

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eriq

Last Name: Augustine

Mailing Address: 465 Pismo St.

City: San Luis Obispo

Country: United States

State or Province: CA

ZIP/Postal Code: 93401

Email Address: eriq.public@gmail.com

Organization Name: California Polytechnic State University Computer Science Department

Comment: Hello,

As a professional Software Engineer and Computer Science Instructor at California Polytechnic State University, I believe that this action would directly hinder innovation in the tech industry as well as harm the US tech industry.

This action would force US companies to be less competitive on the international market as international companies could provide more trusted and feature-rich products.

Please rescind this action.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Frank

Last Name: Lilge

Mailing Address: 3062 S. Steele St

City: Denver

Country: United States

State or Province: CO

ZIP/Postal Code: 80210

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Barlow

Mailing Address: 873 Guerrero St

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94110

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Mario

Last Name: Koller

Mailing Address: Wassermannngasse 25

City: Wien

Country: Austria

State or Province: Wien

ZIP/Postal Code: 1210

Email Address:

Organization Name:

Comment: Dear FCC,

this is an unbelievably bad proposal. It is important to allow the installation and use of open source firmware. Often open source software is more secure and continues to receive security patches. Also, this is the only way to make sure that no hidden spy software is installed in the firmware.

Please vote no. 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: Giles

Last Name: Barton-Owen

Mailing Address: 1 Station Road,Dullingham

City: Newmarket

Country: United Kingdom

State or Province: Suffolk

ZIP/Postal Code: CB89UP

Email Address:

Organization Name:

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

I believe that users should have full control over the software on their device and manufacturers will not just protect the very small enclave of software the FCC has jurisdiction over. The general trend to more restrictive legislation damages research and development for small organisations.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: trevor

Last Name: payne

Mailing Address: 3216 mahaffey ct

City: pickerington

Country: United States

State or Province: OH

ZIP/Postal Code: 43147

Email Address: thetrevorpayne@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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Igor

Last Name: Petrakov

Mailing Address: 505 West 37th St. Apt 701

City: New York

Country: United States

State or Province: NY

ZIP/Postal Code: 10018

Email Address:

Organization Name:

Comment: I'm against any rule that prevents the legal owner of any electronic device from modifying, updating, overwriting, or changing any part of the software initially installed on the device by the manufacturer.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jim

Last Name: Davis

Mailing Address: 141 Minnear St

City: Cookeville

Country: United States

State or Province: TN

ZIP/Postal Code: 38501

Email Address: revhippie@gmail.com

Organization Name:

Comment: Please do not implement rules to restrict the freedom of users to install software of their choosing on devices they own.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Klein

Mailing Address: 21010 Southbank St #100

City: Sterling

Country: United States

State or Province: VA

ZIP/Postal Code: 20165

Email Address: davidklein@dhk.com

Organization Name: DHK Enterprises, Inc

Comment: The proposed changes to 2.1033 , sec. a4i and sec. 8e. and 2.1043 sec. 2 are a complete embarrassment.

Open source software like DD-WRT should remain part of the possible uses of privately owned wireless access points.

Frequently, the manufacturer based software has poor or compromised security for wireless encryption.

By removing the ability of consumers and businesses the capability to upgrade to more secure software, this proposed FCC rule is making our national infrastructure more susceptible to hackers and security intrusions.

I implore the FCC to think twice about forcing consumers and businesses to remain with insecure, faulty software.

Please remove this ruling.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Cody

Last Name: Reynolds

Mailing Address: 2054 seddington ct

City: Dublin

Country: United States

State or Province: OH

ZIP/Postal Code: 43016

Email Address:

Organization Name:

Comment: As a European who wants to see European tech companies become the leaders in the world I say this:

DO IT!!! It's time for European companies, European IT experts, etc. to shine. the European Parliament has been doing stuff but it's not enough. We need something that can kill US IT industry quickly and as painfully as possible and THIS IS IT!!!

We need collaboration from you, Americans, and THIS IS WHAT WE NEED.

DO IT, LOCK YOUR INDUSTRY, 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: Tyler

Last Name: Shiv

Mailing Address: 4607 Burgundy place

City: Oviedo

Country: United States

State or Province: FL

ZIP/Postal Code: 32765

Email Address:

Organization Name:

Comment: This is an absolutely horrible idea! Why would you want to remove our ability to have choice in software? I

LIKE using Linux and alternative Android versions. Don't take our choice!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Newman

Mailing Address: 6 Thirlestane

City: Edinburgh

Country: United Kingdom

State or Province: Lothian

ZIP/Postal Code: EH91HD

Email Address:

Organization Name:

Comment: Consumer computer networking equipment that includes a wireless component- especially home internet "routers" which consist of a combination modem, router, switch, and AP- are generally controlled by a single monolithic firmware package containing both high-level routing logic and low-level binaries to control the wireless hardware.

Your rule might intend only to cover the Wireless AP portion of the hardware, but it would in practice prevent the consumer from modifying any of the software running on the device. A sizeable number of people, myself included, are passionate about controlling the software that runs on their devices, especially their routers.

This is for practical reasons (third-party firmware is usually far more performant and featureful than that provided by the manufacturer), for security purposes (manufacturers rarely patch security vulnerabilities), and for philosophical and ethical ends: I find it important that computer systems and other devices work for me and are under my control, rather than restricting me and insisting that I only use the software provided.

I do not object in principle to a rule restricting the very low-level code that directly affects the wireless signals being sent by the radio hardware, since I understand that interference from unauthorised devices is a real problem. But it is necessary that such a rule would not, in actual practice, restrict the other software controlling the rest of the device.

Under your rule, Americans would not be able in practice to install their desired software on their devices even if they never enable the wireless components of them. To me, this does not seem acceptable.

Thank you for considering my comment.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Mintz

Mailing Address: 131 Woodbridge Avenue

City: Metuchen

Country: United States

State or Province: NJ

ZIP/Postal Code: 08840-2030

Email Address: mintz.eric@gmail.com

Organization Name:

Comment: "the applicant must also demonstrate that the device contains security features to prevent the loading of software that would allow the radio to operate in violation of the Commission's rules."

Many manufacturers will interpret this clause as a mandate to lock out all, even complying, third-party software, thereby gutting the ability of the open-source community to support new devices. Please add a clause requiring manufacturers to permit the installation of third-party software that complies with the commission's rules.

Failure to do so will put the future of high quality, secure, open-source router firmware like Tomato and DD-WRT in jeopardy, which could compromise the security of small businesses and individuals who depend on these packages.

"To minimize the potential for unauthorized modification to the software that controls the RF parameters of the device, grantees would have to implement well-defined measures to ensure that certified equipment is not capable of operating with RF-controlling software for which it has not been approved."

Again, this will render support of open source, community supported, and widely used software like DD-WRT and Tomato. Please reconsider.

Please recognize that the Internet and E-commerce runs on open source software. Large companies like Google and Amazon deploy many thousands of Linux servers, some of which need to support WiFi and Bluetooth. Furthermore, the requirement to "lock down" SDRs has the potential to damage the research community that has, so far, produces such marvels as TCP/IP, the basic protocol of the Internet, Bluetooth, and similar innovations. Also, it would cripple the ability of amateur radio operators (Hams) to experiment with new protocols, novel antennae, and to otherwise enhance existing devices so as to improve their function and advance the state of the art.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Potter

Mailing Address: 2212 Vermont Dr

City: Fort Collins

Country: United States

State or Province: CO

ZIP/Postal Code: 80525

Email Address: jpotter56@gmail.com

Organization Name:

Comment: It is my opinion, and that of many of my friends and coworkers that we should be able to modify any thing that we purchase in any way we see fit, so long as it is not in violation of any laws of the USA. Open source firmware on wireless routers for example. These firmwares make the routers more effective at providing cyber-security, allow for greater customization, provide better wireless coverage in places where stock firmware cannot do the job.

As for custom ROMs on cellular phones, they are often done to remove unnecessary programs that are embedded into the OS provided by the cell service provider. This provides for a faster and smoother operating phone, more storage capability and a more personal tailored interface.

One more item I would like to submit for consideration: if people cannot modify their devices, and a vulnerability is exposed, it would be exploitable for a much longer period with closed source programming as opposed to open source. Corporations do not update their firmware for products near as often as when the program is open source. Cyanogen, the makers of Cyanogenmod for Android cell phones releases an update nightly. My cell service provider has released two updates for my phone in the 1 1/2 years I have owned it.

I strongly urge you not to adopt this rule.

Regards,

Jason Potter

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Hettinger

Mailing Address: 18 Lenape Lane

City: Douglassville

Country: United States

State or Province: PA

ZIP/Postal Code: 19518

Email Address: jaredhettinger@gmail.com

Organization Name:

Comment: Right now, the FCC is considering a proposal to require manufacturers to lock down computing devices (routers, PCs, phones) to prevent modification if they have a "modular wireless radio"[1][2] or a device with an "electronic label"[3].

The rules would likely:

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

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

Ban installation of custom firmware on your Android phone

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Baniszewski

Mailing Address: 6243 Plaited Reed

City: Columbia

Country: United States

State or Province: MD

ZIP/Postal Code: 21044

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Cuevas

Mailing Address: 2729 NW 66th Terrace

City: Gainesville

Country: United States

State or Province: FL

ZIP/Postal Code: 32606

Email Address:

Organization Name:

Comment: I would like to 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. Such rules are akin to telling American citizens they can't modify their car or remodel their home. If I want additional functionality in my WiFi/RF enabled device I should be able to add that functionality if I have the skill set to do so. The thought that implementing such rules will in some way shape or form stops bad people from doing bad things with these devices is ridiculous. These proposed rules are a knee jerk reaction due to a lack of understanding of the actual problem. These devices are tied to protocols that have inherit design flaws and simply locking a device does nothing to fix the core issues.

HAM Radio is better with SDR. Cell phone technology is better with Open Source operating systems.

The ability to enhance or fix a legacy piece of WiFi/RF equipment that a manufacturer no longer supports is a reasonable expectation for an individual to have; much like fixing an old car with a newly built part.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: BRAYDEN

Last Name: DEAN

Mailing Address: 11867 W KINDERMAN DR

City: AVONDALE

Country: United States

State or Province: AZ

ZIP/Postal Code: 85323

Email Address:

Organization Name:

Comment: Technology users must reserve the right to install whatever software they choose on 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. I myself have fixed major security flaws by modifying 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: Brian

Last Name: Dague

Mailing Address: 6615 150th SW

City: Lakewood

Country: United States

State or Province: WA

ZIP/Postal Code: 98439

Email Address: bd77778@gmail.com

Organization Name:

Comment: I feel that this would restrict my ability to use equipment I purchase and currently own. I have reason to want to install alternate operating systems on my computer, mes with the antenna on my home router, and use my iPhone in a way such as I please. THis law restricts not just electronics I use for personal enjoyment, but also my ability for me and others to innovate. The need to restrict our right to modify devices we own is completely unfounded and counterproductive to technological advancement.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Bailey

Mailing Address: 538 Messina Terrace

City: Davis

Country: United States

State or Province: CA

ZIP/Postal Code: 95616

Email Address: etotheright@yahoo.com

Organization Name:

Comment: Revoke this proposal immediately. I'm appalled that this was even considered, and I don't know which of the three options is most fearsome - that the lawmakers are ignorant enough to buy it, that the lawmakers are corrupt enough to sell us out, or that the lawmakers are malicious enough to strike such a blow against the American people.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Rene

Last Name: Horn

Mailing Address: 1435 N McCarthy Rd #4

City: Appleton

Country: United States

State or Province: WI

ZIP/Postal Code: 54913

Email Address: the.rhorn@gmail.com

Organization Name:

Comment: This would effectively outlaw open source software on wireless devices. Open source software is a cornerstone of technological progress these days, and a necessity for its future.

Some of the best ideas have come from people being able to tinker with their own devices, and customize it the way they want. This would prevent that. Researchers are often self-motivated problem solvers, and often times the way they go about solving those problems is to take something they own themselves, and start playing with it, and making customizations.

I implore you to always keep in mind allowing private citizens the freedom to make customizations to their own equipment that they have bought for themselves. This is especially important for when a manufacturer stops supporting a product.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Hans

Last Name: Martin

Mailing Address: 1818 NE 47th St

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98105

Email Address: hansmrtn@gmail.com

Organization Name: Psi Upsilon, Theta Theta, University of Washington

Comment: The decision to block the use of open source is not a good idea. Open source software is the most moral and safe way of data. Blocking this provides no benefit for anything. I urge the the FCC to make reevaluate this idea.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Crawford

Mailing Address: 565 Burnett Ave.

City: San Francisco

Country: United States

State or Province: CA

ZIP/Postal Code: 94131

Email Address: fcc@accounts.acrawford.com

Organization Name:

Comment: This proposal is particularly concerning to me. Having spent my career working on consumer electronics, I can tell you that manufacturers are not interested in security or support. Once the consumer has purchased the device, that is pretty much the end of the relationship; no more security patches and no more feature updates. As a result, many products are found to be vulnerable over time. This is key. Finding vulnerabilities is good. It means that we can improve the products and protect the consumer. By enforcing that the firmware is locked-down and closed-source, you are preventing people from discovering these issues and, more importantly, fixing them. Open source software allows individuals like myself to improve on other people's work and exercise my hardware to its fullest extent. Yes, allowing people to modify the function of a device would allow them to operate the device outside of the regulated parameters, but I can assure you that this will happen regardless. Take a look at Android. It is in the manufacturer's best interest to prevent people from loading custom ROMs (read-only memory images) onto the phones and tablets. After all, if the customer isn't using the manufacturer's store, the manufacturer doesn't make any money. And yet, people find a way to swap out the software anyway. In computer security, the rule of thumb is that if the attacker has physical access to the hardware, it will be compromised. The same is true for consumers and their electronics. There will always be people like myself who understand how to circumvent those protections and will do everything in their power to spread that knowledge. Attempting to limit the software that can be loaded onto these devices is a losing battle and will only serve to cripple the security and functionality of these 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: Derrick

Last Name: Patterson

Mailing Address: 678 E Caston Rd

City: Uniontown

Country: United States

State or Province: OH

ZIP/Postal Code: 44685

Email Address: derricklpatterson@gmail.com

Organization Name:

Comment: See attached file(s)

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.

Sincerely,

Derrick L. Patterson

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kevin

Last Name: Miller

Mailing Address: 15125 SE 40th pl

City: Bellevue

Country: United States

State or Province: WA

ZIP/Postal Code: 98006

Email Address: kevinbladeloganmiller@gmail.com

Organization Name:

Comment: Distinguished decision makers,

It is possible to modify the software on a Software Controlled Radio without affecting its radio parameters.

I propose that the commission create a distinction between software that is used to control a device's radio parameters (power, frequency, etc) and software that provides other functions (user interface, signal processing etc).

Such a distinction could serve as a precedent for establishing rules that reflect consumer needs as well as public safety concerns.

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: Phillip

Last Name: Tran

Mailing Address: 188 Acropolis Rd

City: Lowell

Country: United States

State or Province: MA

ZIP/Postal Code: 01854

Email Address: SuperHunter12345@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jaye

Last Name: Culverhouse

Mailing Address: 40 Clarke road

City: Northampton

Country: United Kingdom

State or Province: Northamptonshire

ZIP/Postal Code: NN1 4PW

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Klamo

Mailing Address: 5049 Hahns Peak Drive

City: Loveland

Country: United States

State or Province: CO

ZIP/Postal Code: 80538

Email Address:

Organization Name:

Comment: Recently I came across the news that the FCC would attempt to crack down on open source software for wireless devices, and I wanted to submit a comment in opposition to this decision. Limiting users to closed source software is a horrendous idea, especially with how concerned users are these days about privacy and software transparency. I urge you to rethink your decision and side with consumers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Brookshire

Mailing Address: 5733 Everglades Lane

City: Norcross

Country: United States

State or Province: GA

ZIP/Postal Code: 30071

Email Address: thbjr2@gmail.com

Organization Name:

Comment: Please vote for open source software to be AVAILABLE. Community review of code allows for others to verify what one installs is secure and free of malware. It is a proven fact that open source software is the most secure software available. Examples of this are OpenBSD, FreeBSD, Ubuntu, ArchLinux, and a plethora more.

Preventing open source software from being available also allows for monopolies to exist for software. An example of this is Gimp and Adobe Photoshop. Gimp is a free alternative for those that cannot afford Adobe Photoshop and still want to hone their skills with photo editing.

As someone that works in cyber security for the CDC, this issue is deeply important to me. Anyone that votes against open source is not someone that receives my vote.

Thank you for reading my request and considering this issue.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Bradley

Last Name: Clements

Mailing Address: 3907 W Valley View Dr

City: Cedar Hills

Country: United States

State or Province: UT

ZIP/Postal Code: 84062

Email Address: bhccomm@gmail.com

Organization Name:

Comment: Please do not enact regulations that would make it difficult or impossible for hobbyists to load their own software on wireless devices they own. I am an amateur radio operator, and I have several wifi devices on which I have replaced the supplied firmware with software that facilitates building mesh networks. I use these devices to provide communications for an ultra-marathon held in the remote west desert of Utah each fall where there is no cellular or other communications networks available. These devices are also ready to form a regional mesh network for emergency communications in the event of a regional disaster. It would be impossible to do this if the proposed regulations were enacted.

Another reason this is a bad idea is that manufacturers of commercial wifi gear (routers, access points, etc.) often do a very poor job of making updates available as standards change or as vulnerabilities are discovered in their software. To continue using these devices securely we need to be able to replace the software that comes installed on these devices with better-maintained open source alternatives such as OpenWRT.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Chance

Last Name: Larson

Mailing Address: P.O. Box 167

City: Solon Springs

Country: United States

State or Province: WI

ZIP/Postal Code: 54873

Email Address:

Organization Name:

Comment: Please do not enact these rules that would prevent people from using 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: Daniel

Last Name: Estes

Mailing Address: PO Box 939

City: Talbott

Country: United States

State or Province: TN

ZIP/Postal Code: 37877-0939

Email Address:

Organization Name:

Comment: I am against taking away the ability of a end-user/consumer to install other software on electronic devices than what the manufacturer installed. First, it goes against the basic notion that once I purchase an item, what I do with it, generally speaking, should be of no one else's concern. Also, if manufacturers refuse to issue patches or security updates to equipment they manufacture (planned obsolescence), under the proposed rule owners will be unable to install third-party software to fix the issues.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Marlin

Mailing Address: 650 Baseline Rd

City: Grand Island

Country: United States

State or Province: NY

ZIP/Postal Code: 14072

Email Address: rxm4946@g.rit.edu

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.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: isaac

Last Name: leese

Mailing Address: 1030 mambrino

City: oregon

Country: United States

State or Province: OH

ZIP/Postal Code: 43616

Email Address:

Organization Name:

Comment: Commissioners, please do not implement rules that take away the ability of users to install the software of our choosing on our computer devices.

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

Consumers 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 and retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Consumers pay for and expect to own the hardware we purchase.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Guilherme

Last Name: Silva

Mailing Address: 28 Edmands

City: Framingham

Country: United States

State or Province: MA

ZIP/Postal Code: 01752

Email Address:

Organization Name:

Comment: Wireless networking research depends on the ability of researchers to investigate and modify their devices, the proposed regulations would transform these devices into "black-boxes" making them much less secure. We need the ability to fix security holes these devices when the manufacturer chooses to not do so or abandons support for the hardware. Users have in the exercised this before to correct bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such hotspot vendors, depend 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: Yui

Last Name: Daoren

Mailing Address: 1140 Calle Amanda Apt A

City: Santa Fe

Country: United States

State or Province: NM

ZIP/Postal Code: 87507

Email Address: ydaoren@gmail.com

Organization Name:

Comment: Please do not implement rules that would limit or remove 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. There can be no innovation from outside large companies with rules restricting this.

Citizens need the ability to fix security holes in their devices when the manufacturer chooses to not do so or is unable to 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: Matt

Last Name: Bell

Mailing Address: 1010 150th Street SE

City: Bellevue

Country: United States

State or Province: WA

ZIP/Postal Code: 98007

Email Address:

Organization Name:

Comment:

Dear FCC,

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

Please consider that:

- 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: Nathaniel

Last Name: Czupka

Mailing Address: 10 Sylvan St

City: Salem

Country: United States

State or Province: MA

ZIP/Postal Code: 01970

Email Address: nathaniel.czupka@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. 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: Ryan

Last Name: Young

Mailing Address: 5093 b Defford Place

City: Eagleville

Country: United States

State or Province: PA

ZIP/Postal Code: 19403

Email Address: ryanyoung1633@live.com

Organization Name:

Comment: This is just going to limit our ability as consumers to take security into our own hands. Manufacturers dont even patch security holes in these embedded devices in a timely manner or even at all. If the device is old, good luck. That is why ddwrt and tomato firmware is popular among the open source communities.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Trey

Last Name: Troyer

Mailing Address: 630 South Mill Street

City: Orrville

Country: United States

State or Province: OH

ZIP/Postal Code: 44667

Email Address:

Organization Name:

Comment: Hello, if you could not restrict the use of open source hardware and software that would be fantastic. Open source materials are quite literally one of the ways freedom exists in our modern technologically driven world. Undoing such an important facet of our freedom in the technology sector is a step in the wrong direction for maintaining the ability for modern tech to stay in a free and competitive market that affects us on a daily basis.

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: John

Last Name: Hancock

Mailing Address: 715 hoyt st

City: portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97208

Email Address:

Organization Name:

Comment: This is an absolutely horrid proposal which reeks of corporate bribery. These days many people install software like DD-WRT or OpenWrt on their routers to add new features. This extends the usable life of the router by bypassing the planned obsolescence implemented by the manufacturer. This proposal is nothing more than a plan to increase corporate profits at the expense of the consumer. The individual who submitted this proposal should be investigated and ultimately arrested for their blatant corruption and disregard for the well-being of the American public.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joel

Last Name: Bennett

Mailing Address: 370 Farrell Road Ext.

City: West Henrietta

Country: United States

State or Province: NY

ZIP/Postal Code: 14586

Email Address: Jaykul@HuddledMasses.org

Organization Name:

Comment: Please reconsider passing rules which will effectively prevent users from installing the software of their choosing on hardware they purchase. People who purchase hardware should not be prevented from using it: they should be able to manipulate and control all aspects of their devices.

If these rules stand, manufacturers will almost certainly employ digital locks as the only practical way to secure things, and blame them on the FCC -- this will mean locking users out of the full usability of their hardware as well as preventing the use of open source for security reasons, and it will mean that users cannot check for back doors, fix security holes, or support hardware after the manufacturer decides it's too old.

Americans need the ability to fix security holes in their devices when the manufacturer chooses not to, and there is a long history of users fixing serious bugs in wifi drivers -- which would now be banned under these proposed "security requirements."

Wireless networking research depends on the ability of researchers to investigate and modify their decides, and billions of dollars of commerce, such as many secure wifi vendors, retail hotspot software and more depends on the ability of users and companies to install custom software of their choosing on this hardware.

On top of all of that, this is a particularly inopportune time, politically speaking, to be locking down hardware and preventing users from installing their own software, or checking for backdoors.