

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Santangelo

Mailing Address: 1132 Edpas Road

City: New Brunswick

Country: United States

State or Province: NJ

ZIP/Postal Code: 08901

Email Address: michael.santangelo@gmail.com

Organization Name: n/a

Comment: I respectfully request that the FCC take a good, long look at this before accepting it. These rules would greatly restrict and limit the ability of end users who own hardware to install, tweak, and modify their personal equipment. This is the wrong direction for technology as a whole, but especially so with regard to any sort of communications equipment.

Specific complaints include:

Wireless research depends on our ability to break down, modify, and investigate hardware and the software that runs on that hardware.

We need the ability to examine and fix security holes in our personally owned devices regardless of whether or not the manufacturer has done so. For example with cell phones, there is an exploit called Stagefright. Custom ROMs for phones like the Galaxy S4 have had the fix for the Stagefright exploit for months. I only received an update from Samsung 3 days ago. Custom ROMs for phones could conceivably be outlawed in your wording of this proposal (modular wireless radios found in cell phones).

Please, do not restrict what we can and cannot do with our own equipment in this day and age.

Thank you for your time and consideration.

I respectfully request that the FCC take a good, long look at this before accepting it. These rules would greatly restrict and limit the ability of end users who own hardware to install, tweak, and modify their personal equipment. This is the wrong direction for technology as a whole, but especially so with regard to any sort of communications equipment.

Specific complaints include:

Wireless research depends on our ability to break down, modify, and investigate hardware and the software that runs on that hardware.

We need the ability to examine and fix security holes in our personally owned devices regardless of whether or not the manufacturer has done so. For example with cell phones, there is an exploit called Stagefright. Custom ROMs for phones like the Galaxy S4 have had the fix for the Stagefright exploit for months. I only received an update from Samsung 3 days ago. Custom ROMs for phones could conceivably be outlawed in your wording of this proposal (modular wireless radios found in cell phones).

Please, do not restrict what we can and cannot do with our own equipment in this day and age.

Thank you for your time and 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: Nathan

Last Name: Johnson

Mailing Address: 1213 NE Green St

City: Lees Summit

Country: United States

State or Province: MO

ZIP/Postal Code: 64086

Email Address:

Organization Name:

Comment: Hello,

Please allow us to continue to install our own firmware on our own personal property. It is a violation of rights for the government to mandate that we free citizens must use a certain product without the ability to choose freely.

Hello,

Please allow us to continue to install our own firmware on our own personal property. It is a violation of rights for the government to mandate that we free citizens must use a certain product without the ability to choose freely.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Larson

Mailing Address: 1665 Hanover At

City: Aurora

Country: United States

State or Province: CO

ZIP/Postal Code: 80010

Email Address: larson.jessem@gmail.com

Organization Name:

Comment: Controlling the way a person uses their devices wither it be browsing facebook, playing games, creating documents, or installing different operating systems isn't right, it isn't constitutional. The government should have no say in what we do with our devices on software or hardware as long as it is not for child pornography or hacking into sysytems. Being able to pit a different OS on a router,phone, or computer is our freedom as a consumer, and a citizen of the United States of America.

Controlling the way a person uses their devices wither it be browsing facebook, playing games, creating documents, or installing different operating systems isn't right, it isn't constitutional. The government should have no say in what we do with our devices on software or hardware as long as it is not for child pornography or hacking into sysytems. Being able to pit a different OS on a router,phone, or computer is our freedom as a consumer, and a citizen of the United States of America.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Damian

Last Name: Sosnowski

Mailing Address: Zarudawie

City: Krakw

Country: Poland

State or Province: Maopolskie

ZIP/Postal Code: 30-144

Email Address: sosnowski.damian@gmail.com

Organization Name:

Comment: Accepting these changes means death to huge development communities that better devices available around the world. It's restricting people freedom to do what they choose with their devices. It will affect global community aswell since many software developers are from USA and most countries would see same restrictions because manufacturers would give them the same hardware with the same restrictions.

Accepting these changes means death to huge development communities that better devices available around the world. It's restricting people freedom to do what they choose with their devices. It will affect global community aswell since many software developers are from USA and most countries would see same restrictions because manufacturers would give them the same hardware with the same 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: Jordan

Last Name: Beacher

Mailing Address: 132 Main St

City: Parkesburg

Country: United States

State or Province: PA

ZIP/Postal Code: 19365

Email Address: null

Organization Name: null

Comment: "Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety." - Benjamin Franklin

Freedom has always been at the core of this country's belief system. Americans in general believe that their own personal freedom is worth more than the assurance that "nothing will ever be able to hurt them". When federal laws start getting passed limiting our freedoms and privacy in order to try to better protect us from terrorists or anyone wishing to do us harm, in the end limiting these freedoms and privacies only serves to further our enemies' cause. It stifles innovation and the free market, and creates an environment of dangerous false security while imposing less effective, less efficient, and generally less useful technology on the american people.

Firstly, the thinking that one would need a permit or for some reason would be unable to investigate or modify a wifi device is ridiculous. This is supposed to be a free country and we can't even take a look at the inside of a product we buy, to learn how it works or modify it to better suit our goals/intentions? What if there's a small bug/problem with the device? We would have to ship the product in, wait for them to fix it (while they're mid-recall, presumably extremely busy), and ship it back? Wait for a software/firmware update from the manufacturer? If this becomes law, Americans would not have the ability to fix security holes on their own when the manufacturer fails to do so/chooses not to. In effect, that part of the rule alone could open more security holes and cause more potential harm than not restricting our access to wifi devices.

In addition, there is a huge commerce factor, as there are secure wifi vendors and retail hotspot vendors that depend on the ability of users and companies to install the software of their choosing. This is a huge industry worth billions of dollars.

Thank you for your time and for hearing my opinion. Please don't make this rule law.

"Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety." - Benjamin Franklin

Freedom has always been at the core of this country's belief system. Americans in general believe that their own personal freedom is worth more than the assurance that "nothing will ever be able to hurt them". When federal laws start getting passed limiting our freedoms and privacy in order to try to better protect us from terrorists or anyone wishing to do us harm, in the end limiting these freedoms and privacies only serves to further our enemies' cause. It stifles innovation and the free market, and creates an environment of dangerous false security while imposing less effective, less efficient, and generally less useful technology on the american people.

Firstly, the thinking that one would need a permit or for some reason would be unable to investigate or modify a wifi device is ridiculous. This is supposed to be a free country and we can't even take a look at the inside of a product we buy, to learn how it works or modify it to better suit our goals/intentions? What if there's a small bug/problem with the device? We would have to ship the product in, wait for them to fix it (while they're mid-recall, presumably extremely busy), and ship it back? Wait for a software/firmware update from the manufacturer? If this becomes law, Americans would not have the ability to fix security holes on their own when the manufacturer fails to do so/chooses not to. In effect, that part of the rule alone could open more security holes and cause more potential harm than not restricting our access to wifi devices.

In addition, there is a huge commerce factor, as there are secure wifi vendors and retail hotspot vendors that depend on the ability of users and companies to install the software of their choosing. This is a huge industry worth billions of dollars.

Thank you for your time and for hearing my opinion. Please don't make this rule law.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Judson

Last Name: Anderson

Mailing Address: 740 E Coolidge Ave.

City: Appleton

Country: United States

State or Province: WI

ZIP/Postal Code: 54915

Email Address: andejp12

Organization Name:

Comment: Please do not take away the legal option of putting software or OS of a consumers choosing on hardware that they have purchased. This is very useful to make a piece of equipment either more secure or to learn more about networking in general. This rule only helps corporations and simply limits consumer choices.

Please do not take away the legal option of putting software or OS of a consumers choosing on hardware that they have purchased. This is very useful to make a piece of equipment either more secure or to learn more about networking in general. This rule only helps corporations and simply limits consumer choices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Noe

Last Name: Kaur

Mailing Address: PSc 78 BOX 7309

City: APO

Country: United States

State or Province: CA

ZIP/Postal Code: 96326

Email Address: noe.kaur@gmail.com

Organization Name:

Comment: If this proposal would disable my ability to use DD-WRT or Tomato, then I am VERY MUCH AGAINST it. I enjoy being able to flash my wireless routers with open firmware. I also enjoy being able to change the base OS on my PC, which I'm unsure is being attacked with this proposal as well.

Thank you for taking the time to read my comment.

If this proposal would disable my ability to use DD-WRT or Tomato, then I am VERY MUCH AGAINST it. I enjoy being able to flash my wireless routers with open firmware. I also enjoy being able to change the base OS on my PC, which I'm unsure is being attacked with this proposal as well.

Thank you for taking the time to read 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: david

Last Name: Wood

Mailing Address: 88 Belmont st

City: Watertown

Country: United States

State or Province: MA

ZIP/Postal Code: 02472

Email Address: davechuckwood@gmail.com

Organization Name:

Comment: I personally enjoy a lot of free community developed software. In most cases it is vastly superior to anything being sold. These new rules have the ability to stifle the creative forces making said software. Please remove language from this proposal which would seek to lock down or digitally sign software on personal devices and routers. These rules would negatively effect the freedom of a lot of hobbyists, tinkerers, and enthusiasts to explore their own property.

I personally enjoy a lot of free community developed software. In most cases it is vastly superior to anything being sold. These new rules have the ability to stifle the creative forces making said software. Please remove language from this proposal which would seek to lock down or digitally sign software on personal devices and routers. These rules would negatively effect the freedom of a lot of hobbyists, tinkerers, and enthusiasts to explore their own property.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: AAA

Last Name: AAA

Mailing Address: 69 Briar Crescent

City: London

Country: United Kingdom

State or Province: Northolt

ZIP/Postal Code: ub54nd

Email Address: thefaggot@gmail.com

Organization Name: null

Comment: I want my WIFI to be free and need to stop these limitations from being made. This has not been an issue for years so leave it.

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

[https://www.reddit.com/r/technology/comments/3jsiex/the\\_fcc\\_wants\\_to\\_prevent\\_you\\_from\\_installing/](https://www.reddit.com/r/technology/comments/3jsiex/the_fcc_wants_to_prevent_you_from_installing/)

I want my WIFI to be free and need to stop these limitations from being made. This has not been an issue for years so leave it.

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

[https://www.reddit.com/r/technology/comments/3jsiex/the\\_fcc\\_wants\\_to\\_prevent\\_you\\_from\\_installing/](https://www.reddit.com/r/technology/comments/3jsiex/the_fcc_wants_to_prevent_you_from_installing/)

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Ellison

Mailing Address: 5801 Nicholson Lane

City: North Bethesda

Country: United States

State or Province: MD

ZIP/Postal Code: 20852

Email Address: jtelliso@gmail.com

Organization Name:

Comment: Hi,

I respectfully ask that the FCC not enforce rules that would restrict 3rd Party firmware on Wifi devices. I would ask that they work with the 3rd Party makers to become "in code" with the FCC rules, but to not fully take them out of being able to modify Wifi 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.

Hi,

I respectfully ask that the FCC not enforce rules that would restrict 3rd Party firmware on Wifi devices. I would ask that they work with the 3rd Party makers to become "in code" with the FCC rules, but to not fully take them out of being able to modify Wifi 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: N

Last Name: Murray

Mailing Address: 136 W Filbert St

City: East Rochester

Country: United States

State or Province: NY

ZIP/Postal Code: 14445

Email Address:

Organization Name:

Comment: Any rule or regulation which prohibits consumers from modifying a device is against the public interest.

Let us stipulate after the past few decades of demonstrated security problems in devices of all classes that use software (or firmware, which is merely compiled software for flash loading) that no manufacturer is capable of releasing a product that is actually secure.

Restricting the ability of a consumer from loading new software (or firmware) on the device leads to a situation where the useful life of a new device is measured in days or minutes from purchase as the device no longer functions as intended to provide reasonable security of consumer information or network. Even if we stipulate that the manufacturers can provide a secure product for original sale, manufacturers do not, have not, and have no incentive to support each product and keep it secure until the end of its functional life.

It is therefore imperative that each and every consumer be able to update and keep secure each and every device that they have purchased - on their own terms, for as long as they see fit.

Failure to keep these devices secure (something the manufacturers have no ability or even desire to do for the length of the device's functional life) leads to security breaches which can compromise the consumer financial information, credit card information, personal information and in some cases medical information. Increasing the rate and ease at which personal security breaches occur will (already is) having a huge detrimental effect upon the economy.

I urge you instead of forbidding the consumer modification of these devices, to instead mandate that every such device have full source code made public so that these devices can be kept updated and secured by interested and technically adept consumers in a mutual support community.

Any rule or regulation which prohibits consumers from modifying a device is against the public interest.

Let us stipulate after the past few decades of demonstrated security problems in devices of all classes that use software (or firmware, which is merely compiled software for flash loading) that no manufacturer is capable of releasing a product that is actually secure.

Restricting the ability of a consumer from loading new software (or firmware) on the device leads to a situation where the useful life of a new device is measured in days or minutes from purchase as the device no longer functions as intended to provide reasonable security of consumer information or network. Even if we stipulate that the manufacturers can provide a secure product for original sale, manufacturers do not, have not, and have no incentive to support each

product and keep it secure until the end of its functional life.

It is therefore imperative that each and every consumer be able to update and keep secure each and every device that they have purchased - on their own terms, for as long as they see fit.

Failure to keep these devices secure (something the manufacturers have no ability or even desire to do for the length of the device's functional life) leads to security breaches which can compromise the consumer financial information, credit card information, personal information and in some cases medical information. Increasing the rate and ease at which personal security breaches occur will (already is) having a huge detrimental effect upon the economy.

I urge you instead of forbidding the consumer modification of these devices, to instead mandate that every such device have full source code made public so that these devices can be kept updated and secured by interested and technically adept consumers in a mutual support community.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Diljot

Last Name: Garcha

Mailing Address: 11 Wankling Court

City: Winnipeg

Country: Canada

State or Province: Manitoba

ZIP/Postal Code: R3P2P8

Email Address: diljot@garcha.com

Organization Name:

Comment: I kindly 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. Additional points of emphasis include:

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

Citizens of the world 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 Wi-Fi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure Wi-Fi vendors, retail hotspot vendors, depend on the ability of users and companies to install the software of their choosing.

Why would you infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster? I am a radio amateur myself, and this would destroy our ability to assist others during times of distress and setting up a local mesh network for communication. (My callsign: VE4DSG).

Why would you ban installation of custom firmware on your Android phone? The main feature of Android phones is the deep customization. Banning this ability would cause sales of Android devices to plummet.

Why would you discourage the development of alternative free and open source Wi-Fi firmware, like OpenWrt? Seriously why? Open source software is great, it allows many people to contribute to the project, and it allows bug fixes and new features to be added before other closed source software.

When a user builds a computer they are able to choose what software they can run on the machine. So why would you hinder this ability? Regardless of who built the computer or component.

Once again I kindly 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. This would seriously damage the computing industry, I feel like the FCC needs to reconsider, and in the future the FCC needs to pay more attention to the phrase: If it aint broke, dont fix it. Thank you for reading.

I kindly 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. Additional points of emphasis include:

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

Citizens of the world 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 Wi-Fi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure Wi-Fi vendors, retail hotspot vendors, depend on the ability of users and companies to install the software of their choosing.

Why would you infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster? I am a radio amateur myself, and this would destroy our ability to assist others during times of distress and setting up a local mesh network for communication. (My callsign: VE4DSG).

Why would you ban installation of custom firmware on your Android phone? The main feature of Android phones is the deep customization. Banning this ability would cause sales of Android devices to plummet.

Why would you discourage the development of alternative free and open source Wi-Fi firmware, like OpenWrt? Seriously why? Open source software is great, it allows many people to contribute to the project, and it allows bug fixes and new features to be added before other closed source software.

When a user builds a computer they are able to choose what software they can run on the machine. So why would you hinder this ability? Regardless of who built the computer or component.

Once again I kindly 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. This would seriously damage the computing industry, I feel like the FCC needs to reconsider, and in the future the FCC needs to pay more attention to the phrase: If it aint broke, dont fix it. Thank you for reading.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Remsen

Mailing Address: 20 High Falls Road

City: Saugerties

Country: United States

State or Province: NY

ZIP/Postal Code: 12477

Email Address: ian@ianremsen.com

Organization Name:

Comment: The free software movement and philosophy have been vital to the growth of the international technology sector, and therefore the world economy and culture since the establishment of the Free Software Foundation thirty years ago. Without these ideas, there would be a fraction of the infrastructure and foundation for developers to make new things, none of which would be as easily publicly available. Freedom of software means freedom of ideas and therefore, transparency of information.

It also means better software, and all the things listed above directly benefit from that. This is extremely important for a multitude of reasons, security being on my short list. When independent groups can stress and audit software's security implementation without being given explicit permission, and even better, being given permission at-large, we are rendered safer than could ever be attainable otherwise. This is the case for all respected encryption ciphers and security suites in general. Americans require the ability and the right to fix security vulnerabilities in their devices, when it isn't done for them, or even when it is.

Furthermore, billions (trillions?) of dollars depend on the ability and right of users and companies to install the software of their choosing, this compounds into better software.

As is in general, as is with networking device firmware, it is not fundamentally different than general purpose software, and is even more vital with our gateways to the Internet. This is a solution in search of a problem, that creates a gaping flaw in the process.

The free software movement and philosophy have been vital to the growth of the international technology sector, and therefore the world economy and culture since the establishment of the Free Software Foundation thirty years ago. Without these ideas, there would be a fraction of the infrastructure and foundation for developers to make new things, none of which would be as easily publicly available. Freedom of software means freedom of ideas and therefore, transparency of information.

It also means better software, and all the things listed above directly benefit from that. This is extremely important for a multitude of reasons, security being on my short list. When independent groups can stress and audit software's security implementation without being given explicit permission, and even better, being given permission at-large, we are rendered safer than could ever be attainable otherwise. This is the case for all respected encryption ciphers and security suites in general. Americans require the ability and the right to fix security vulnerabilities in their devices, when it isn't done for them, or even when it is.

Furthermore, billions (trillions?) of dollars depend on the ability and right of users and companies to install the software

of their choosing, this compounds into better software.

As is in general, as is with networking device firmware, it is not fundamentally different than general purpose software, and is even more vital with our gateways to the Internet. This is a solution in search of a problem, that creates a gaping flaw in the process.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Brainerd

Mailing Address: 5451 Litchfield Drive

City: Flint

Country: United States

State or Province: MI

ZIP/Postal Code: 48532

Email Address:

Organization Name:

Comment: With all due respect to the FCC mandate to patrol the frequency spectrum, I'm against the current proposal, because it appears to be too far reaching and locks users into hardware/software configurations that they cannot remove or improve upon.

The ability to use hardware with new and/or novel software is one the hallmarks of current innovation - with respect to both PCs and cell phones.

Restricting users and developers from accessing the platform(s) because of the presence of a radio device may inadvertently stop the creation of the next great Operating System (like Linux which is currently the backbone of the internet) or damage the ability of users to fix security holes or other bugs in their devices.

Billions of dollars are pouring into cellphone technology as we become ever more connected worldwide, and the ability of developers and companies to continue innovation on these devices are key components in our Information Economy.

I urge the FCC to not take up any restrictions or rules that will harm the end users ability to modify their devices (cellphones, WiFi routers and PCs) and leave only manufacturing companies with the ability to manipulate them.

With all due respect to the FCC mandate to patrol the frequency spectrum, I'm against the current proposal, because it appears to be too far reaching and locks users into hardware/software configurations that they cannot remove or improve upon.

The ability to use hardware with new and/or novel software is one the hallmarks of current innovation - with respect to both PCs and cell phones.

Restricting users and developers from accessing the platform(s) because of the presence of a radio device may inadvertently stop the creation of the next great Operating System (like Linux which is currently the backbone of the internet) or damage the ability of users to fix security holes or other bugs in their devices.

Billions of dollars are pouring into cellphone technology as we become ever more connected worldwide, and the ability of developers and companies to continue innovation on these devices are key components in our Information Economy.

I urge the FCC to not take up any restrictions or rules that will harm the end users ability to modify their devices

(cellphones, WiFi routers and PCs) and leave only manufacturing companies with the ability to manipulate them.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Rodger

Last Name: Nugent

Mailing Address: 2517 N. Main St

City: North Newton

Country: United States

State or Province: KS

ZIP/Postal Code: 67117

Email Address: Rodger.nugent@gmail.com

Organization Name:

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

-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.

Call to FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis:

-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: william

Last Name: vanskike

Mailing Address: 1205 e 22 street apt 609

City: marysville

Country: United States

State or Province: CA

ZIP/Postal Code: 95901

Email Address:

Organization Name:

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

Some points to consider via savewifi.org:

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.

Some personal points of mine:

I sincerely believe that I should legally be allowed to modify my devices in whatever ways I choose so long as they function in a legal manner (like not transmitting on frequencies reserved by the fcc for other purposes.)

To illustrate if I hypothetically bought a table should a governing party be allowed to determine what colors I could LEGALLY be allowed to paint the table or whether or not I am legally allowed to paint the table in the first place? Should the government be allowed to tell me whether I am allowed to attach wheels to my table or modify it in other non harmful ways? What if my table is too tall and thus does not suit my needs? What if my table is unsafe and my modifications make it safer?

I do not support the FCC implement rules that take away my rights to install the software of my choosing on my computing devices.

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

Some points to consider via savewifi.org:

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.

Some personal points of mine:

I sincerely believe that I should legally be allowed to modify my devices in whatever ways I choose so long as they function in a legal manner (like not transmitting on frequencies reserved by the fcc for other purposes.)

To illustrate if I hypothetically bought a table should a governing party be allowed to determine what colors I could LEGALLY be allowed to paint the table or whether or not I am legally allowed to paint the table in the first place? Should the government be allowed to tell me whether I am allowed to attach wheels to my table or modify it in other non harmful ways? What if my table is too tall and thus does not suit my needs? What if my table is unsafe and my modifications make it safer?

I do not support the FCC implement rules that take away my rights to install the software of my choosing on my computing devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Dennis

Mailing Address: 70 Lafayette Ave

City: New York

Country: United States

State or Province: NY

ZIP/Postal Code: 11238

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Gabor

Last Name: Tjong A Hung

Mailing Address: g.v.tjongahung@gmail.com

City: Paramaribo

Country: Suriname

State or Province: Paramaribo

ZIP/Postal Code: None

Email Address: g.v.tjongahung@gmail.com

Organization Name:

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

The following are some of the reasoning behind this:

- \* 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, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
- \* Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
- \* Users should be able to manipulate and control all aspects of their devices.
- \* The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
- \* These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

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

The following are some of the reasoning behind this:

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Miguel

Last Name: Esparza

Mailing Address: 130 W Grove St

City: Rialto

Country: United States

State or Province: CA

ZIP/Postal Code: 92376

Email Address: miguelme777@rocketmail.com

Organization Name:

Comment: Hi.

I believe that taking the right to install the software of our choosing on our devices will be more detrimental than beneficial. Why? Well, not only does this give us the ability to keep supporting and using older devices that manufacturers decide to stop supporting keeping them out of landfills and recycling centers, but it gives more control and security over them. This brings new life to older devices and even helps manufacturers patch bugs, security holes, and bring new features to these devices, specifically wireless routers. Manufacturers could potentially lose billions of dollars due to the fact that some of them live off of open source hardware and their devices are specifically to be used with this custom software. Many consumers, such as myself, often opt into buying this hardware because of how open it is and how quickly security holes and bugs get patched. Please hear us. Thank you

Hi.

I believe that taking the right to install the software of our choosing on our devices will be more detrimental than beneficial. Why? Well, not only does this give us the ability to keep supporting and using older devices that manufacturers decide to stop supporting keeping them out of landfills and recycling centers, but it gives more control and security over them. This brings new life to older devices and even helps manufacturers patch bugs, security holes, and bring new features to these devices, specifically wireless routers. Manufacturers could potentially lose billions of dollars due to the fact that some of them live off of open source hardware and their devices are specifically to be used with this custom software. Many consumers, such as myself, often opt into buying this hardware because of how open it is and how quickly security holes and bugs get patched. Please hear us. 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: Neal C.

Last Name: Bowie III

Mailing Address: 16548 Gala Avenue

City: Fontana

Country: United States

State or Province: CA

ZIP/Postal Code: 92337

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Public servants of the Federal Communications Commission,

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

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their

own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Young

Mailing Address: 117 Caston Ave

City: McComb

Country: United States

State or Province: MS

ZIP/Postal Code: 39648

Email Address:

Organization Name:

Comment: Start your comment by respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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

Americans need the ability to fix security holes in their devices when the manufacturer 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.

Start your comment by respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points of emphasis you should consider adding:

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

Americans need the ability to fix security holes in their devices when the manufacturer 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: Bryce

Last Name: Dombrowski

Mailing Address: 3694 Dunsmuir Way

City: Abbotsford

Country: Canada

State or Province: British Columbia

ZIP/Postal Code: v2s 6j2

Email Address:

Organization Name:

Comment: Please consider refraining from going through with these restrictions to be put on wireless devices. As a programmer it is important to be able to install whatever custom firmware I would like on my devices for learning and even for just personal preference. If the manufacturer decides not to fix security leaks, I need to be able to use custom software to fix these patches instead of relying on a non-compliant manufacturer.

I am not an american citizen, but I live in Canada right across the border so any restrictions set in place in the USA directly affects my electronic usage.

Please do not go through with this.

Please consider refraining from going through with these restrictions to be put on wireless devices. As a programmer it is important to be able to install whatever custom firmware I would like on my devices for learning and even for just personal preference. If the manufacturer decides not to fix security leaks, I need to be able to use custom software to fix these patches instead of relying on a non-compliant manufacturer.

I am not an american citizen, but I live in Canada right across the border so any restrictions set in place in the USA directly affects my electronic usage.

Please do not go through with this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Dan

Last Name: Pock

Mailing Address: 4733 Omar

City: Lansing

Country: United States

State or Province: MI

ZIP/Postal Code: 48917

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kent

Last Name: Andersen

Mailing Address: 14-1037

City: Pahoia

Country: United States

State or Province: HI

ZIP/Postal Code: 96778-0000

Email Address:

Organization Name:

Comment: This is an incredibly bad idea. Lets not stifle technology. Just say no to this.

This is an incredibly bad idea. Lets not stifle technology. Just say no to this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: William

Last Name: Norton

Mailing Address: 17033 Bainbridge Drive

City: Eden Prairie

Country: United States

State or Province: MN

ZIP/Postal Code: 55347

Email Address:

Organization Name:

Comment: I think it is absolutely preposterous, and a violation of my rights, that I should not be allowed to load whatever software I choose on hardware that I purchased with my own money. I think this extends to mobile phones, laptops, desktop computers, as well as any other electronic device I buy, including network routers. To propose a restriction on a consumer's right to do what they want to the software on the thing that they purchase is absurd. Such a restriction, as proposed, will punish unfairly the minority to whom this is important, while benefiting nobody. This benefits only companies and corporations, and restrictions the rights of ordinary citizens.

I think it is absolutely preposterous, and a violation of my rights, that I should not be allowed to load whatever software I choose on hardware that I purchased with my own money. I think this extends to mobile phones, laptops, desktop computers, as well as any other electronic device I buy, including network routers. To propose a restriction on a consumer's right to do what they want to the software on the thing that they purchase is absurd. Such a restriction, as proposed, will punish unfairly the minority to whom this is important, while benefiting nobody. This benefits only companies and corporations, and restrictions the rights of ordinary citizens.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Tyler

Last Name: Perrotto

Mailing Address: 13708 Larimore Ave

City: Omaha

Country: United States

State or Province: NE

ZIP/Postal Code: 68164

Email Address: coolonroblox@gmail.com

Organization Name:

Comment: Dear FCC,

I'm sorry, but this is not the route to take. This change will affect many people in several ways.  
It will 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.

I wish for you not to continue with this.

Dear FCC,

I'm sorry, but this is not the route to take. This change will affect many people in several ways.  
It will 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.

I wish for you not to continue with this.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Elliott

Last Name: Indiran

Mailing Address: 5338 South Woodlawn Avenue

City: Chicago

Country: United States

State or Province: IL

ZIP/Postal Code: 60615

Email Address: eindiran@uchicago.edu

Organization Name: null

Comment: I would like to respectfully ask that the FCC not write any legislation or implement any rules which would prevent or interfere with an any users ability to modify software or install software of their choosing on their computing devices. An incredible number of areas of research in academic computer science will be greatly damaged by the instantiation of such rules as it will prevent researchers from gaining access to/constructing tools and computing environments needed to complete their research. This includes vital areas such as independent driver development, OS research and tweaking, and networking research.

Under the NPRM, the operating systems run on both of my computers, as well as the firmware updates used on my (Android) phone would fall outside the rules. In the interest of continued freedom of research in computing please reconsider this plan.

I would like to respectfully ask that the FCC not write any legislation or implement any rules which would prevent or interfere with an any users ability to modify software or install software of their choosing on their computing devices. An incredible number of areas of research in academic computer science will be greatly damaged by the instantiation of such rules as it will prevent researchers from gaining access to/constructing tools and computing environments needed to complete their research. This includes vital areas such as independent driver development, OS research and tweaking, and networking research.

Under the NPRM, the operating systems run on both of my computers, as well as the firmware updates used on my (Android) phone would fall outside the rules. In the interest of continued freedom of research in computing please reconsider this plan.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Hogue

Mailing Address: 2224 Jersey Ave S

City: St Louis Park

Country: United States

State or Province: MN

ZIP/Postal Code: 55426

Email Address: dreyco676@gmail.com

Organization Name:

Comment: Please do not impose rules that will limit the choice software available for installation on computing devices.

I believe that this puts us at serious risk since all security patching would need to be performed by a manufacturer. As we all know firms can go out of business or stop supporting a product. By allowing users to install firmware of their choice they can stay secure.

Please do not impose rules that will limit the choice software available for installation on computing devices.

I believe that this puts us at serious risk since all security patching would need to be performed by a manufacturer. As we all know firms can go out of business or stop supporting a product. By allowing users to install firmware of their choice they can stay secure.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Dickason

Mailing Address: 2154 Kimberly Circle

City: Eugene

Country: United States

State or Province: OR

ZIP/Postal Code: 97405

Email Address:

Organization Name:

Comment: This proposed law would overshadow such firmwares as DD-WRT and generally restrict everyone's freedom. Please, think of the hams.

This proposed law would overshadow such firmwares as DD-WRT and generally restrict everyone's freedom. Please, think of the hams.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and 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: Winkler

Mailing Address: 6701 Miller Rd

City: Newark

Country: United States

State or Province: NY

ZIP/Postal Code: 14513

Email Address: brian.c.winkler@gmail.com

Organization Name:

Comment: I strongly disagree with the content and consequences of this regulation and urge the FCC not to adopt it in its current form.

In my capacity as a systems administrator, I have used custom open-source firmware for WiFi routers, something this regulation would disallow, to create a secure and safe public wireless network for a group of public libraries. This system allowed library patrons in rural areas to get free access to the Internet at their public library using just their library card. Without the use of custom firmware, this system would not have been possible to develop due to the prohibitively high cost of similar commercial systems.

If this regulation had been in place, the development of this system and the service to the community it provided would simply not have been possible. For reasons such as this, I feel that such a regulation is not in best interest of both our local, and the larger, community.

I strongly disagree with the content and consequences of this regulation and urge the FCC not to adopt it in its current form.

In my capacity as a systems administrator, I have used custom open-source firmware for WiFi routers, something this regulation would disallow, to create a secure and safe public wireless network for a group of public libraries. This system allowed library patrons in rural areas to get free access to the Internet at their public library using just their library card. Without the use of custom firmware, this system would not have been possible to develop due to the prohibitively high cost of similar commercial systems.

If this regulation had been in place, the development of this system and the service to the community it provided would simply not have been possible. For reasons such as this, I feel that such a regulation is not in best interest of both our local, and the larger, community.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Massimiliano

Last Name: CARNEMOLLA

Mailing Address: Via Marche, 13

City: Siracusa

Country: Italy

State or Province: SR

ZIP/Postal Code: 96100

Email Address:

Organization Name:

Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

\* manufacturers 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 wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures 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 manufacturer 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 manufactures.

Thanks for listening.

I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

\* manufacturers 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 wont be fixed for almost all of the affected devices. 3rd-party firmwares are the only safeguard against this kind of situations: manufactures 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 manufacturer 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 manufactures.

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: Michael

Last Name: Beiro

Mailing Address: 1413 Jacquelin St

City: Richmond

Country: United States

State or Province: VA

ZIP/Postal Code: 23220

Email Address: miqi95@gmail.com

Organization Name:

Comment: To whom it may concern,

This proposal would take away massive freedoms for general consumers to use and customize their own electronic devices by restricting software options to those officially sanctioned by the FCC and manufacturers. This is an unnecessary breach of freedoms, as the laws and systems in place have functioned well since the beginning of wifi networking.

I personally have found great use in software such as Linux for self-teaching computer technology and troubleshooting all kinds of computer problems and would hate to see such a wide swath of software rendered inert by poorly-thought-out legislation.

Sincerely,  
Michael Beiro

To whom it may concern,

This proposal would take away massive freedoms for general consumers to use and customize their own electronic devices by restricting software options to those officially sanctioned by the FCC and manufacturers. This is an unnecessary breach of freedoms, as the laws and systems in place have functioned well since the beginning of wifi networking.

I personally have found great use in software such as Linux for self-teaching computer technology and troubleshooting all kinds of computer problems and would hate to see such a wide swath of software rendered inert by poorly-thought-out legislation.

Sincerely,  
Michael Beiro

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Chet

Last Name: Michals

Mailing Address: 1801 N. Greenville Avenue

City: Richardson

Country: United States

State or Province: TX

ZIP/Postal Code: 75081

Email Address: chet.michals@gmail.com

Organization Name:

Comment: I just want to ask how this proposed rule change will effect end users creating new software for commercial RF devices.

How does this effect end users creating new device drivers for for open source operating system? Or end users wanting to create new firmware for a commercial Wifi Router? Would such things now be subject to getting FCC approval before they could distribute their software?

I just want to ask how this proposed rule change will effect end users creating new software for commercial RF devices.

How does this effect end users creating new device drivers for for open source operating system? Or end users wanting to create new firmware for a commercial Wifi Router? Would such things now be subject to getting FCC approval before they could distribute their software?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Chris

Last Name: Postrero

Mailing Address: 3671 Jamestown Rd

City: Fremont

Country: United States

State or Province: CA

ZIP/Postal Code: 94538

Email Address: postcg@gmail.com

Organization Name:

Comment: I am against this proposed rule. This is serves no other purpose than to prohibit the end user of a product from using it in his/her own manner. It poses no credible safety threat.

I am against this proposed rule. This is serves no other purpose than to prohibit the end user of a product from using it in his/her own manner. It poses no credible safety threat.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Benjamin

Last Name: Myers

Mailing Address: 942 Paterson Road

City: Woodville

Country: Australia

State or Province: New South Wales

ZIP/Postal Code: 2321

Email Address: bmyers.freddy926@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