Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Pennycuff
Mailing Address: 610 N Dyer Park
City: Eagle River
Country: United States
State or Province: WI
ZIP/Postal Code: 54521
Email Address: dap6000@hotmail.com
Organization Name:
Comment: I have concerns with the software defined radio (SDR) rules.

I fail to see how modifying software on consumer grade RF equipment is significantly different from "jailbreaking" a cell phone, which has been cleared of any legal issues for the past several years. When I buy hardware, I should own it. And I should have the right to modify it within reasonable limits, including changing or replacing its software. Sections A.38 - A.42 cover some of this, although SDRs are placed under additional limits due to their extensible nature.

I understand part of the goal here is to establish what those reasonable limits are. If any third party, open source, or "homebrewed" software can be loaded into such hardware it becomes impossible to test every possible configuration. That's a hard problem. But I prefer solutions that don't limit 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: Gidon
Last Name: Rosenthol
Mailing Address: 4423 Lehigh Road #112
City: College Park
Country: United States
State or Province: MD
ZIP/Postal Code: 20740
Email Address:
Organization Name:
Comment: If I understand the proposed rule change correctly, this would prevent end users from modifying their home router firmware. While many users are content with the factory-provided firmware, there are quite a number of folks using aftermarket alternatives that offer greater flexibility and security. As one of those folks--I use DD-WRT to secure my home network far beyond what Netgear's factory firmware would allow--I must protest the suggested changes in the strongest possible terms.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Gary
Last Name: Mirkin
Mailing Address: 23 Wintergreen Way
City: Sewell
Country: United States
State or Province: NJ
ZIP/Postal Code: 08080
Email Address: mirkin3@gmail.com
Organization Name:
Comment: I would respectfuly request the FCC consider Not allowing restrictions on WIFI networking equipment. This would inhibit radio amateurs & others, from personally modifying devices for private & community service networks. Setting up a situation, where is a proprietary restriction on the use of such devices, would Not be in the public, or community interests.

With sincere regards,

Gary Mirkin
WA3SVW

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Dion
Last Name: Dennis
Mailing Address: 113 Lake View Drive
City: Cedar Creek
Country: United States
State or Province: TX
ZIP/Postal Code: 78612-3055
Email Address: dion.dennis@gmail.com
Organization Name:
Comment: As someone who has had to install Open Source firmware to deal with the abysmal security holes in manufacturer firmware, I would ask the FCC to revisit this issue, for the following reasons:

1. As has been the case with the burgeoning of the Internet of Things (and has been well-pointed out by security experts such as Bruce Schneier), manufacturers have often installed firmware which was poorly coded to begin with, and contained many security holes. In addition, generally, they have also been slow (or absent) in upgrading router firmware to deal with widespread and dangerous exploits. (Ars Technica and ZDNet, in particular, documented this fact in some trenchant 2014 articles. A very brief Google Search will verify this fact).

I can tell you, for a fact, that the security of my interactions online, via my router, is enhanced by my ability to install more up-to-date and reliable firmware for my router. Frankly, given the poor record of providing such updated firmware by manufacturers, the net takeaway is that we will all be more insecure, more vulnerable to digital criminality.

In addition, there's a broader issue, at work. Frankly, the best work in the digital community comes from those who productively create improved systems outside of official channels. "Lock in" to modify specific code "locks out" those who wish to exercise the freedom to positively improve performance and reduce risk.

It would be far preferable if manufacturers WORKED WITH the OPEN SOURCE COMMUNITY, rather than banish them, via administrative rules. That will NOT make us safer. That will NOT reduce collective risk. It will make us, collectively, more insecure, given the inherent secrecy of most bureaucratic and corporate cultures.

The ruling has implications beyond just routers, then, to tablets, smartphones and the like. (As a Linux user, an Open Source advocate, I am also very concerned about the precedent of just such a "lockout.") There's an active community of lawful and competent "modders" who work for the Public Good. Please don't use administrative rules to lock them out of their ability to contribute, to invent and to improve, and to hold corporations accountable for, too often, sacrificing security, in the design of their products, in pursuit of short-term profit.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Stefano
Last Name: De Carlo
Mailing Address: Via Per Papanice
City: Crotone
Country: Italy
State or Province: Crotone
ZIP/Postal Code: 88900
Email Address:
Organization Name:
Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. They will hamper security, commerce, and innovation.

* Manifacturers are known for their terrible record in providing security fixes, most of the devices involved are *never* updated during their lifetime, instead preferring to just ignore current devices and iterate on a new product. This has come to its ultimate consequences recently, when a software bug affecting a *billion* of smartphones has been discovered and won't be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manifactures are not and cannot be forced to provide security fixes.

* Without the ability to modify the software running on these devices, nothing more than the very limited, more lucrative use cases addressed by the manifacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

* Research and innovation in wireless communications, ranging from entirely new designs, models and protocols to software implementations, would basically come to an halt, severely harmed by the unavailability of low-cost, readily-available solutions upon which to experiment. Community Mesh Networks are entirely reliant on the ability to customize low-cost networking equipment.

* These rules are overreaching and not even helping in ensuring compliance. Virtually none of the FCC rule breaches is due to 3rd-party software modification. It is however *still* possible to trivially enable non-compliant modes on unmodified devices on major wireless equipment manifactures.

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: McConachie
Mailing Address: 4305 Centre Ave
City: Pittsburgh
Country: United States
State or Province: PA
ZIP/Postal Code: 15213
Email Address: smutt@depht.com
Organization Name:
Comment: Please do not do anything to interfere with the development of OpenWRT, DD-WRT or similar alternative firmware. It is important that consumers maintain the right to change the OS of any devices they own.

For the purposes of preventing spectrum interference it is necessary that software controlled radios not be easily reprogrammable. However, this requirement should in no way interfere with the legitimate right of consumers to change the general purpose OS's of their legally purchased devices.

Sincerely,
Andrew McConachie

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Blazosky
Mailing Address: 2104 Willow Creek Dr
City: Little Elm
Country: United States
State or Province: TX
ZIP/Postal Code: 75068
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: Jeff
Last Name: Byers
Mailing Address: 12321 Buckskin Trl
City: Poway
Country: United States
State or Province: CA
ZIP/Postal Code: 92064-6007
Email Address: jeff.byers@gmail.com
Organization Name:
Comment: Hello,

With this FCC NPRM, if your intent is to eliminate the hobbyist and open source re-purposing of old WiFi equipment, to serve the purpose of lobbying commercial manufactures, or governmental security agencies (i.e. NSA, FCC, etc.), do please rethink this! I do not think that this is your job.

If the intent and understanding of this rule change is being misunderstood, please make the necessary changes to correct the wording.

I'm running a number of WiFi routers using open-source firmware, and am considering upgrading to a new device that would also support that. I've gotten many years out of older equipment, that without the open firmware, would have had to be retired into a landfill because of security issues that the manufactures would not address.

I am also a Amateur Radio enthusiast that is interested in HSMM using re-purposed WiFi equipment:

High-speed multimedia radio (HSMM)
https://en.wikipedia.org/wiki/High-speed_multimedia_radio

I am also worried how this ruling will, acting as a precedent, impact SDR in general, operating on other bands.

As many have pointed out, this rule change could cripple or limit these efforts:

Wi-Fi Hobbyists Worry New FCC Rules Could Ban Custom Firmware
http://www.dslreports.com/shownews/WiFi-Hobbyists-Worry-New-FCC-Rules-Could-Ban-Custom-Firmware-134765

FCC Introduces Rules Banning WiFi Router Firmware Modification
https://hackaday.com/2015/08/31/fcc-introduces-rules-banning-wifi-router-firmware-modification/comment-page-2/

FCC considering proposal to lock down computing devices (routers, PCs, phones, SDRs) to prevent modification
http://www.southgatearc.org/news/2015/august/fcc_proposes_ban_on_sdr_radios_and_more.htm

Thanks.

~ Jeff Byers ~

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Ian
Last Name: Sorensen
Mailing Address: 14510 Hampton Pl
City: Davie
Country: United States
State or Province: FL
ZIP/Postal Code: 33325
Email Address: ianakselsorensen@gmail.com
Organization Name:
Comment: Dear Public Servants of the Federal Communication Commission,

I write to you today with great concern and urgency. Current proposals in place will severely limit the freedoms of the American people with great impact on the future of America, and the ability of the country to go proceed into the 21st century.

We live in a society that is proud to be free, but yet this proposal limits the freedoms of the future. Alternative operating systems do no harm, instead they benefit society. The ability to install these with unlimited access allows users to experiment with computers. This can peak the interest of children and teens and influence them to join the work force and specialize in the fields that are necessary for America's survival, engineering. It seems completely pointless to limit the top achievers and innovators of America, and then wonder what happened to innovation.

Not only does this stifle innovation but it also hampers security research. This proposal makes it illegal for researchers to experiment with new technologies, something that has proven detrimental in the past. Most security holes in networking technologies are discovered and patched by third parties, but with this proposal, the patching of technology, even for personal use, becomes illegal. How does that make sense? This proposal appears to value businesses more than consumers, and that is a major problem.

I hope my pleas do not fall on deaf ears and the FCC chooses wisely in scrapping this proposal. The FCC gained huge rep when it supported Net Neutrality, do not let that reputation fall or turn into disgust.

Respectfully,
Ian Sorensen, a concerned citizen and aspiring computer science researcher

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Morgan
Mailing Address: 878 Venoy Ave
City: Madison Heights
Country: United States
State or Province: MI
ZIP/Postal Code: 48071
Email Address:
Organization Name:
Comment: I've seen several mentions from associates that the language included essentially forces manufacturers to lock down software defined radio. I wanted to add my voice to the choir opposing this.

Freely being able to install firmware on devices such as wireless routers is critical for innovation and user freedom. Opensource projects such as Tomato allow users full access and use of their equipment that would otherwise be hobbled by the manufacturers indifference. Look at the explosion of access that occurred after Linksys open-sourced their firmware- people were taking the devices so far beyond what had been previously possible.

Please reconsider this stand- banning things because someone might abuse them is a slippery slope, and anyone wanting to accomplish what you're trying to prevent will easily be able to work around these 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: William
Last Name: Marone
Mailing Address: 250 McAdoo Dr. Apt. 523
City: Folsom
Country: United States
State or Province: CA
ZIP/Postal Code: 95630
Email Address: wmarone@gmail.com
Organization Name:
Comment: The proposed rules require heavy restrictions on the firmware that operates on home routers, devices that up to this point have been relatively unrestricted.

While I understand the concerns of the FCC with respect to pollution of the EM spectrum, particularly public use ranges, up to now this has not been a problem and I don't see a compelling argument for why it would become one.

There are compelling arguments against the lock-down rules, which explicitly attack 3rd party firmware like DD-WRT (mentioned in the proposal) and OpenWRT, which I use personally.

Consumer routers have a track record for problems not with EM interference, but they do have a history of privacy violations, instability, security weaknesses, and general lack of features. 3rd party firmware resolves these issues by providing extensive feature capabilities, no privacy intruding software, very stable middle-ware, and frequent security updates and secure default configurations.

Mandatory lock down as proposed by the FCC would do little to protect the spectrum from abuse, but would undoubtedly go far in harming end 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: Aeschliman
Mailing Address: 232 NW Timothy St
City: Pullman
Country: United States
State or Province: WA
ZIP/Postal Code: 99163
Email Address: jbajbajba@gmail.com
Organization Name:
Comment: NO!
I find this extremely concerning.

Editing drivers or firmware is causing no harm in itself and should not be illegal. Innovation and freedom would be limited in ways not helpful for the American people. This would be a fundamental over reach by the government.

The freedom to edit one's own phone, router, PC and SDR should not be limited in itself. One shouldn't have to ask permission for this!

A law could limit the modification for a specific purpose but not limitation period!
And one would have there device checked according to the 4th amendment.

IN SHORT DO NOT LIMIT FREEDOM ON THE BASIS THAT ONE "COULD" DO HARM!!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Williams
Mailing Address: 365 SW State St.
City: Pullman
Country: United States
State or Province: WA
ZIP/Postal Code: 99163
Email Address: morgan.will@gmail.com
Organization Name:
Comment: The intended actions go far beyond the intended result. Removing the options to make under penalty of normal and personal/industry decisions (like which computer Operating System one uses, which System their router uses, and the ability to buy hardware custom configured and supported from re-sellers, what type of network protocol to use, etc.). The intended scope seems to go after an incredibly small usage case scenario, but impacts in a vast swath of practical and imperative options that are otherwise benign in terms of the FCC's charge.

Though the focus is to keep RF usage within their regulatory capacities, and limit the unintentional use outside those boundaries it to much a much greater effect, affects all areas of personal and business technology. Beyond that the proposed actions limit the technologies and their uses WITHIN the legal usage boundaries of which does nothing but hamper further development and innovation. It will add a greater course of regulation to that which is already within the the regulatory guidelines, and for no apparent result. What is the advantage of dictating what software used the licensed and regulated rf device if it is broadcasting within its allocated spectrum and within power guidelines?

Regulatory capacities are important and needed, but beyond the specific scope of RF usage the FCC is hampering personal and business technology decisions and advancement. Please do not further limit the development or the advancement of technology. Instead please scope and define what is proper usage and what isn't and leave it open within them for innovation and personal choices to flourish. There is a great opportunity to shepard the technological spaces used under the FCC's jurisdiction, and guide them within a proper usage. The proposed actions do nothing to do this, and impact sectors outside the intended RF usage as stated.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Maciej
Last Name: Urbaski
Mailing Address: rooter.kun+federalregister@gmail.com
City: Poznan
Country: Poland
State or Province: Wielkopolska
ZIP/Postal Code: 60-716
Email Address:
Organization Name:
Comment: Hello,
I'm not a USA citizen, but as you should be aware products are created with the widest target possible, thus if some restriction have to implemented for one large region you can expect them to be released in every region as tailoring product for each region would mean extra costs.

That is why I'm very worried about proposed restrictions for software manipulation. I have done my share of work in wireless mesh networks research field and use my freedom of choosing software for home use as well. Even my Android phone has installed Cyanogenmod firmware. None of these will be possible (at reasonable cost) anymore if your proposition will pass.

Why this is important?
* because everybody should have be able to contribute to scientific community and dedicated hardware cost are prohibitive, while now we can take almost any hardware and thanks to project like openwrt make a wireless testbed very cheaply
* as previously mentioned my phone uses community-supplied software - why did I make an effort to install it? my phone is no longer supported by its producer. This means my personal data was constantly at risk and if not for possibility of installing alternative software I wouldn't be able to do anything about it. Well except throwing perfectly working hardware away contributing to meaningless pollution of our environment.
* the same applies to wireless routers (again Openwrt to the rescue)
* implementing these protections will cost and that cost has to be shifted onto end users

Please note while as I have written above your regulations will affect people worldwide they will affect USA the most. These means the security issues will make the USA citizens the most likely targets and lower your nation security as a whole.

The consequences of such software modification

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Ed
Last Name: Champion
Mailing Address: 630 Reed Avenue
City: Franklinville
Country: United States
State or Province: NJ
ZIP/Postal Code: 08322
Email Address: n2ro.ed@gmail.com
Organization Name:
Comment: I am the Emergency Coordinator for Gloucester County for the ARRl. In addition, I am the RACES Radio Officer for Gloucester County. The use of WIFI router with modified software plays an important part in our EmComm communications.

It is my belief that stopping the use of these routers will setback EmComm communications.

Please do not enact this restriction.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Baumbach
Mailing Address: Hauptstrae 8
City: Saarbrcken
Country: Germany
State or Province: Saarland
ZIP/Postal Code: 66125
Email Address:
Organization Name:
Comment: I object to these rules because:

* 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: Stephen
Last Name: Goble
Mailing Address: 105 White Pine Road
City: Newland
Country: United States
State or Province: NC
ZIP/Postal Code: [28657]
Email Address: goblenc@yahoo.com
Organization Name:
Comment: I support fascist tyrant suicides!

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Mauro
Last Name: Parra
Mailing Address: 10685-B Hazelhurst Dr. # 17617
City: Houston
Country: United States
State or Province: TX
ZIP/Postal Code: 77043
Email Address: mauropm@me.com
Organization Name:
Comment: Dear FCC,

please don't implement this 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.

Thanks for reading this 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: James
Last Name: Klaas
Mailing Address: 5986 Runnymeade Dr
City: Canton
Country: United States
State or Province: MI
ZIP/Postal Code: 48187-2838
Email Address: jklaas@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: Jennifer
Last Name: Sensiba
Mailing Address: 870 Maple
City: Las Cruces
Country: United States
State or Province: NM
ZIP/Postal Code: 88001
Email Address: jennifer@sensiba.com
Organization Name:
Comment: It is common for amateur radio operators to modify commercial WiFi hardware for amateur use by changing the firmware.

This rule needs to specifically make clear that part 97 users are exempt.

Additionally, any requirements for firmware modification protections need to include easy workarounds for part 97 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: Matti
Last Name: Lammi
Mailing Address: Pekkalankatu 18
City: Kemi
Country: Finland
State or Province: Lappi
ZIP/Postal Code: 94700
Email Address:
Organization Name:
Comment: I oppose these updates on the rules that govern the evaluation and approval of RF devices. These updates are too restrictive and pose a significant threat to a free digital society. These updates are likely to:

1. Restrict installation of alternative operating systems on one's PC, like GNU/Linux, OpenBSD, FreeBSD, etc. limiting people's options to use computers in freedom from corporate control
2. Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes hindering innovation and progress
3. Ban installation of custom firmware on one's Android phone
4. Discourage the development of alternative free and open source WiFi firmware, like OpenWrt
5. Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.
6. Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses. This reduces competition and hinders economic growth.

So, even though I am not US citizen, I oppose these updates because they are harmful to US citizens and they are more than likely to find their way into the EU legistlation if approved in the US.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Elliott
Last Name: Dicus
Mailing Address: 55 Hermann St.
City: San Francisco
Country: United States
State or Province: CA
ZIP/Postal Code: 94102
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,

I urge you to reconsider this proposed rule for a few very important reasons.

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices. This should not be limited to corporations and internal testing.

2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Many times in the past, hardware that is no longer supported by a manufacturer is improved by community efforts.

3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under this rule. This will have a tangible and wide reaching negative effect on security.

4. 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.

Please consider these wide reaching effects, and reject 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: Daniel
Last Name: Baumgarten
Mailing Address: 43 Hutchinson Dr
City: Port Monmouth
Country: United States
State or Province: NJ
ZIP/Postal Code: 07758
Email Address:
Organization Name:
Comment: I respectfully request that the current proposal be rejected or at least modified so as not to require the locking down of computing devices with wireless radios.

This aspect of the proposal would gravely injure the common good. With no way to install the firmware of one's choosing on one's own computing devices, the consumer is no longer an equal party in exchange with the manufacturer. The relationship between individual private citizens and the large corporations that manufacture consumer electronics is therefore no longer equitable. Consumers no longer have the freedom to fix bugs in their devices in spite of the manufacturer's choice not to. They cannot know for sure that their device does not contain a mass surveillance backdoor, which infringes their human right to privacy. In the present political climate, it immediately arouses suspicions that large corporations and government spy agencies will use this FCC regulation as a means to unlawfully spy on U.S. citizens.

Therefore, the proposal is unacceptable. If it is not rejected or changed accordingly within a reasonable time frame, I plan to contact my representative.

Sincerely,
Daniel Baumgarten

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Romick
Mailing Address: 156 Oakridge Dr
City: Choctaw
Country: United States
State or Province: OK
ZIP/Postal Code: 73020
Email Address: romick.rb@gmail.com
Organization Name:
Comment: An possible unintended consequence of this regulation is preventing users from running open source software on their router. I run OpenWRT on my Netgear router because consumer grade router manufacturers have historically not been interested in improving and updating the firmware on their routers. The most concerning consequence of this is poor security.

Other concerns I have heard include:
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 ban me from loading custom software on my router.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Pollock
Mailing Address: 16 Wellington St. #4
City: Boston
Country: United States
State or Province: MA
ZIP/Postal Code: 02118
Email Address: ryan@ckfce.com
Organization Name:
Comment: I respectfully request the FCC not to implement rules which would take away the ability of users to install software of their own choosing on computing devices. I believe that it is essential to the long term freedom and success of the United States that general purpose computing devices be free from restrictions on who decides what is acceptable to run on them.

I believe that existing laws and regulations more than cover the legal usage of computing devices. Enforcement of these laws should not require technical lock down on who can execute code on a device.

The future of computing will see computers and devices moving to many devices. Americans need the ability to maintain and update these independent of the companies that produce them. This is of great importance with regards to security holes that will inevitably arise.

Additionally I think that it is vital for the experimentation, exploration, learning, and ultimately entrepreneurship of our country that devices remain accessible. Locking down hardware benefits incumbent technology vendors at the cost of new players who may not even realize the business implications rising from tinkering and invention. New wireless network research is one area that relies on free access to devices.