictive regulations globally.

It seems clear that most consumer device manufacturers will choose the latter option. That is why I am writing this comment.

Unintended Harms

=====

The proposed regulations do not clearly define the limits of what must be protected, especially considering the inevitable fact that the relevant reader - based in the Far East - speaks English only as a second language. This will lead to a misunderstanding of the true requirements, and the following likely consequences:

- Firmware modification will be prevented on the entire device, not just the parts which intentionally radiate RF energy.
- Software updates will be disallowed as well, even when they are clearly necessary to fix bugs and security holes in the original, certified firmware.

- Malicious actors (including such state-level actors as the NSA, GCHQ, Russia and China) will find and exploit holes unknown at the time of certification. This already occurs, due to the minimal effort manufacturers currently put into producing secure, high-quality firmware, but it will become difficult or impossible to close these holes subsequently, as is presently possible by installing third-party, actively-maintained firmware such as OpenWRT.

- Legitimate end-user modifications, including those performed by licenced amateur-radio operators (whose permitted frequencies overlap with the capabilities of many SDR devices), will be actively discouraged. Amateur radio has often proved invaluable during crises, including natural disasters and terrorist attacks; hampering its capabilities in this way could conceivably have fatal consequences.

- Research which requires firmware modifications will be severely hampered. One current focus of this research is improving the robustness and latency of wired and wireless networks through advanced queuing disciplines; this requires close integration with the relevant network hardware. For example: <http://www.bufferbloat.net/projects/codel/wiki/CakeTechnical>

- FCC-compliant devices will be unable to use the wider frequency ranges and higher powers that may be available in other jurisdictions.

- Devices sold abroad, but brought to the US by visitors, will radiate beyond the regulated limits (eg. on channels 12-14 in the 2.4GHz band), with no way for the user to prevent it, unless those capabilities are denied even in jurisdictions in which they are permitted.

- An entire class of innovative products may be stifled due to the increased regulatory burden.

It is worth emphasising that most recent Wi-Fi devices use SDR techniques, and thus fall under these proposed rules. One reasonable interpretation of the rules as presently proposed would encompass an entire laptop, including its operating system and applications, as the device for which software modifications are to be prevented. If this seems absurd - as it should - then there is clearly scope to define the rules more narrowly.

Ineffectiveness

=====

As noted above, Far East manufacturers do not have an intrinsic incentive to adopt genuine best practices with respect to software quality and security. While regulations can impose extrinsic incentives, these serve only to enforce the appearance of security, not its effect in practice. This inevitably leads to measures which impose at least as much inconvenience and frustration on end-users as a genuinely secure system would, but without noticeably impeding the efforts of experienced, motivated attackers.

Previous experience in this area can be seen in the Digital Rights Management sphere, where technologies such as corrupted floppy-disk sectors, DVD's CSS encryption, SecuROM, HDMI's HDCP et al have all been bypassed, some with greater ease than others. Of those mentioned, HDCP is both the least intrusive - most consumers are completely unaware of its operation - and stood the test of time best, but it too was eventually cracked. Some DRM technologies actively harmed the equipment of legitimate users, in pursuit of the extrinsic goal of copy-protection imposed by the entertainment industry, but were immediately bypassed by experienced "software pirates" - the supposed targets of the technology - who already routinely removed copy-protection software before repackaging the product for distribution.

The response of corporations to security breaches is also instructive, with regulations being necessary even to make them admit that a major consumer-privacy breach has occurred, and even then cover-ups undoubtedly still occur. This type of regulation is more difficult to extend to the Far East, where it would be required.

Typically, consumer devices of this type are based on a standard piece of hardware which, to simplify software development, has a variety of debugging interfaces included - generally including a serial console

and a JTAG debugger interface. While the connection headers are generally omitted from the final product for cost reasons, it is easy for an engineer or hacker to fit them manually, using a soldering iron. Instructions for doing so are widely circulated for legitimate purposes, such as porting OpenWRT to the wide range of new devices which regularly appear on the market. It seems highly unlikely that these interfaces can be modified or disabled in a way that would not also inhibit the manufacturer's own development practices. Hence, even if these debug interfaces become the only reliable way to modify firmware (thus removing this option from the general consumer), they will remain available to sufficiently motivated individuals and organisations.

Absence of Harm

=====

In proposing these rules, the FCC has not clearly articulated a specific harm that they could reasonably address. Only the "potential" for the originally licenced and certified emissions limits to be bypassed, with no evidence that this is already occurring or likely to occur in practice, and some images of interference caused to a handful of obsolete radar installations (which are already due for replacement) by devices already in the field - devices which can reasonably be assumed to be certified and compliant in any case, but whose emissions can in aggregate be detected by sensitive equipment.

Meanwhile, it is straightforward and inexpensive to construct devices which do emit harmful interference in the relevant bands, whether using SDR techniques or not. It is arguably easier to do so than to modify an existing device's firmware to do so, even without any technological restrictions on the latter.

There has also, surprisingly, been little or no mention of any harm caused by certified and compliant devices which have been configured for a foreign jurisdiction with more permissive regulations. For example, 2.4GHz channels 12 and 13 are available in the EU but not in the US; channel 14 is available only in Japan. Power limits also vary between regulatory domains. The volume of visitors to the US from these regions, and the general ignorance among consumers of these differences, implies that a significant amount of misconfigured radio equipment already exists in the US at any given time.

Alternatives

=====

I make the charitable assumption, here, that reducing the potential for accidental emissions beyond the regulated limits is a desirable goal. Here are some rules which address this goal while also retaining the ability to modify device firmware. This should reduce harms on both sides of the equation, as well as being more realistically practical to implement.

- Isolate the components of the radio responsible for the frequency and intensity of emissions from the rest of the system, and provide a narrow, clearly defined interface between the two. This reduces the attack surface, making these isolated components easier to secure. This isolation boundary may include, at maximum, the components of a distinct module such as a PCI Express card (which is currently the industry-standard method of attaching Wi-Fi radios to a device); preferably it would encompass only a minimal portion of that hardware.

- Store the firmware of the isolated components securely within those components, eliminating the dependence on the integrity of the larger device's software or firmware for compliance. The isolated components can then be certified separately from any device they may be attached to. It should, in this case, be possible to adjust certain parameters of the emission spectrum to cater for different regulatory domains; this could be done via a regulatory-domain configuration file uploaded through the defined interface, or via a simple numerical selector between such files stored within the firmware.

- Alternatively, integrate a cryptographic verification system within the isolated components, which ensures firmware loaded into the components is verified as authentic before use. This would allow updates to the firmware to be distributed after sale of the device, or different firmware to be loaded for different

regulatory domains, while still ensuring that only certified firmware is loaded.

- Alternatively, publish the firmware for the isolated components in a human-readable format, so that it can be audited for compliance and modified if necessary. It must then be straightforward to verify (through conversion of the human-readable version into device format) that the published firmware corresponds to that actually loaded into devices on sale. This option is the most beneficial for amateur-radio operators and researchers, since they would then be able to modify the firmware to meet their needs; they would of course assume liability for any regulatory compliance problems their modifications introduce.

The above rules specifically address the problem of potential harmful emissions at the RF level. But I would go further to reduce other harms, though these aspirations may require a separate round of rulemaking:

- Require device firmware to be demonstrably free of known security vulnerabilities at time of sale. This should include reference to design best-practices (such as verification of digital certificates used for secure communication, absence of fixed default passwords) in consultation with acknowledged software security experts, and reference to a database of known software vulnerabilities, such as the CVE series. There are well-established vulnerability scanners on the market which can be used to assist this process.

- Require device firmware to be updated, automatically and without the need for end-user attention, to fix defects (in the above category or otherwise) discovered after time of sale, for the expected lifetime of the device. This should, at minimum, extend to the ordinary manufacturer's warranty period of the last device of the type sold at retail, and preferably to the period of an extended warranty which might be sold for that device. This update process must also be demonstrably designed to be secure against man-in-the-middle hijack attempts.

- Require claims of functionality made in marketing material for the device (including but not limited to the packaging and manual) to have a verifiable basis in fact. In particular, it must be straightforward to quantifiably demonstrate the feature's functionality and benefits in a typical installation configuration in the laboratory, using only configuration options available to the user and (if relevant) described in the user manual.

- Require the ability to replace the manufacturer's software or firmware with any alternative from a third-party, given explicit and verified consent from the end-user (such as holding down a button during power-on to initiate the firmware reload). This would not necessarily include replacing the firmware of isolated radio components as described above. Exercising this ability would necessarily relieve the manufacturer of any liability related to problems with the firmware, unless the process is repeated to replace the third-party firmware with the original. This would enhance the ability of third-party firmware projects (such as DD-WRT and OpenWRT for consumer devices, or Linux on laptops) to take advantage of hardware advances.

The above requirements, if enforced, would go a long way to address the worrying state of consumer device security, especially with respect to the so-called "Internet of Things". In any case, without them any attempt to implement the rules on SDR as presently proposed are doomed to failure.

Thank you for your attention.

- Jonathan Morton

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: Schneider

Mailing Address: 200 S. Brentwood 2f

City: Clayton

Country: United States

State or Province: MO

ZIP/Postal Code: 63105

Email Address: xskills@me.com

Organization Name:

Comment: The EAELWD would deprive users of electronic devices the freedom to use license and royalty free firmware such as OpenWRT and the prerogative to use open source code/free software on personal devices.

The EAELWD would deprive users of electronic devices the freedom to use license and royalty free firmware such as OpenWRT and the prerogative to use open source code/free software on personal 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: Chase

Last Name: Holt

Mailing Address: 4680 E 145 St S

City: Bixby

Country: United States

State or Province: OK

ZIP/Postal Code: 74008

Email Address: cellioth@gmail.com

Organization Name:

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

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

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Patrick

Last Name: O'Connor

Mailing Address: 11691 N Dragoon Springs DR

City: Tucson

Country: United States

State or Province: AZ

ZIP/Postal Code: 85737

Email Address:

Organization Name:

Comment: This legislation will greatly imperil internet security. Embedded devices are becoming much more ubiquitous and with that consumers are becoming much more susceptible to identity theft. Cell phone & router manufacturers have a dismal track record for patching vulnerable software on their devices. And even if some companies take responsibility for the software they sell on their embedded electronics, many companies go out of business. This is a very competitive market.

The ability for people to legally flash the software on devices they purchase is not just a consumer choice issue but data security issue, which has implications for personal privacy, national security, public safety.

This legislation will greatly imperil internet security. Embedded devices are becoming much more ubiquitous and with that consumers are becoming much more susceptible to identity theft. Cell phone & router manufacturers have a dismal track record for patching vulnerable software on their devices. And even if some companies take responsibility for the software they sell on their embedded electronics, many companies go out of business. This is a very competitive market.

The ability for people to legally flash the software on devices they purchase is not just a consumer choice issue but data security issue, which has implications for personal privacy, national security, public safety.

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: Josip

Last Name: Sagaj

Mailing Address: Vally-Weigl-Gasse 1/2/9

City: Vienna / Wien

Country: Austria

State or Province: Vienna

ZIP/Postal Code: A-1100

Email Address:

Organization Name:

Comment: The third party firmware market is a driving force for innovation and product functionality. A lot of (perfectly legal and harmless) product features first started in a third party firmware product, and was eventually integrated into manufacturer's official firmware.

While some of these projects can indeed provide functionalities that allow for circumventing channel and power output limitations, that does not mean that the entire third party firmware market is doing so.

It is my belief, both as a long-time user and a third party firmware developer myself that forcing manufacturers to flat out prevent the flashing of a third party firmware will be harmful to the market, and deny end users of choice (for cases where an original manufacturer's firmware would be devoid of advanced features and/or contain unfixed security holes and/or has software defects and/or are no longer being supported by the original manufacturer.

Therefore, I recommend that the scope of these rules be reduced to only ensuring that the radio components are operating within the legal parameters, possibly by shifting the solution to a hardware limitation, rather than a software limitation.

The third party firmware market is a driving force for innovation and product functionality. A lot of (perfectly legal and harmless) product features first started in a third party firmware product, and was eventually integrated into manufacturer's official firmware.

While some of these projects can indeed provide functionalities that allow for circumventing channel and power output limitations, that does not mean that the entire third party firmware market is doing so.

It is my belief, both as a long-time user and a third party firmware developer myself that forcing manufacturers to flat out prevent the flashing of a third party firmware will be harmful to the market, and deny end users of choice (for cases where an original manufacturer's firmware would be devoid of advanced features and/or contain unfixed security holes and/or has software defects and/or are no longer being supported by the original manufacturer.

Therefore, I recommend that the scope of these rules be reduced to only ensuring that the radio components are operating within the legal parameters, possibly by shifting the solution to a hardware limitation, rather than a software limitation.

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: Denis

Last Name: Pastukhov

Mailing Address: Moscow

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: Moscow

Email Address: Denis.Pastukhov@gmail.com

Organization Name:

Comment: This law does not take into account the opinion of third-party software vendors and extremely damaging to competition, which will lead to stagnation and slowdown in the industry

This law does not take into account the opinion of third-party software vendors and extremely damaging to competition, which will lead to stagnation and slowdown in the industry

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Tecklenburg

Mailing Address: 3911 145th ST SE

City: Mill Creek

Country: United States

State or Province: WA

ZIP/Postal Code: 98012

Email Address: daveandglenda@yahoo.com

Organization Name: N/A

Comment: Isn't this proposal infringing upon current computing users rights? At this point in time, today's users of most computing devices have had the ability to install the software of their choice. Examples include the ability to install free and open source operating systems and other application software which most appropriately fits the users own specific needs. That would include installing open source router software such as OpenWrt or installing a Linux kernel on their laptop or smartphone. This is the ability of users to control what their computing devices do for them and limits somebody else from controlling that user experience. To some extent, experienced users can aid in protecting themselves from uninvited guests through their own initiative and not have to rely on the manufacturer to provide that capability for as long as they choose to own and use that computing device.

This rule will also interfere with legitimate innovations in the wireless space. Innovation in network and wireless technology depends on the ability of users and resellers to experiment with software and hardware at all levels. An example of this is CeroWrt. It is open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix has been to the Linux kernel to be used by the millions of users of Linux.

It would also seem that many of the over 7,000 scholarly articles on wireless networking technologies that reference open and modifiable hardware would be banned under these rules.

User-access to source code is another innovation process that has led to numerous bug fixes, security enhancements, and features that were not part of the original code base for many products. There are many documented cases where users took it upon themselves to fix bugs that manufacturers were ignoring. This could not have been possible had the source code for the firmware been unavailable or had these devices otherwise been locked.

Numerous companies modify the software on off-the-shelf wireless devices for custom uses. Companies who sell hardware to retailers for WiFi hotspots often install software customized to that task. Additionally 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. It also seems that some companies are wanting this to protect themselves from legitimate competition.

Isn't this proposal infringing upon current computing users rights? At this point in time, today's users of most computing devices have had the ability to install the software of their choice. Examples include the ability to install free and open source operating systems and other application software which most appropriately fits the users own specific needs. That would include installing open source router software such as OpenWrt or installing a Linux kernel on their laptop or smartphone. This is the ability of users to control what their computing devices do for them and limits

somebody else from controlling that user experience. To some extent, experienced users can aid in protecting themselves from uninvited guests through their own initiative and not have to rely on the manufacturer to provide that capability for as long as they choose to own and use that computing device.

This rule will also interfere with legitimate innovations in the wireless space. Innovation in network and wireless technology depends on the ability of users and resellers to experiment with software and hardware at all levels. An example of this is CeroWrt. It is open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is has been to the Linux kernel to be used by the millions of users of Linux.

It would also seem that many of the over 7,000 scholarly articles on wireless networking technologies that reference open and modifiable hardware would be banned under these rules.

User-access to source code is another innovation process that has led to numerous bug fixes, security enhancements, and features that were not part of the original code base for many products. There are many documented cases where users took it upon themselves to fix bugs that manufacturers were ignoring. This could not have been possible had the source code for the firmware been unavailable or had these devices otherwise been locked.

Numerous companies modify the software on off-the-shelf wireless devices for custom uses. Companies who sell hardware to retailers for WiFi hotspots often install software customized to that task. Additionally 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. It also seems that some companies are wanting this to protect themselves from legitimate competition.

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: Greene

Mailing Address: 9246 Cazador St

City: Las Vegas

Country: United States

State or Province: NV

ZIP/Postal Code: 89123

Email Address: keith.greene@gmail.com

Organization Name:

Comment: This is a very short-sighted and potentially devastating proposal. Preventing people from installing their own software/firmware on devices THEY OWN will cause nothing but trouble. DON'T DO IT.

This is a very short-sighted and potentially devastating proposal. Preventing people from installing their own software/firmware on devices THEY OWN will cause nothing but trouble. DON'T DO IT.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Renard

Last Name: Dellafave

Mailing Address: 7113 Summerland Dr.

City: Raleigh

Country: United States

State or Province: NC

ZIP/Postal Code: 27612

Email Address: radellaf@gmail.com

Organization Name:

Comment: The FCC should not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

- * Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- * Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- * Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- * 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.
- * There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

The FCC should not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

- * Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- * Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- * Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- * 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.
- * There is no evidence that open-source firmware has caused any more wireless interference than closed-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: Nathaniel

Last Name: Gray

Mailing Address: 1940 Pawlet Dr.

City: Crofton

Country: United States

State or Province: MD

ZIP/Postal Code: 21114

Email Address: nathaniel.gray@gmail.com

Organization Name:

Comment: Software defined radios are too vaguely defined. The concept of a wireless device is not limited to wireless internet access points.

Mobile ad hoc network seen in areas where governments have disrupted normal Wi-Fi and GSM communications rely on open hardware and software defined radios to restore communication.

Without these ad hoc mesh networks the disruption of free speech is just as simple as turning off the devices protected in this proposal.

Within the scope proposed I believe Equipment Authorization and Electronic Labeling for Wireless Devices will violate the First and Second Amendments of the US Constitution in even the lightest restrictions.

The right and to ability peacefully assemble, report on actions taken by governments, and communicate to our loved ones depend on protecting the use of software defined radios from US government restrictions.

Software defined radios are too vaguely defined. The concept of a wireless device is not limited to wireless internet access points.

Mobile ad hoc network seen in areas where governments have disrupted normal Wi-Fi and GSM communications rely on open hardware and software defined radios to restore communication.

Without these ad hoc mesh networks the disruption of free speech is just as simple as turning off the devices protected in this proposal.

Within the scope proposed I believe Equipment Authorization and Electronic Labeling for Wireless Devices will violate the First and Second Amendments of the US Constitution in even the lightest restrictions.

The right and to ability peacefully assemble, report on actions taken by governments, and communicate to our loved ones depend on protecting the use of software defined radios from US government restrictions.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: M. Oliver

Last Name: Ghingold

Mailing Address: 50 Renihan Meadows

City: Lebanon

Country: United States

State or Province: NH

ZIP/Postal Code: 03766

Email Address:

Organization Name:

Comment: We already have enough device makers locking down the firmware on their devices WITHOUT a legal compulsion to do so. All these proposed rules do is give license to manufacturers to lock out users from controlling the products that they buy. If you do a five second web search you will kindly take note that this will NOT make consumer hardware any less vulnerable to being compromised by malicious software. It will ONLY prevent lawful uses of individual devices.

If you are even faintly capable of doing your job, DO NOT PASS THESE RULES AS-WRITTEN:

(0) The FCC should NOT implement rules that take away the ability of users to install the software of their choosing on their computing devices. THIS SHOULD BE THE ONLY REASON YOU NEED TO READ TO SCRAP THIS PROPOSAL.

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

How dare you even consider this, you incompetent, myopic, stooges.

We already have enough device makers locking down the firmware on their devices WITHOUT a legal compulsion to do so. All these proposed rules do is give license to manufacturers to lock out users from controlling the products that they buy. If you do a five second web search you will kindly take note that this will NOT make consumer hardware any less vulnerable to being compromised by malicious software. It will ONLY prevent lawful uses of individual devices.

If you are even faintly capable of doing your job, DO NOT PASS THESE RULES AS-WRITTEN:

(0) The FCC should NOT implement rules that take away the ability of users to install the software of their choosing on their computing devices. THIS SHOULD BE THE ONLY REASON YOU NEED TO READ TO SCRAP THIS PROPOSAL.

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

How dare you even consider this, you incompetent, myopic, stooges.

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: Patricia

Last Name: Maples

Mailing Address: 175 India Street, Apt. 1

City: Brooklyn

Country: United States

State or Province: NY

ZIP/Postal Code: 11222

Email Address:

Organization Name:

Comment: Please reconsider making the modification of routers illegal. If I understand the hardware correctly, the CPU and the radio are built together. Banning mods on one prevents making mods to the other. The FCC should consult a broader range of specialists, especially those working in open-source software, before making proposals such as this one. Those of the US public who actually know enough about these subjects to care grow increasingly tired of the incremental encroachment upon our rights of ownership. If I buy it, I want to be able to hack it and mod it. I should be able to add the software of my choice. Tech advances, personal safety and privacy, and business opportunity (WiFi hotspots, etc.) all rely on the ability to investigate and modify devices. Thank you for your consideration.

Please reconsider making the modification of routers illegal. If I understand the hardware correctly, the CPU and the radio are built together. Banning mods on one prevents making mods to the other. The FCC should consult a broader range of specialists, especially those working in open-source software, before making proposals such as this one. Those of the US public who actually know enough about these subjects to care grow increasingly tired of the incremental encroachment upon our rights of ownership. If I buy it, I want to be able to hack it and mod it. I should be able to add the software of my choice. Tech advances, personal safety and privacy, and business opportunity (WiFi hotspots, etc.) all rely on the ability to investigate and modify devices. 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: James

Last Name: Bremenour

Mailing Address: 25 Sunnyside Dr. Apt. 1E

City: Yonkers

Country: United States

State or Province: NY

ZIP/Postal Code: 10705-1732

Email Address: Bremenour@gmail.com

Organization Name:

Comment: Please refrain from implementing rules that would inhibit the ability of users to install software of their choosing on their devices. I realize that the ability of the proposed rules to have such an impact is contested, but I have only learned of them recently and have not had time to scrutinize them to my satisfaction. I, therefore, have cherry-picked some talking points concerning the proposal that I feel are important in the event that NPRM might impinge upon them.

"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." Arcesilus,
<https://www.voat.co/v/technology/comments/460322>

Additionally: "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." <https://archive.is/tGCKU#selection-143.1-155.175>

Thank you for your time and attention.

Please refrain from implementing rules that would inhibit the ability of users to install software of their choosing on their devices. I realize that the ability of the proposed rules to have such an impact is contested, but I have only learned of them recently and have not had time to scrutinize them to my satisfaction. I, therefore, have cherry-picked some talking points concerning the proposal that I feel are important in the event that NPRM might impinge upon them.

"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." Arcesilus,
<https://www.voat.co/v/technology/comments/460322>

Additionally: "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." <https://archive.is/tGCKU#selection-143.1-155.175>

Thank you for your time and attention.

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: Arianne

Last Name: Spurlock

Mailing Address: 2323 Bear Springs Dr Apt 1902

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78245

Email Address: zarniwoop626@hotmail.com

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of our choosing on our 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.

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.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Please do not implement rules that take away the ability of users to install the software of our choosing on our 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.

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.

There is no evidence that open-source firmware has caused any more wireless interference than closed-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: Ryan

Last Name: Flaherty

Mailing Address: 134 Adelaide Oaks

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78249

Email Address: t3kk.driverchief@gmail.com

Organization Name:

Comment: Please do not do this. Being able to modify our own devices is a good thing. Protect the airwaves some other way please.

Please do not do this. Being able to modify our own devices is a good thing. Protect the airwaves some other way please.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Nathan

Last Name: Bonsal

Mailing Address: 3405 Martin Meadows Drive

City: Rio Rancho

Country: United States

State or Province: NM

ZIP/Postal Code: 87144

Email Address: nathanbonsal@gmail.com

Organization Name:

Comment: The FCC has no authority to enact this rule because it conflicts with various rulings on consumer choice, and falls afoul of the burden of proof standards of our justice system- that is, that without proof that a particular version of software violates some FCC rule with applicability to RF power, RF emissions out-of-band or in some other way out of character with the FCC authorization previously granted to the hardware, the FCC may not restrict the use of software.

Certainly, with software-defined-radio applications, the FCC license for the hardware is granted for the software as well, in situations where the software's treatment of hardware is a part of its compliance behavior, however, with system-on-a-chip type wifi solutions in PCs, routers, and other devices, there is no expectation that alteration of software or firmware will cause noncompliant emissions.

This action is transparently not a part of the FCC's charter, but is instead being ordered by intelligence agencies who would like to restrict OS and router behavior such that the currently installed access protocols for NSA interference with device security are preserved, a position only necessary for a police-state government which believes that the 4th amendment does not apply because they really feel that they could make us all safer if only the 4th Amendment was never written. Well, it HAS been written, and if you don't like it, you'll need 2/3rds of the House, 2/3rds of the Senate, and 3/4ths of the state legislatures to get rid of it. Good luck.

Such legislation would also prevent timely patches to router firmware in the case of a zero-day attack, as closed-source router firmware forces the user agency to be at the mercy of the router manufacturer, which may be defunct.

The FCC has no authority to enact this rule because it conflicts with various rulings on consumer choice, and falls afoul of the burden of proof standards of our justice system- that is, that without proof that a particular version of software violates some FCC rule with applicability to RF power, RF emissions out-of-band or in some other way out of character with the FCC authorization previously granted to the hardware, the FCC may not restrict the use of software.

Certainly, with software-defined-radio applications, the FCC license for the hardware is granted for the software as well, in situations where the software's treatment of hardware is a part of its compliance behavior, however, with system-on-a-chip type wifi solutions in PCs, routers, and other devices, there is no expectation that alteration of software or firmware will cause noncompliant emissions.

This action is transparently not a part of the FCC's charter, but is instead being ordered by intelligence agencies who would like to restrict OS and router behavior such that the currently installed access protocols for NSA interference with

device security are preserved, a position only necessary for a police-state government which believes that the 4th amendment does not apply because they really feel that they could make us all safer if only the 4th Amendment was never written. Well, it HAS been written, and if you don't like it, you'll need 2/3rds of the House, 2/3rds of the Senate, and 3/4ths of the state legislatures to get rid of it. Good luck.

Such legislation would also prevent timely patches to router firmware in the case of a zero-day attack, as closed-source router firmware forces the user agency to be at the mercy of the router manufacturer, which may be defunct.

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: Benjamin

Last Name: Hahl

Mailing Address: 1415 Webster St. #302

City: Alameda

Country: United States

State or Province: CA

ZIP/Postal Code: 94501

Email Address: benhahl@gmail.com

Organization Name:

Comment: To the FCC,

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

Sincerely,
Benjamin Hahl

To the FCC,

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

Sincerely,
Benjamin Hahl

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: Stephen

Last Name: Albert

Mailing Address: 1187 Woodland Road Exd

City: Petersburg

Country: United States

State or Province: VA

ZIP/Postal Code: 23805

Email Address: stephen.a.albert@gmail.com

Organization Name:

Comment: Please do not violate user freedom by locking down computers!

People need to own their computing devices. This requires the freedom to run *any* software on them. If the user uses a particular piece of software to commit an illegal act, then of course their actions should be punished. But by prohibiting the installation of any software other than the manufacturer's, the FCC is eliminating freedom for all based on potential abuse by a few.

This is dangerous in itself, but it also sets an extremely dangerous precedent for the future of computing. A wireless router or a mobile phone radio is a computing device at its core. Of course computers can be used to violate regulations or break laws - that's been true since the beginning of computing. But taking away the freedom of the user to run the software of their choice has never been the answer, and it never will be.

I stand for user freedom, along with the Electronic Frontier Foundation and the Free Software Foundation, to save WiFi and other RF computing from this proposed attack on users.

Please do not violate user freedom by locking down computers!

People need to own their computing devices. This requires the freedom to run *any* software on them. If the user uses a particular piece of software to commit an illegal act, then of course their actions should be punished. But by prohibiting the installation of any software other than the manufacturer's, the FCC is eliminating freedom for all based on potential abuse by a few.

This is dangerous in itself, but it also sets an extremely dangerous precedent for the future of computing. A wireless router or a mobile phone radio is a computing device at its core. Of course computers can be used to violate regulations or break laws - that's been true since the beginning of computing. But taking away the freedom of the user to run the software of their choice has never been the answer, and it never will be.

I stand for user freedom, along with the Electronic Frontier Foundation and the Free Software Foundation, to save WiFi and other RF computing from this proposed attack on users.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: Smith

Mailing Address: 107 Hilltop Drive

City: Weatogue

Country: United States

State or Province: CT

ZIP/Postal Code: 06089

Email Address:

Organization Name:

Comment: This law is significantly too broad, and could be used to abuse and hinder open-source projects upon which many entities (including the United States Government) relies on.

The modification of firmware on devices is of important economic value, so much so that Linksys/Cisco continues to sell a 13-year-old router specifically designed for such modifications. This device is based on open-source software, and might not exist were this law enacted before the router's creation.

Security experts will potentially be blocked from doing legitimate security research to protect important health and safety systems because they cannot modify devices as an attacker would.

Consumers will be at the mercy of corporations, including foreign entities that might have malicious intent.

In 2010, Dell discovered malware on important replacement components (motherboards) buried in the firmware. This could be true of *any* firmware, and it would be up to manufacturers to detect and repair the problem in millions of machines. In an era where software and hardware manufacturers may take weeks, months, or even years to fix security problems, this is entirely unacceptable. Consumers must be able to remedy such problems freely on their own.

These restrictions would endanger Americans. Do not enact them.

This law is significantly too broad, and could be used to abuse and hinder open-source projects upon which many entities (including the United States Government) relies on.

The modification of firmware on devices is of important economic value, so much so that Linksys/Cisco continues to sell a 13-year-old router specifically designed for such modifications. This device is based on open-source software, and might not exist were this law enacted before the router's creation.

Security experts will potentially be blocked from doing legitimate security research to protect important health and safety systems because they cannot modify devices as an attacker would.

Consumers will be at the mercy of corporations, including foreign entities that might have malicious intent.

In 2010, Dell discovered malware on important replacement components (motherboards) buried in the firmware. This could be true of *any* firmware, and it would be up to manufacturers to detect and repair the problem in millions of machines. In an era where software and hardware manufacturers may take weeks, months, or even years to fix security

problems, this is entirely unacceptable. Consumers must be able to remedy such problems freely on their own.

These restrictions would endanger Americans. Do not enact them.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Wilson

Mailing Address: 100 N Lakewood Ave

City: Baltimore

Country: United States

State or Province: MD

ZIP/Postal Code: 21224

Email Address: drwils01@gmail.com

Organization Name:

Comment: Please do not implement these rules on any devices. This proposal will be highly detrimental to innovation, the open source community and society as a whole. Locking down all devices with cellular radios limits the ability of legitimate researchers to develop new network technologies as well as explore existing technology for flaws that leave networks exposed to hackers.

Furthermore, many device manufacturers fail to update released device software after as little as 12 months. Locking down the software on the device would then expose consumers to flaws in the software that they could otherwise patch themselves with open sourced solutions. In mobile phone firmware in particular, aftermarket ROMs for android smartphones can extend the life and functionality of the phones greatly.

Please reject this proposal and do not sacrifice all the hard work and innovation Americans depend on for our economic success in technology centric fields.

Please do not implement these rules on any devices. This proposal will be highly detrimental to innovation, the open source community and society as a whole. Locking down all devices with cellular radios limits the ability of legitimate researchers to develop new network technologies as well as explore existing technology for flaws that leave networks exposed to hackers.

Furthermore, many device manufacturers fail to update released device software after as little as 12 months. Locking down the software on the device would then expose consumers to flaws in the software that they could otherwise patch themselves with open sourced solutions. In mobile phone firmware in particular, aftermarket ROMs for android smartphones can extend the life and functionality of the phones greatly.

Please reject this proposal and do not sacrifice all the hard work and innovation Americans depend on for our economic success in technology centric fields.

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: Smith

Mailing Address: 12345 Street

City: St. Paul

Country: United States

State or Province: MN

ZIP/Postal Code: 55555

Email Address:

Organization Name:

Comment: Please do not restrict firmware. Let people use the devices they purchase in the way they would like.

Please do not restrict firmware. Let people use the devices they purchase in the way they would like.

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: Bob

Last Name: Iannaccone

Mailing Address: 1686 Garfield St.

City: Ferndale

Country: United States

State or Province: MI

ZIP/Postal Code: 48220

Email Address: riannaccone@gmail.com

Organization Name: null

Comment: To Whom It may concern:

I would like to urge you NOT to implement the section of the proposed rule that would limit user's ability to run custom firmware on their networking hardware (such as routers, modems, switches). A huge community has sprung up around custom firmware for these devices, often times fixing bugs that the manufacturer neglects. I personally have done this on many networking components and the custom firmwares have always been an improvement. Locking users out of their own equipment isn't only unethical, but it will lead to a less secure internet.

Thank you for your time and for taking my comment into consideration.

To Whom It may concern:

I would like to urge you NOT to implement the section of the proposed rule that would limit user's ability to run custom firmware on their networking hardware (such as routers, modems, switches). A huge community has sprung up around custom firmware for these devices, often times fixing bugs that the manufacturer neglects. I personally have done this on many networking components and the custom firmwares have always been an improvement. Locking users out of their own equipment isn't only unethical, but it will lead to a less secure internet.

Thank you for your time and for taking my comment into 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: Erich

Last Name: Keyes

Mailing Address: 3455 Rockway Ave

City: Annapolis

Country: United States

State or Province: MD

ZIP/Postal Code: 21403

Email Address: linearboy@gmail.com

Organization Name: The people

Comment: Hi Please do not lock down the WiFi Routers or regulation the bands use for WiFi.

Open and free software is wave of future please do lock down the future. I thank Wifi are part 15 devices are more Regulations needed ? I am Amateur radio Op (N3JGH) and Linux user.

Thank You

Erich Keyes

Hi Please do not lock down the WiFi Routers or regulation the bands use for WiFi.

Open and free software is wave of future please do lock down the future. I thank Wifi are part 15 devices are more Regulations needed ? I am Amateur radio Op (N3JGH) and Linux user.

Thank You

Erich Keyes

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: Marc

Last Name: Harper

Mailing Address: 8063 Redlands St #305

City: Playa del Rey

Country: United States

State or Province: CA

ZIP/Postal Code: 90293

Email Address:

Organization Name:

Comment: As a technology professional, I oppose these restrictions on the following grounds:

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

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

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

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

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

As a technology professional, I oppose these restrictions on the following grounds:

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

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

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

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

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.

The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jordan

Last Name: Yerkes

Mailing Address: 4049 Texas St

City: San Diego

Country: United States

State or Province: CA

ZIP/Postal Code: 92104

Email Address: jkyerkes@gmail.com

Organization Name:

Comment: Under the guise of "streamlining", "promoting significant cost savings", "reducing burdens", these rules are an attack on consumer communications. Please protect the consumer's right to control of their own communications and do not pass these regulations.

Under the guise of "streamlining", "promoting significant cost savings", "reducing burdens", these rules are an attack on consumer communications. Please protect the consumer's right to control of their own communications and do not pass these regulations.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Morgan

Last Name: Jones

Mailing Address: 2547 S. Milwaukee St

City: Denver

Country: United States

State or Province: CO

ZIP/Postal Code: 80210

Email Address:

Organization Name:

Comment: I am a monetary supporter of the DD-WRT project, a community-supported project to replace router firmware with a more feature-complete version.

Making router flashing against FCC regulations would prevent community innovation, similar to how bootloader locking on phones prevents end users from completely owning their phones.

I would urge the FCC to consider the open-source community and the innovation and collaboration that gave us projects like DD-WRT.

I am a monetary supporter of the DD-WRT project, a community-supported project to replace router firmware with a more feature-complete version.

Making router flashing against FCC regulations would prevent community innovation, similar to how bootloader locking on phones prevents end users from completely owning their phones.

I would urge the FCC to consider the open-source community and the innovation and collaboration that gave us projects like DD-WRT.

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: Eddie

Last Name: T

Mailing Address: 123 No

City: Somewhere

Country: United States

State or Province: FL

ZIP/Postal Code: 12345

Email Address:

Organization Name:

Comment: Are you people smoking crack?

Did you even think about people's jobs finding major bugs in shitty firmware that won't get updated? Or, how many fucking HORRIBLE firmware exists already, and now you're trying to cut off it's updates, so we're all as vulnerable as the government.

You didn't? Well, you can go fuck yourself, I will install whatever I want on whatever wifi device I want.

Thanks for nothing FCC.

Are you people smoking crack?

Did you even think about people's jobs finding major bugs in shitty firmware that won't get updated? Or, how many fucking HORRIBLE firmware exists already, and now you're trying to cut off it's updates, so we're all as vulnerable as the government.

You didn't? Well, you can go fuck yourself, I will install whatever I want on whatever wifi device I want.

Thanks for nothing FCC.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Rolf

Last Name: Freitag

Mailing Address: Jahnstrasse 11

City: Aalen

Country: Germany

State or Province: Baden-Wuerttemberg

ZIP/Postal Code: 73431

Email Address: nobodyo@webd

Organization Name:

Comment: I want to control the devices i own and that includes the firmware and software. I do not want backdoors and bugs. And i want to have the right to choose the firmware i want.

I want to control the devices i own and that includes the firmware and software. I do not want backdoors and bugs. And i want to have the right to choose the firmware i want.

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: Cziryak

Mailing Address: 2904 Hilltop Dr

City: Parma

Country: United States

State or Province: OH

ZIP/Postal Code: 44134

Email Address: acziryak@gmail.com

Organization Name:

Comment: Don't be a fool.

Don't be a fool.

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: Sutton

Last Name: Hathorn

Mailing Address: 354 S Grant St Apt 3

City: West Lafayette

Country: United States

State or Province: IN

ZIP/Postal Code: 47906

Email Address: srhathorn@gmail.com

Organization Name:

Comment: The ability to place non-OEM firmware on networking equipment is absolutely necessary to ensure that security and functionality issues are fixed. Wireless router manufacturers often abandon development for old hardware quickly leading to its obsolescence. Allowing for alternative open source software to run on these devices prevents their disposal and also improves the online safety of the users.

The FCC needs to avoid the heavy handed approach of needlessly banning all custom firmware and instead look for more prudent and enforceable solutions. This proposed rule only serves to punish the users that abide by the rules and will not prevent anyone from transmitting on others licensed spectrum. Removing the options for non-OEM tested firmware will not prevent the problem the FCC is attempting to address since the individuals who are willing to violate FCC regulations will continue to find a way to do so.

Don't punish everyone for the intentions of a few, especially if that punishment won't stop the perpetrators from continuing to commit crimes.

The ability to place non-OEM firmware on networking equipment is absolutely necessary to ensure that security and functionality issues are fixed. Wireless router manufacturers often abandon development for old hardware quickly leading to its obsolescence. Allowing for alternative open source software to run on these devices prevents their disposal and also improves the online safety of the users.

The FCC needs to avoid the heavy handed approach of needlessly banning all custom firmware and instead look for more prudent and enforceable solutions. This proposed rule only serves to punish the users that abide by the rules and will not prevent anyone from transmitting on others licensed spectrum. Removing the options for non-OEM tested firmware will not prevent the problem the FCC is attempting to address since the individuals who are willing to violate FCC regulations will continue to find a way to do so.

Don't punish everyone for the intentions of a few, especially if that punishment won't stop the perpetrators from continuing to commit crimes.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Scott

Last Name: Parish

Mailing Address: 1141 Laforest Dr SE

City: North Bend

Country: United States

State or Province: WA

ZIP/Postal Code: 98045

Email Address: srparish@gmail.com

Organization Name:

Comment: Please don't implement rules that limit my ability to install software of my choice on my computational hardware. It's important that I'm able to use software that implements features that hardware manufactures don't support such as custom traffic shaping. It's also important that I can continue to keep my software up to date with the latest security updates without having to wait for the hardware manufacture, who may choose to ignore security exploits for older hardware, leaving me at security risk. Finally, as a software developer, it's very important that custom software can be installed for research and educational purposes.

Please don't implement rules that limit my ability to install software of my choice on my computational hardware. It's important that I'm able to use software that implements features that hardware manufactures don't support such as custom traffic shaping. It's also important that I can continue to keep my software up to date with the latest security updates without having to wait for the hardware manufacture, who may choose to ignore security exploits for older hardware, leaving me at security risk. Finally, as a software developer, it's very important that custom software can be installed for research and educational purposes.

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: Alexander

Last Name: Pechlivanos

Mailing Address: 4343 Beverly Drive

City: Toledo

Country: United States

State or Province: OH

ZIP/Postal Code: 43614

Email Address: apechlivanos@gmail.com

Organization Name:

Comment: This proposal would effectively make it impossible for users to install custom firmwarw on their own property. The government and more specifically the FCC shouldn't have the right to be able to tell me what I can and can't install on my personal property.

This proposal would effectively make it impossible for users to install custom firmwarw on their own property. The government and more specifically the FCC shouldn't have the right to be able to tell me what I can and can't install on my personal property.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Daniel

Last Name: Toon

Mailing Address: 409 River Run Dr

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30350

Email Address:

Organization Name:

Comment: While significant changes have occurred in technology and use of Wifi communications, the users of these devices still fall in simple groups, those who use an item out of the box and enthusiast users who seek to use the maximum legal potential of a piece of personal property.

If communication devices are limited to thresholds suitable for most users and prevented from further use by those aware of their legal potential, the market will split and a demand for enthusiast hardware will develop and likely not be served by the regulated market.

If the FCC desires to increase or create a grey or black market for wireless communications items, it seems to be working against its founding principles.

When staying within the law, using broadcast equipment to its appropriate limit poses no harm and speculating about inappropriate use to restrict or alter future products is absurd if not paranoid.

Please use enforcement dollars to restrict the activities of those not using products in a legal manner rather than restrict future products from being useful at all.

While significant changes have occurred in technology and use of Wifi communications, the users of these devices still fall in simple groups, those who use an item out of the box and enthusiast users who seek to use the maximum legal potential of a piece of personal property.

If communication devices are limited to thresholds suitable for most users and prevented from further use by those aware of their legal potential, the market will split and a demand for enthusiast hardware will develop and likely not be served by the regulated market.

If the FCC desires to increase or create a grey or black market for wireless communications items, it seems to be working against its founding principles.

When staying within the law, using broadcast equipment to its appropriate limit poses no harm and speculating about inappropriate use to restrict or alter future products is absurd if not paranoid.

Please use enforcement dollars to restrict the activities of those not using products in a legal manner rather than restrict future products from being useful at all.

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: Samuel

Last Name: Reaves III

Mailing Address: 121 Oak Ridge Drive

City: Stephens City

Country: United States

State or Province: VA

ZIP/Postal Code: 22655

Email Address: sam.reaves@gmail.com

Organization Name: W3OHM - Amateur Radio Station

Comment: Infringing upon computing users rights

Until now, users of computing devices have had the ability to install the software of their choice. In particular, users have had the ability to install free and open source operating systems and software which most appropriately fits their needs. Whether the user wants to install OpenWrt on a router or a distribution based upon the Linux kernel on their laptop computer or smartphone, users have been able to control the devices they own. Through this control, users can explore how their computing devices work, educate themselves on the design of hardware, protect themselves from invasive spying by competitors and foreign governments and enrich their own lives and the lives of others through improved software.

Interfering with innovation in the wireless space

Innovation in network and wireless technology depends on the ability of users and resellers 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.

Mesh networking technologies for developing stable distributed internet access are regularly implemented using various versions of Linux installed by an end-user 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. Mesh networking is used for data communication by amateur radio operators responding to natural disasters. Without the ability to change the software on the device, these innovations would not have occurred.

User-access to source code is another innovation in and of itself. It has led to bug fixes, security enhancements, and features that were not part of the original code base. In one instance a user was able to fix a critical bug impacting all wifi adapters based on a particular set of Qualcomm Atheros wireless chipset(s). As users were frequently being disconnected under certain conditions one user took it upon themselves to track down and fix the bug [1]. This would not have been possible had the source code for the firmware been unavailable, or had these devices otherwise been locked.

Finally, numerous companies modify the software on off-the-shelf wireless devices for custom uses. Companies who sell hardware to retailers for WiFi hotspots often install software customized to that task. Additionally many commercial VPN providers sell wireless routers as part of there 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.

The regulations on software defined radios should not restrict the ability to replace software on computing devices

As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law abiding users to understand and improve the software on their devices.

The regulations on e-labels should not restrict the ability to replace software on computing devices

I understand and appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

Infringing upon computing users rights

Until now, users of computing devices have had the ability to install the software of their choice. In particular, users have had the ability to install free and open source operating systems and software which most appropriately fits their needs. Whether the user wants to install OpenWrt on a router or a distribution based upon the Linux kernel on their laptop computer or smartphone, users have been able to control the devices they own. Through this control, users can explore how their computing devices work, educate themselves on the design of hardware, protect themselves from invasive spying by competitors and foreign governments and enrich their own lives and the lives of others through improved software.

Interfering with innovation in the wireless space

Innovation in network and wireless technology depends on the ability of users and resellers 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.

Mesh networking technologies for developing stable distributed internet access are regularly implemented using various versions of Linux installed by an end-user 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. Mesh networking is used for data communication by amateur radio operators responding to natural disasters. Without the ability to change the software on the device, these innovations would not have occurred.

User-access to source code is another innovation in and of itself. It has led to bug fixes, security enhancements, and features that were not part of the original code base. In one instance a user was able to fix a critical bug impacting all wifi adapters based on a particular set of Qualcomm Atheros wireless chipset(s). As users were frequently being disconnected under certain conditions one user took it upon themselves to track down and fix the bug [1]. This would not have been possible had the source code for the firmware been unavailable, or had these devices otherwise been locked.

Finally, numerous companies modify the software on off-the-shelf wireless devices for custom uses. Companies who sell hardware to retailers for WiFi hotspots often install software customized to that task. Additionally many commercial VPN providers sell wireless routers as part of there 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.

The regulations on software defined radios should not restrict the ability to replace software on computing devices

As written, the regulations require that manufacturers prevent modification of all software computing devices which use

software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law abiding users to understand and improve the software on their devices.

The regulations on e-labels should not restrict the ability to replace software on computing devices

I understand and appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

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: Vernon

Mailing Address: 6 Moorlands Westwoodside

City: Doncaster

Country: United Kingdom

State or Province: Youth Yorkshire

ZIP/Postal Code: DN9 2HB

Email Address:

Organization Name:

Comment: This legislation poses a huge and substantial threat to the open source world. If it were to become illegal to put open source software on devices with a wifi antenna it would force over 50% of webservers to change their operating systems, 99.8% of super computers to do the same, 90% of embedded devices (due to the linux kernel running on it) and so on...

It would mean as a sysadmin it would require a complete restructuring of our business if the same legislation was enforced in the UK as many laws trickle down to us in one form or another eventually. It could literally put us out of business by forcing us to pay hundreds of thousands of pounds on software licenses which we have would have no idea if they are secure or not. The impact this would have is enormous. This is the first time I have ever commented to the FCC and I do not live in the US.

I implore you as a professional in the IT industry to reconsider this.

This legislation poses a huge and substantial threat to the open source world. If it were to become illegal to put open source software on devices with a wifi antenna it would force over 50% of webservers to change their operating systems, 99.8% of super computers to do the same, 90% of embedded devices (due to the linux kernel running on it) and so on...

It would mean as a sysadmin it would require a complete restructuring of our business if the same legislation was enforced in the UK as many laws trickle down to us in one form or another eventually. It could literally put us out of business by forcing us to pay hundreds of thousands of pounds on software licenses which we have would have no idea if they are secure or not. The impact this would have is enormous. This is the first time I have ever commented to the FCC and I do not live in the US.

I implore you as a professional in the IT industry to reconsider this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Doe

Mailing Address: 1 West Lakeshore Drive

City: Birmingham

Country: United States

State or Province: AL

ZIP/Postal Code: 35242

Email Address: sniper@mailinator.com

Organization Name: n/a

Comment: Don't do this

Don't do this

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Edward

Last Name: Keating

Mailing Address: 140 Deer Valley Dr.

City: Deer Park

Country: United States

State or Province: IL

ZIP/Postal Code: 60010

Email Address: Edward.Keating@outlook.com

Organization Name: Motorola Solutions Inc/ Zebra Technologies, Teksystems.

Comment: The proposed rules would seem to inhibit manufacturers from creating a generic platform which can be configure by the end user for operation within his country. Different standards exist for operation on 2.4Ghz and 5Ghz throughout the world. This proposed rule would force the manufacturer to only deliver wireless devices that conform to that country's current restrictions. Changes to the Country's allowed frequencies would require sending the equipment back to the manufacturer. A device that could have been designed for use in EU, USA, Canada would no longer exist, you would need to create special versions (and likely software for each) which would impact manufacturers. You probably didn't consider this before drafting this rule.

I work with and have worked for a wireless equipment manufacturer and as a System Test Engineer, have to verify operation of equipment in various configurations. Now as a contractor (after being an employee for 35 years), this legislation would impact me directly and block my abilities to work as a contractor. (Since I'm not a manufacturer, the interpretation of whom can perform changes to the equipment will likely be locked down by this rule and I would be unable to change defaults set into the equipment.)

I think the rule is ill conceived and should not be approved. Your rule will only apply to engineers working in the US and would not apply to the rest of the world, so why are you blocking our ability to compete in the world market?

The proposed rules would seem to inhibit manufacturers from creating a generic platform which can be configure by the end user for operation within his country. Different standards exist for operation on 2.4Ghz and 5Ghz throughout the world. This proposed rule would force the manufacturer to only deliver wireless devices that conform to that country's current restrictions. Changes to the Country's allowed frequencies would require sending the equipment back to the manufacturer. A device that could have been designed for use in EU, USA, Canada would no longer exist, you would need to create special versions (and likely software for each) which would impact manufacturers. You probably didn't consider this before drafting this rule.

I work with and have worked for a wireless equipment manufacturer and as a System Test Engineer, have to verify operation of equipment in various configurations. Now as a contractor (after being an employee for 35 years), this legislation would impact me directly and block my abilities to work as a contractor. (Since I'm not a manufacturer, the interpretation of whom can perform changes to the equipment will likely be locked down by this rule and I would be unable to change defaults set into the equipment.)

I think the rule is ill conceived and should not be approved. Your rule will only apply to engineers working in the US and would not apply to the rest of the world, so why are you blocking our ability to compete in the world market?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Timothy

Last Name: Esau

Mailing Address: P.O. Box 230695

City: Tigard

Country: United States Minor Outlying Islands

State or Province: Oregon

ZIP/Postal Code: 97281

Email Address: timesau+fcc@gmail.com

Organization Name:

Comment: Dear FCC Commissioners & Committee members,

I respectfully request you do not implement rules that take away the ability of users to install the software of their choosing on their computing devices, and specifically, I ask your reject rule "Equipment Authorization and Electronic Labeling for Wireless Devices" (ET Docket No. 15-170; RM-11673).

Often research begins with off-the-shelf equipment because it is affordable and easily available. Imposing further regulation on our personal devices will unnecessarily hamper wireless networking research that depends on the ability of researchers to investigate and modify such devices. Either reject this rule, or modify the rule to exclude computer networking devices and wifi networking communications equipment.

We as citizens need the opportunity to fix security holes and flaws in our equipment when the manufacturer fails to do so. Granted, not all have the ability, but for those who do it is essential. Historically, users have fixed serious bugs in their wifi drivers, this would be banned under the ET Docket No. 15-170; RM-11673.

Additionally, Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, and others in the IT service industry depend on the ability of individual users and companies to customize or further secure commercial products by installing software of their choosing.

Thank you for taking a stand for individual rights and protecting our liberty by voting against ET Docket No. 15-170; RM-11673!

Respectfully,

Tim Esau

Private citizen

Dear FCC Commissioners & Committee members,

I respectfully request you do not implement rules that take away the ability of users to install the software of their choosing on their computing devices, and specifically, I ask your reject rule "Equipment Authorization and Electronic Labeling for Wireless Devices" (ET Docket No. 15-170; RM-11673).

Often research begins with off-the-shelf equipment because it is affordable and easily available. Imposing further regulation on our personal devices will unnecessarily hamper wireless networking research that depends on the ability of researchers to investigate and modify such devices. Either reject this rule, or modify the rule to exclude computer networking devices and wifi networking communications equipment.

We as citizens need the opportunity to fix security holes and flaws in our equipment when the manufacturer fails to do so. Granted, not all have the ability, but for those who do it is essential. Historically, users have fixed serious bugs in their wifi drivers, this would be banned under the ET Docket No. 15-170; RM-11673.

Additionally, Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, and others in the IT service industry depend on the ability of individual users and companies to customize or further secure commercial products by installing software of their choosing.

Thank you for taking a stand for individual rights and protecting our liberty by voting against ET Docket No. 15-170; RM-11673!

Respectfully,
Tim Esau
Private citizen

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jerry

Last Name: McGuire

Mailing Address: 2029 Atlantic Ave

City: Kingman

Country: United States

State or Province: AZ

ZIP/Postal Code: 86401

Email Address: mcguirejl@gmail.com

Organization Name:

Comment: Please withdraw this proposed rule. Innovation is difficult enough in the US. While sounding like a common sense approach to a problem that doesn't exist, this proposed rule, if approved and enacted, will foreclose thousands of innovations under development. These innovations will have profound effects on human health treatment, climate mapping and monitoring, and food production / distribution. Please withdraw this proposed rule.

Please withdraw this proposed rule. Innovation is difficult enough in the US. While sounding like a common sense approach to a problem that doesn't exist, this proposed rule, if approved and enacted, will foreclose thousands of innovations under development. These innovations will have profound effects on human health treatment, climate mapping and monitoring, and food production / distribution. Please withdraw this proposed rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Budarz

Mailing Address: 62 E. Transit St., Fl. 2

City: Providence

Country: United States

State or Province: RI

ZIP/Postal Code: 02906

Email Address: james_budarz@brown.edu

Organization Name: Brown University

Comment: I believe that it is every American's right to write and operate Open and Free software if they have the ability and reason to do so. Limiting the types of software that can be implemented means handing over unprecedented power to telecommunications companies yet again, and that is an act I cannot support from this administration. The dangers presented by such an act outweigh their benefits, and I put my support behind those who would craft and implement improved software free of the bugs, feature locks, and security holes found constantly in WiFi router firmware.

I believe that it is every American's right to write and operate Open and Free software if they have the ability and reason to do so. Limiting the types of software that can be implemented means handing over unprecedented power to telecommunications companies yet again, and that is an act I cannot support from this administration. The dangers presented by such an act outweigh their benefits, and I put my support behind those who would craft and implement improved software free of the bugs, feature locks, and security holes found constantly in WiFi router 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: Patrick

Last Name: Wolfe

Mailing Address: 1309 Dalesford Dr

City: Alpharetta

Country: United States

State or Province: GA

ZIP/Postal Code: 30004-7828

Email Address: pjw@whistl.com

Organization Name:

Comment: I know of no good reason to restrict operating system software on any computing hardware I purchase, as I see fit. There is no security risk, in fact, there is LESS security risk, in INCREASED diversity of operating systems. Hackers mostly target Windows because most people use it. Forcing people to use the buggiest OS on their hardware is not improving security.

Locking down wifi routers is plain stupid. Most good network engineers install the open source software, because: a) it works better and more consistently with other manufacturers equipment, and b) because bug fixes are quickly distributed and upgraded. Locking down wifi routers so computer literate engineers cannot secure their own network, without worrying about unintentional, or even by design, backdoors that are discovered every year.

I know of no good reason to restrict operating system software on any computing hardware I purchase, as I see fit. There is no security risk, in fact, there is LESS security risk, in INCREASED diversity of operating systems. Hackers mostly target Windows because most people use it. Forcing people to use the buggiest OS on their hardware is not improving security.

Locking down wifi routers is plain stupid. Most good network engineers install the open source software, because: a) it works better and more consistently with other manufacturers equipment, and b) because bug fixes are quickly distributed and upgraded. Locking down wifi routers so computer literate engineers cannot secure their own network, without worrying about unintentional, or even by design, backdoors that are discovered every year.

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: Owen

Last Name: Parsons

Mailing Address: 101 Mount Vernon Cir

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30338

Email Address: owen.parsons@gmail.com

Organization Name:

Comment: This would only stifle innovation. Many of the most useful features being incorporated into consumer level wireless routers were created first in open source. The safety you seek by closing this option is left wide open on non wifi related devices.

this effort seem like a close minded attempted to help the industry, written by someone with a limited understanding of the technology.

This would only stifle innovation. Many of the most useful features being incorporated into consumer level wireless routers were created first in open source. The safety you seek by closing this option is left wide open on non wifi related devices.

this effort seem like a close minded attempted to help the industry, written by someone with a limited understanding of the technology.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anonymous

Last Name: Anonymous

Mailing Address: Anonymous

City: CHICAGO

Country: United States

State or Province: IL

ZIP/Postal Code: 60608

Email Address: null

Organization Name: null

Comment: This is a terrible idea. You reducing the citizen's ability to actively participate and modify the technology they by all rights should own. By doing this, you are also restricting the people's ability to create and modify their own technology without being a part of a major corporation.

This is a terrible idea. You reducing the citizen's ability to actively participate and modify the technology they by all rights should own. By doing this, you are also restricting the people's ability to create and modify their own technology without being a part of a major corporation.

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: Lesbirel

Mailing Address: 4801 SW 1st Ave

City: Ocala

Country: United States

State or Province: FL

ZIP/Postal Code: 34471

Email Address: nlesbirel@gmail.com

Organization Name:

Comment: This proposed rule is a miserable idea, comparable to a WiFi version of SOPA/PIPA. Not only would it completely prevent individual wireless research (open source projects have been leading the way in advancement and standards for some time now), but also unfairly target any organizations not large enough to officially create their own devices to put their own firmware on. Thousands of local and high school electronics clubs across the country would be severely limited, and networking education would be much more difficult to happen legally. This completely goes against any ownership of any products, and is an incredibly broad rule. User created firmware for wireless devices is already very widespread, this rule would make millions of Americans (And thousands of businesses) criminals, and many without any knowledge of that. Not to mention, there is simply no advantage of this rule other than to provide more power to companies who won't necessarily be acting in the best interests of consumers. Custom firmware is done by teams with an actual devotion to what they do, and is shown to be more secure than the preinstalled firmware many companies leave on their devices, without updates or support, and open to vulnerabilities that may never get fixed.

This proposed rule is a miserable idea, comparable to a WiFi version of SOPA/PIPA. Not only would it completely prevent individual wireless research (open source projects have been leading the way in advancement and standards for some time now), but also unfairly target any organizations not large enough to officially create their own devices to put their own firmware on. Thousands of local and high school electronics clubs across the country would be severely limited, and networking education would be much more difficult to happen legally. This completely goes against any ownership of any products, and is an incredibly broad rule. User created firmware for wireless devices is already very widespread, this rule would make millions of Americans (And thousands of businesses) criminals, and many without any knowledge of that. Not to mention, there is simply no advantage of this rule other than to provide more power to companies who won't necessarily be acting in the best interests of consumers. Custom firmware is done by teams with an actual devotion to what they do, and is shown to be more secure than the preinstalled firmware many companies leave on their devices, without updates or support, and open to vulnerabilities that may never get fixed.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Richard

Last Name: Colson

Mailing Address: Derryrush

City: Rosmuc

Country: Ireland

State or Province: Galway

ZIP/Postal Code: 0001

Email Address: richardcolson@eircom.net

Organization Name:

Comment: I totally disagree with this proposal.

If this proposal becomes law it will seriously impinge on civil liberties and individual freedom and will detract from the advancement of private research. Furthermore it will concentrate future developments in a few corporate hands.

I totally disagree with this proposal.

If this proposal becomes law it will seriously impinge on civil liberties and individual freedom and will detract from the advancement of private research. Furthermore it will concentrate future developments in a few corporate hands.

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: Garcia

Mailing Address: 1552 Millington Dr.

City: Virginia Beach

Country: United States

State or Province: VA

ZIP/Postal Code: 23464

Email Address: mdotgarcia@live.com

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points:

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

Thank you.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points:

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

Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Gabe

Last Name: Grimes

Mailing Address: 1200 E Byers Ave

City: Owensboro

Country: United States

State or Province: KY

ZIP/Postal Code: 42303

Email Address: jee.grimes+fcc@gmail.com

Organization Name:

Comment: I respectfully ask that you not remove users' ability to install software of their choosing on electronic devices they have purchased. Allowing users to install security patches to their devices, as well as improve upon the security of their devices by creating their own software, is something that the FCC shouldn't actively try to hinder.

Please reconsider.

I respectfully ask that you not remove users' ability to install software of their choosing on electronic devices they have purchased. Allowing users to install security patches to their devices, as well as improve upon the security of their devices by creating their own software, is something that the FCC shouldn't actively try to hinder.

Please reconsider.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Dave

Last Name: Symons

Mailing Address: 989 112th AVE NE #802

City: Bellevue

Country: United States

State or Province: WA

ZIP/Postal Code: 98004

Email Address:

Organization Name:

Comment: I respectfully ask the FCC not to implement rules that take away the ability of 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. Additionally Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

I respectfully ask the FCC not to implement rules that take away the ability of 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. Additionally Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Public

Last Name: Info

Mailing Address: 10 Downing Street

City: London

Country: United Kingdom

State or Province: I live in the UK

ZIP/Postal Code: SW1A 2AA

Email Address:

Organization Name:

Comment: I must strongly disagree with this. Not only is giving people access to their own modifications not hurting anybody, but many of the largest infrastructures in the world actually USE Linux to operate. I do not believe stopping people modifying will accomplish anything, and as such, no point enforcing it.
Literally the stupidest thing I've seen all year.

I must strongly disagree with this. Not only is giving people access to their own modifications not hurting anybody, but many of the largest infrastructures in the world actually USE Linux to operate. I do not believe stopping people modifying will accomplish anything, and as such, no point enforcing it.
Literally the stupidest thing I've seen all year.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Kluver Jr.

Mailing Address: 724 cottonwood drive

City: Allen

Country: United States

State or Province: TX

ZIP/Postal Code: 75002

Email Address: vanaric@gmail.com

Organization Name: null

Comment: As long as they are not breaking any laws, users should be able to modify the firmware of their router, or indeed any device that they own, if they decide to. Please stop taking away rights from citizens and giving them to corporations.

As long as they are not breaking any laws, users should be able to modify the firmware of their router, or indeed any device that they own, if they decide to. Please stop taking away rights from citizens and giving them to corporations.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Richard

Last Name: Torpey

Mailing Address: 117 Junard Dr

City: Bay Shore

Country: United States

State or Province: NY

ZIP/Postal Code: 11706

Email Address: rich@torpey.com

Organization Name:

Comment: This document needs a clear exemption for hobbyists and individuals who may chose to modify commercial equipment. There should be a clear statement that there is no requirement for such an individual to need a new FCC ID and they shall be held harmless as long as the modified device does not cause any interference.

This document needs a clear exemption for hobbyists and individuals who may chose to modify commercial equipment. There should be a clear statement that there is no requirement for such an individual to need a new FCC ID and they shall be held harmless as long as the modified device does not cause any interference.

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: Ray

Last Name: Marshall

Mailing Address: 706 Norman St

City: Anchorage

Country: United States

State or Province: AK

ZIP/Postal Code: 99504

Email Address:

Organization Name:

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

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing 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: Fred

Last Name: Gardner

Mailing Address: 2419 Olive Street

City: Philadelphia

Country: United States

State or Province: PA

ZIP/Postal Code: 19130

Email Address:

Organization Name:

Comment: This is a terrible idea. As a consumer, I should have the right to hack, flash, or otherwise modify any device I OWN in any way I choose. This is yet another attempt to stifle innovation and turn physical devices into subscription services for their manufacturers. Please focus on the rights of the consumer rather than the profit making desires of corporations.

This is a terrible idea. As a consumer, I should have the right to hack, flash, or otherwise modify any device I OWN in any way I choose. This is yet another attempt to stifle innovation and turn physical devices into subscription services for their manufacturers. Please focus on the rights of the consumer rather than the profit making desires of corporations.

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: Don

Last Name: Smith

Mailing Address: 1609 Mendota St.

City: Madison

Country: United States

State or Province: WI

ZIP/Postal Code: 53704

Email Address:

Organization Name:

Comment: Don't stifle innovation !!!

Don't stifle innovation !!!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jameal

Last Name: Jordon

Mailing Address: 1440-201 Nine Iron Way

City: Raleigh

Country: United States

State or Province: NC

ZIP/Postal Code: 27603

Email Address: jameal.jordon@yahoo.com

Organization Name:

Comment: The United States of America is supposed to be a beacon for freedom and innovation, since the inception of its government. Government and its agencies and bureaucracies are not supposed to stand in the way of freedom, innovation, and new possibilities with rules, ordinances, laws, legislation, and regulations.

Imposing more rules and banning innovation, custom firmware, software, and even hardware modifications will further stifle this great republic. Tying the hands of the best and brightest, those willing to explore new avenues of this technology.

Do not stand in the way of progress. Someone else, in some other country, in some other place will benefit and the USA will lose in the long run.

Also, will this ban, ever affect governmental agencies and bureaucracies? If the FCC is willing to use its 'banhammer' then it should apply across the ENTIRE spectrum of the US (from the CIA, NSA, to the military, then lastly to its citizens). If not, then what is the purpose making this modification illegal?

The United States of America is supposed to be a beacon for freedom and innovation, since the inception of its government. Government and its agencies and bureaucracies are not supposed to stand in the way of freedom, innovation, and new possibilities with rules, ordinances, laws, legislation, and regulations.

Imposing more rules and banning innovation, custom firmware, software, and even hardware modifications will further stifle this great republic. Tying the hands of the best and brightest, those willing to explore new avenues of this technology.

Do not stand in the way of progress. Someone else, in some other country, in some other place will benefit and the USA will lose in the long run.

Also, will this ban, ever affect governmental agencies and bureaucracies? If the FCC is willing to use its 'banhammer' then it should apply across the ENTIRE spectrum of the US (from the CIA, NSA, to the military, then lastly to its citizens). If not, then what is the purpose making this modification illegal?

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: Ronan

Last Name: McAllister

Mailing Address: POB 1535

City: Meadow Vista

Country: United States

State or Province: CA

ZIP/Postal Code: 95722

Email Address:

Organization Name:

Comment: FCC,

I am a licensed radio amateur in the US ; I am asking the FCC to not implement rules that take away the ability of users to install the open-source firmware/software of their choosing on their wireless routers.

If the FCC implement such a rule, this will not only interfere with HAM radio operators who need the open platform of wireless routers/gateways to enable future technology, but please also consider the following:

- * 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.
- * There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

If anyone should know the benefits gained by HAM radio operators having full and complete access to the firmware in the WiFi routers they purchase for emergency communications, it should be the FCC!

Thank you

Ronan McAllister

FCC,

I am a licensed radio amateur in the US ; I am asking the FCC to not implement rules that take away the ability of users to install the open-source firmware/software of their choosing on their wireless routers.

If the FCC implement such a rule, this will not only interfere with HAM radio operators who need the open platform of wireless routers/gateways to enable future technology, but please also consider the following:

- * 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.
- * There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

If anyone should know the benefits gained by HAM radio operators having full and complete access to the firmware in the WiFi routers they purchase for emergency communications, it should be the FCC!

Thank you
Ronan McAllister

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: William

Last Name: Washburn

Mailing Address: 1651 Camelot Circle

City: Tucker

Country: United States

State or Province: GA

ZIP/Postal Code: 30084-7706

Email Address: dygituljunky@gmail.com

Organization Name:

Comment: I object to any section which would prevent me from installing aftermarket firmware on my phone(s) or router(s). Firmware from third parties, especially the open source varieties, often provide better features and bug fixes than the original firmware or manufacturer provide and on a better timeline.

By locking out aftermarket firmware packages, this regulation would essentially lock OWNERS of hardware into buggy original firmware with no way of providing their own remedy for firmware that includes hackable bugs or intentional privacy breaches. This is especially concerning with regard to operators of hardware who must comply with HIPAA and other privacy-enforcing regulations.

I object to any section which would prevent me from installing aftermarket firmware on my phone(s) or router(s). Firmware from third parties, especially the open source varieties, often provide better features and bug fixes than the original firmware or manufacturer provide and on a better timeline.

By locking out aftermarket firmware packages, this regulation would essentially lock OWNERS of hardware into buggy original firmware with no way of providing their own remedy for firmware that includes hackable bugs or intentional privacy breaches. This is especially concerning with regard to operators of hardware who must comply with HIPAA and other privacy-enforcing regulations.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Isaiah

Last Name: Berson

Mailing Address: 22 Terrace Ave

City: Newton

Country: United States

State or Province: MA

ZIP/Postal Code: 02461

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joel

Last Name: Fuster

Mailing Address: 745 Arbor Ct

City: Warrenton

Country: United States

State or Province: VA

ZIP/Postal Code: 20186

Email Address: s2@fuster.org

Organization Name:

Comment: Dear Commission:

I am writing this comment to ask you to please think more carefully about this proposed rule. While there are always bad actors, the benefits of allowing consumers to load new software onto their devices far outweigh the occasional enforcement issue.

- 1) Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- 2) Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Manufacturers are notorious for abandoning these low-margin products, preferring to spend their resources on new products instead.
- 3) Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- 4) Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

If these new rules are not carefully limited in scope and their implications thought through, it will be very tempting for manufacturers simply to lock down their WiFi devices entirely and prevent any third-party firmware installation rather than merely restricting the truly problematic functions.

Thank you for your time.

Dear Commission:

I am writing this comment to ask you to please think more carefully about this proposed rule. While there are always bad actors, the benefits of allowing consumers to load new software onto their devices far outweigh the occasional enforcement issue.

- 1) Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- 2) Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Manufacturers are notorious for abandoning these low-margin products, preferring to spend their resources on new products instead.
- 3) Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- 4) Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

If these new rules are not carefully limited in scope and their implications thought through, it will be very tempting for manufacturers simply to lock down their WiFi devices entirely and prevent any third-party firmware installation rather than merely restricting the truly problematic functions.

Thank you for your time.

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: Higgins

Mailing Address: 855 Patterson Ave

City: New York

Country: United States

State or Province: NY

ZIP/Postal Code: 10306

Email Address:

Organization Name:

Comment: Please do not.

Please do not.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Hurst

Mailing Address: 3856 S 2700 E

City: Salt Lake City

Country: United States

State or Province: UT

ZIP/Postal Code: 84109-3560

Email Address: jhurst@xmission.com

Organization Name:

Comment: To whom it may concern:

I am respectfully asking the FCC to not implement the proposed rules that will take away the ability of users to install the software/firmware of my choosing on my privately owned computer devices.

Please consider that wireless networking research depends on researchers to investigate and modify such devices. We also need the ability to fix security holes when the manufacturer will not. Along this line, users have also found and fixed serious bugs in the operating system of the unit. All of these would be banned under the NPRM.

By not fixing these security holes, it allows for the increase of cyberthreats and can actually lead to identity theft and fraud. Billions of dollars in commerce "pass through" these access points and retailers depend on their customers to use secure access points.

There is also no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. Also, the amateur radio community had made great strides in functionality with the open-source firmware.

To reiterate: Please do not implement the rules being proposed as mentioned above.

Sincerely,

John J Hurst

KF7NQQ

To whom it may concern:

I am respectfully asking the FCC to not implement the proposed rules that will take away the ability of users to install the software/firmware of my choosing on my privately owned computer devices.

Please consider that wireless networking research depends on researchers to investigate and modify such devices. We also need the ability to fix security holes when the manufacturer will not. Along this line, users have also found and fixed serious bugs in the operating system of the unit. All of these would be banned under the NPRM.

By not fixing these security holes, it allows for the increase of cyberthreats and can actually lead to identity theft and

fraud. Billions of dollars in commerce "pass through" these access points and retailers depend on their customers to use secure access points.

There is also no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. Also, the amateur radio community had made great strides in functionality with the open-source firmware.

To reiterate: Please do not implement the rules being proposed as mentioned above.

Sincerely,

John J Hurst
KF7NQW

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: Valerie

Last Name: Kramer

Mailing Address: P.O. Box 49

City: Port Orford

Country: United States

State or Province: OR

ZIP/Postal Code: 97465

Email Address: valerie@mydfz.com

Organization Name:

Comment: Dear Sirs,

I understand that there are some concerns with users modifying software or hardware but I believe that banning such practices is not the right answer. It will stifle creativity and technical innovation, limit the usefulness of products, and most likely create a number of criminals as some people will no doubt proceed with such activities anyway.

I believe a more reasonable approach would be to specify, as you already do, the technical details of the various classes of transmitters and to make illegal any which overstep their limits. That should be ample protection for the public and it should be easier to detect malfunctioning equipment and to prove such charges in court.

I believe this proposed legislation is driven more by corporate greed than by any serious need and should not be put into law.

Thank you.

Dear Sirs,

I understand that there are some concerns with users modifying software or hardware but I believe that banning such practices is not the right answer. It will stifle creativity and technical innovation, limit the usefulness of products, and most likely create a number of criminals as some people will no doubt proceed with such activities anyway.

I believe a more reasonable approach would be to specify, as you already do, the technical details of the various classes of transmitters and to make illegal any which overstep their limits. That should be ample protection for the public and it should be easier to detect malfunctioning equipment and to prove such charges in court.

I believe this proposed legislation is driven more by corporate greed than by any serious need and should not be put into law.

Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ryan

Last Name: Cragun

Mailing Address: 1738 W Ferris Ave.

City: Tampa

Country: United States

State or Province: FL

ZIP/Postal Code: 33603

Email Address: ryantcragun@gmail.com

Organization Name:

Comment: Please continue to allow people to modify the firmware on their routers. Some of us like to "hack" our routers with improved firmware to improve their efficiency and increase their functionality. Why would you reduce our ability to do this? That makes no sense.

Please continue to allow people to modify the firmware on their routers. Some of us like to "hack" our routers with improved firmware to improve their efficiency and increase their functionality. Why would you reduce our ability to do this? That makes no sense.

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: Paul

Last Name: Clifton

Mailing Address: 800 Peachtree St. # 8506

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30308

Email Address: paulgclifton@gmail.com

Organization Name:

Comment: Please do not implement rules that take away an owners ability to install software of their choosing on computing devices, in this case, routers. The rules that you are considering will ultimately make that impossible and will potentially cause more harm than good to the development and use of router technology and stifle the development of computing technology.

It is worth emphasizing the following points:

- * Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- * Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- * Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- * Not fixing security holes either feeds cyberthreats or increases electronic waste.
- * Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
- * There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Thank you for your consideration and for not implementing the proposed rules.

Please do not implement rules that take away an owners ability to install software of their choosing on computing devices, in this case, routers. The rules that you are considering will ultimately make that impossible and will potentially cause more harm than good to the development and use of router technology and stifle the development of computing technology.

It is worth emphasizing the following points:

- * Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- * Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- * Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- * Not fixing security holes either feeds cyberthreats or increases electronic waste.
- * Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
- * There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Thank you for your consideration and for not implementing the proposed 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: George

Last Name: Driver

Mailing Address: 8785 Kuhn Road

City: Greencastle

Country: United States

State or Province: PA

ZIP/Postal Code: 17225

Email Address: george.driver@gmail.com

Organization Name:

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

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing 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: Valerij

Last Name: Shilay

Mailing Address: Igumensky tract, h.18 apt.53

City: Minsk

Country: Belarus

State or Province: Minsk

ZIP/Postal Code: 220112

Email Address: shiller777@gmail.com

Organization Name:

Comment: This law project will disable creating alternative operating systems and will bring harm to IT innovations sphere

This law project will disable creating alternative operating systems and will bring harm to IT innovations sphere

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Timothy

Last Name: Pearson

Mailing Address: 2556 Anderson Dr.

City: Belvidere

Country: United States

State or Province: IL

ZIP/Postal Code: 61008

Email Address: tpearson@raptorengineeringinc.com

Organization Name: Raptor Engineering

Comment: This is a horrible idea on so many levels. While, as an electrical engineer, I fully support limits being placed on consumer devices, said limits should be built into the hardware itself instead of restricting consumer choice, damaging the open source movement, and inevitably reducing security of all wireless and wireless connected devices.

If open source software cannot be used within wireless devices, under the device owner's direct control, said wireless devices cannot be used within a secured environment, with no exceptions. This ruling will have the effect of sending many corporations within the United States back to the technological dark ages, as they will not be able to safely and securely use wireless technology as they have up until this poing.

I strongly oppose this new ruling. Additionally, the engineering business I work at will not be using any wireless technology in the future as a sole and direct result of this ruling, and I will encourage the various IT professionals I have contact with to do the same.

This is a horrible idea on so many levels. While, as an electrical engineer, I fully support limits being placed on consumer devices, said limits should be built into the hardware itself instead of restricting consumer choice, damaging the open source movement, and inevitably reducing security of all wireless and wireless connected devices.

If open source software cannot be used within wireless devices, under the device owner's direct control, said wireless devices cannot be used within a secured environment, with no exceptions. This ruling will have the effect of sending many corporations within the United States back to the technological dark ages, as they will not be able to safely and securely use wireless technology as they have up until this poing.

I strongly oppose this new ruling. Additionally, the engineering business I work at will not be using any wireless technology in the future as a sole and direct result of this ruling, and I will encourage the various IT professionals I have contact with to do the same.

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: Martin

Last Name: Campbell

Mailing Address: 701 E Pennengton Apt 147

City: West Burlington

Country: United States

State or Province: IA

ZIP/Postal Code: 52655

Email Address: null

Organization Name: null

Comment: I feel that this proposed rule is neither necessary, nor desirable. Nothing should eliminate or limit the purchaser of any device from modifying the software or hardware of that device, provided that said changes do not violate current laws or FCC rules, either by causing interference or by causing unauthorized transmissions. I feel that the ability of the purchaser to modify their devices (while maintaining the above conditions) is necessary for innovation to occur, as well as to improve the functionality and security of said devices. Any rule or law that hinders the purchaser's rights and abilities in this area is must not be approved, and any current rules or laws that hinder the purchasers rights and ability in this area must be repealed/struck down.

I feel that this proposed rule is neither necessary, nor desirable. Nothing should eliminate or limit the purchaser of any device from modifying the software or hardware of that device, provided that said changes do not violate current laws or FCC rules, either by causing interference or by causing unauthorized transmissions. I feel that the ability of the purchaser to modify their devices (while maintaining the above conditions) is necessary for innovation to occur, as well as to improve the functionality and security of said devices. Any rule or law that hinders the purchaser's rights and abilities in this area is must not be approved, and any current rules or laws that hinder the purchasers rights and ability in this area must be repealed/struck down.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joseph

Last Name: Rimmer

Mailing Address: 430 Spall Rd S

City: Remsen

Country: United States

State or Province: NY

ZIP/Postal Code: 13438

Email Address: josephrimmeriii@gmail.com

Organization Name:

Comment: As someone in the IT field, I must request that this does not get passed. This would not only limit some freedoms of owning a computer, it would largely reduce what we are capable of using to increase security and perform penetration testing and research. By adding restrictions like this, technological advancements would be slower, and some research even considered illegal (along with changes to personally owned device). This would only decrease the protection against possible exploits and/or malicious code, while increasing the lifetime of the exploits and/or malicious code.

As someone in the IT field, I must request that this does not get passed. This would not only limit some freedoms of owning a computer, it would largely reduce what we are capable of using to increase security and perform penetration testing and research. By adding restrictions like this, technological advancements would be slower, and some research even considered illegal (along with changes to personally owned device). This would only decrease the protection against possible exploits and/or malicious code, while increasing the lifetime of the exploits and/or malicious code.

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: Mayeaux

Mailing Address: 217 Suzanne Dr

City: Shreveport

Country: United States

State or Province: LA

ZIP/Postal Code: 71115

Email Address:

Organization Name:

Comment: Please do not implement any rule that would remove Americans' ability to modify their own firmware. This would inevitably disastrous for digital security on every level, from personal to corporate to national.

Please do not implement any rule that would remove Americans' ability to modify their own firmware. This would inevitably disastrous for digital security on every level, from personal to corporate to national.

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: Gladen

Mailing Address: PO BOX 87

City: Goshen

Country: United States

State or Province: CA

ZIP/Postal Code: 93227-0087

Email Address: jason_gladen@yahoo.com

Organization Name:

Comment: This action will have several knock-on effects. one of which is the closing of the source code for every WIFI device. This sounds to me like a way to hurt public security and give undue power to hidden stake holders. An open-source well maintained firmware is often better then a old busted closed source one. The proposed action will make it HARDER to maintain new systems. The new systems will be more fragile. They will be more likely to be in error and produce a break downs communication. This goes against the public trust.

Instead of more regulation, use the existing ones and promote the development of tools to locate and identify misbehaving systems. Even with the proposed action there are and will be system that violate the rules. The proposed action does nothing to resolve that and seem counter-productive. I think the "trust but verify" is a much better approach. Instead of spending billions in retooling and closing systems, lets spend less than 1% on prizes and bounties for finding bad systems and fixing them.

This action will have several knock-on effects. one of which is the closing of the source code for every WIFI device. This sounds to me like a way to hurt public security and give undue power to hidden stake holders. An open-source well maintained firmware is often better then a old busted closed source one. The proposed action will make it HARDER to maintain new systems. The new systems will be more fragile. They will be more likely to be in error and produce a break downs communication. This goes against the public trust.

Instead of more regulation, use the existing ones and promote the development of tools to locate and identify misbehaving systems. Even with the proposed action there are and will be system that violate the rules. The proposed action does nothing to resolve that and seem counter-productive. I think the "trust but verify" is a much better approach. Instead of spending billions in retooling and closing systems, lets spend less than 1% on prizes and bounties for finding bad systems and fixing them.

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: Matthias

Last Name: Alphart

Mailing Address: Wiener Strae 46

City: Traiskirchen

Country: Austria

State or Province: Niedersterreich

ZIP/Postal Code: 2514

Email Address: spam1@alphart.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.

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.

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: Toby

Last Name: Horton

Mailing Address: 11960 SW Faircrest St

City: Portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97225

Email Address: toby.horton@unoc.me

Organization Name:

Comment: As a career Information Technology professional, I believe that access to the core firmware of your home computing devices is an essential need in ensuring and maintaining proper security, privacy, and control over personal data.

Taking this ability out of the hands of consumers seriously threatens personal privacy, data security, and stifles creativity in the technology community. A community that uses customization as a means to exploring new methods and approaches to solving problems, which drives improvements to security for all devices and protects the technology community from exploitation and surveillance, keeping technology stable, free, and healthy.

Thank you.

As a career Information Technology professional, I believe that access to the core firmware of your home computing devices is an essential need in ensuring and maintaining proper security, privacy, and control over personal data.

Taking this ability out of the hands of consumers seriously threatens personal privacy, data security, and stifles creativity in the technology community. A community that uses customization as a means to exploring new methods and approaches to solving problems, which drives improvements to security for all devices and protects the technology community from exploitation and surveillance, keeping technology stable, free, and healthy.

Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mahmud

Last Name: ullah

Mailing Address: mahmudullahs97@gmail.com

City: Dhaka

Country: Bangladesh

State or Province: Bangladesh

ZIP/Postal Code: 3161

Email Address: mahmudullahs97@gmail.com

Organization Name: none

Comment: I want to be free to use my device operating system, apps, by my choice

What you are going to do is very very unauthentic to my country..

finally "I object this because security and privacy is *important* to me.

I want to be free to use my device operating system, apps, by my choice

What you are going to do is very very unauthentic to my country..

finally "I object this because security and privacy is *important* to me.

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: Max

Last Name: Chan

Mailing Address: Room 1404, 200 Jianhe Rd

City: Shanghai

Country: China

State or Province: Municipality of Shanghai

ZIP/Postal Code: 200335

Email Address: max@maxchan.info

Organization Name:

Comment: This proposal, while simplifying the procedure of approval, carry the tendency of causing the manufacturers to lock down the device from installation of third party operating systems that can be code reviewed.

This may not seem significant, however it is long proven that a locked down firmware can and will end up carrying malicious software. This will encourage both cybercrime and mass surveillance which both affects the rights of the user of such equipments negatively.

I would suggest while preventing the unauthorized spectrum from being occupied, measure must be taken to prevent the devices from being locked down.

This proposal, while simplifying the procedure of approval, carry the tendency of causing the manufacturers to lock down the device from installation of third party operating systems that can be code reviewed.

This may not seem significant, however it is long proven that a locked down firmware can and will end up carrying malicious software. This will encourage both cybercrime and mass surveillance which both affects the rights of the user of such equipments negatively.

I would suggest while preventing the unauthorized spectrum from being occupied, measure must be taken to prevent the devices from being locked down.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mark

Last Name: Smith

Mailing Address: 56 Woolford Ave

City: Franklinville

Country: United States

State or Province: NJ

ZIP/Postal Code: 08322

Email Address: zebiddy8@gmail.com

Organization Name:

Comment: As both a computer user and amateur radio operator I would prefer that the FCC reconsider implementation of this unnecessary rule prohibiting the flashing of devices by the end user. As it stands now, the vast majority of electronic devices remain in the original manufacturers "as delivered" state, so this rule would certainly represent an unnecessary burden on equipment manufacturers to address the minuscule amount of their products that might be modified. In addition, the inability to add innovation and features to existing devices tends to retard the growth and creativity of gifted individuals in their pursuit of learning about hardware and software, more of which can only be beneficial to society.

As both a computer user and amateur radio operator I would prefer that the FCC reconsider implementation of this unnecessary rule prohibiting the flashing of devices by the end user. As it stands now, the vast majority of electronic devices remain in the original manufacturers "as delivered" state, so this rule would certainly represent an unnecessary burden on equipment manufacturers to address the minuscule amount of their products that might be modified. In addition, the inability to add innovation and features to existing devices tends to retard the growth and creativity of gifted individuals in their pursuit of learning about hardware and software, more of which can only be beneficial to society.

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: Jonathan

Last Name: Windham

Mailing Address: 1000 Smith Level Road

City: Carrboro

Country: United States

State or Province: NC

ZIP/Postal Code: 27510

Email Address: jon2kx@gmail.com

Organization Name: null

Comment: If you want to plunge the united states in to an economic landslide into irrelevancy you would pass this act.

Linux runs on 93% of the worlds devices, most of the software being generated is Open Source. If you stop people from installing Linux on their devices, including PC and router, you would be killing the largest organic and grassroot movement that has powered and continues to power the modern age.

After linux's release in 1991, it quickly grew to be a platform of choice for IT and programmers in the know. By 2000 it had made it's way its way into every scope of society. Every day that you use the internet, the cloud, visit any website you can think of. You are touching Linux. It is insanity to try and block the installation of Linux, the OS that BUILT the IT industry. Microsoft was once found out for running hotmail on linux hosts, Microsoft is simply a desktop operating system. Linux is an operating system that is at the core of Android, at the core of greater than 90% of web servers, 100% of Cloud service operators, and in greater that 70% of all servers in the world. The talented people who dedicate their life to this software and the creation of this software must program on a platform they are comfortable with.

If you do this, you will gut the IT industry. You will gut competition, and you will grow to realize that this was the single greatest failure of your political career, because the world will never forget who you are. Whatever you are being bought with is not worth ending your political career, or being the cause of decline in the united states.

I know that none of you understand or appreciate the technology that powers your life. I do IT for a living, I have that knowledge and appreciation. You don't know what the hell you are doing here, you just have no idea what on earth you are doing. There are hundreds of thousands of us who know what is going on, this is not mundane, this is not benign, this is important, this is massive.

If you sign this, you are signing a death warrant on the IT industry. I can't make it clearer, this is absolutely and massively important. DO NOT SIGN THIS BILL IN TO LAW. I work in IT, I'm telling you not to rob the future for a few dip shit lobbyists and corporations. DO NOT SIGN THIS. YOU WILL BE AT FAULT FOR THE LARGEST ECONOMIC FAILURE IN THE HISTORY OF THIS COUNTRY. I live IT, I breathe IT, I work in IT. DO NOT SIGN THIS BILL.

IF THIS BILL PASSES, THE WORLD, NOT THE UNITED STATES WILL FEEL IT. IF YOU SIGN THIS BILL, IT WILL ABSOLUTELY SHUT THE DOOR ON DEVELOPMENT OF SOFTWARE. IF YOU SIGN THIS BILL, YOU ARE ENDING AMERICAN IT COMPANIES. DO NOT PASS THIS BILL.

If you want to plunge the united states in to an economic landslide into irrelevancy you would pass this act.

Linux runs on 93% of the worlds devices, most of the software being generated is Open Source. If you stop people from installing Linux on their devices, including PC and router, you would be killing the largest organic and grassroots movement that has powered and continues to power the modern age.

After linux's release in 1991, it quickly grew to be a platform of choice for IT and programmers in the know. By 2000 it had made it's way its way into every scope of society. Every day that you use the internet, the cloud, visit any website you can think of. You are touching Linux. It is insanity to try and block the installation of Linux, the OS that BUILT the IT industry. Microsoft was once found out for running hotmail on linux hosts, Microsoft is simply a desktop operating system. Linux is an operating system that is at the core of Android, at the core of greater than 90% of web servers, 100% of Cloud service operators, and in greater that 70% of all servers in the world. The talented people who dedicate their life to this software and the creation of this software must program on a platform they are comfortable with.

If you do this, you will gut the IT industry. You will gut competition, and you will grow to realize that this was the single greatest failure of your political career, because the world will never forget who you are. Whatever you are being bought with is not worth ending your political career, or being the cause of decline in the united states.

I know that none of you understand or appreciate the technology that powers your life. I do IT for a living, I have that knowledge and appreciation. You don't know what the hell you are doing here, you just have no idea what on earth you are doing. There are hundreds of thousands of us who know what is going on, this is not mundane, this is not benign, this is important, this is massive.

If you sign this, you are signing a death warrant on the IT industry. I can't make it clearer, this is absolutely and massively important. **DO NOT SIGN THIS BILL IN TO LAW.** I work in IT, I'm telling you not to rob the future for a few dip shit lobbyists and corporations. **DO NOT SIGN THIS. YOU WILL BE AT FAULT FOR THE LARGEST ECONOMIC FAILURE IN THE HISTORY OF THIS COUNTRY.** I live IT, I breathe IT, I work in IT. **DO NOT SIGN THIS BILL.**

IF THIS BILL PASSES, THE WORLD, NOT THE UNITED STATES WILL FEEL IT. IF YOU SIGN THIS BILL, IT WILL ABSOLUTELY SHUT THE DOOR ON DEVELOPMENT OF SOFTWARE. IF YOU SIGN THIS BILL, YOU ARE ENDING AMERICAN IT COMPANIES. DO NOT PASS THIS BILL.

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: Peter

Last Name: Lonjers

Mailing Address: 7705 Hampton ave

City: West Hollywood

Country: United States

State or Province: CA

ZIP/Postal Code: 900046

Email Address: utilitarianexe@gmail.com

Organization Name:

Comment: You should not in anyway prevent the installation of user built software onto wireless devices. There are many reasons this is a bad idea. But for me the number one problem is education. If American students can not experiment on their own with wireless devices it greatly reduces the chances they will become innovators in the field. And no specific educational devices are not a substitute. Controlled enviroments ruin the fun and interest the leads to innovation. I understand that the radio spectrum is a shared resource. But the people who want to ruin that resource will in no way be stopped by your regulations. Further the problem is simply insignificant. I have never once had a problem with a radio device due to interference under the current regulations. I would be happy to deal with that to give some kid the chance to mess around with their home wifi.

You should not in anyway prevent the installation of user built software onto wireless devices. There are many reasons this is a bad idea. But for me the number one problem is education. If American students can not experiment on their own with wireless devices it greatly reduces the chances they will become innovators in the field. And no specific educational devices are not a substitute. Controlled enviroments ruin the fun and interest the leads to innovation. I understand that the radio spectrum is a shared resource. But the people who want to ruin that resource will in no way be stopped by your regulations. Further the problem is simply insignificant. I have never once had a problem with a radio device due to interference under the current regulations. I would be happy to deal with that to give some kid the chance to mess around with their home wifi.

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: Jared

Last Name: Gibson

Mailing Address: 10734 Borman Cir

City: Omaha

Country: United States

State or Province: NE

ZIP/Postal Code: 68127

Email Address: jgibson639@gmail.com

Organization Name:

Comment: Users should be able install custom firmware on what ever product they want as long as its not effecting anyone. By that logic gay marriage should be relooked at. I dont see why this is even an issue for the FCC. They should be more focused on looking at allowing cable companies to force users to pay for a cable box that hasent changed internally since 2011. What product technology wise hasent changed since 2011???? Anyways back on topic this is a non fcc issue. Are you going to not allow custom os choices for PC or Servers next? This is a feature that sells many routers!!!! So not only are you hurting companies that sell this as a feature but you are hurting innovation. In the USA we are all about choice and freedom of it. By taking away freedom such as choice of OS for a product for a router you are hurting the consumer and big business so who is this really a win for then????

-Nerds everywhere

Users should be able install custom firmware on what ever product they want as long as its not effecting anyone. By that logic gay marriage should be relooked at. I dont see why this is even an issue for the FCC. They should be more focused on looking at allowing cable companies to force users to pay for a cable box that hasent changed internally since 2011. What product technology wise hasent changed since 2011???? Anyways back on topic this is a non fcc issue. Are you going to not allow custom os choices for PC or Servers next? This is a feature that sells many routers!!!! So not only are you hurting companies that sell this as a feature but you are hurting innovation. In the USA we are all about choice and freedom of it. By taking away freedom such as choice of OS for a product for a router you are hurting the consumer and big business so who is this really a win for then????

-Nerds everywhere

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: ben

Last Name: freedheim

Mailing Address: 12514 4th ave nw

City: seattle

Country: United Kingdom

State or Province: washington

ZIP/Postal Code: 98177

Email Address: ben.freedheim@comcast.net

Organization Name:

Comment: Do not pass this bill as it destroys the ability to customize stuff that i own. Also, there is no way to enforce this type of ruling, effectively making it useless destruction of freedom

Do not pass this bill as it destroys the ability to customize stuff that i own. Also, there is no way to enforce this type of ruling, effectively making it useless destruction of freedom

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: Al

Last Name: Amin

Mailing Address: Shyamoli

City: Dhaka

Country: Bangladesh

State or Province: Dhaka

ZIP/Postal Code: 1207

Email Address: ialamin.pro@gmail.com

Organization Name: DIU

Comment: I object this because security and privacy is **important** to me.

I object this because security and privacy is **important** to me.

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: McKenzie

Last Name: Rochester

Mailing Address: 165 Tana Drive

City: Fayetteville

Country: United States

State or Province: GA

ZIP/Postal Code: 30214

Email Address:

Organization Name:

Comment: I refuse to have my rights infringed upon like this and I refuse to see such a massive blow against the open source community. Custom firmwares and OS's harm no one and they foster creativity among budding developers. This regulation to prohibit the downloading of custom software does no good for any citizen.

I refuse to have my rights infringed upon like this and I refuse to see such a massive blow against the open source community. Custom firmwares and OS's harm no one and they foster creativity among budding developers. This regulation to prohibit the downloading of custom software does no good for any citizen.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Thompson

Mailing Address: 5108 Stockton Dr.

City: Raleigh

Country: United States

State or Province: NC

ZIP/Postal Code: 27606

Email Address: thompsonutil@gmail.com

Organization Name:

Comment: There is really no reason for these rules to exist. I am a Computer Engineer and an Amateur Radio operator (KE4GIY) and I have been using Open Source firmware on Linksys wireless routers for years.

If you don't think the Open Source replacements are a good thing then explain to me why that is currently the best route for dealing just this one security exploit:

<http://www.pcworld.com/article/2925552/netgear-and-zyxel-confirm-netusb-flaw-are-working-on-fixes.html>

There is really no reason for these rules to exist. I am a Computer Engineer and an Amateur Radio operator (KE4GIY) and I have been using Open Source firmware on Linksys wireless routers for years.

If you don't think the Open Source replacements are a good thing then explain to me why that is currently the best route for dealing just this one security exploit:

<http://www.pcworld.com/article/2925552/netgear-and-zyxel-confirm-netusb-flaw-are-working-on-fixes.html>