Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Anon
Last Name: Adderlan
Mailing Address: 23 Ann Dr
City: Syosset
Country: United States
State or Province: NY
ZIP/Postal Code: 117911
Email Address: anon.adderlan@gmail.com
Organization Name:
Comment: We've already seen what businesses will do when they think they can get away with it: root kits by Sony, benchmark cheats by Samsung, SSL disabling adware by Lenovo, tracking software by Verizon, and routers with wifi that cannot be turned off from Cablevision are just a few examples. So if businesses are legally required to protect the code which controls the wifi radio from user modifications, you can bet they'll just protect the entire system from user modifications, both because it gives them more leverage over the customer and it's the most reliable way to meet the legal requirements of this proposal. It means not only will it be impossible to hold them accountable for things like above, but it will be a crime to fix them yourself.

This goes beyond routers too, as cellphones, laptops, and even some desktop computers now come with software programmable wifi radios. And let me tell you, nothing would make the mobile OEMs and carriers happier than a law which makes rooting or jailbreaking your device illegal. So a proposal either needs to only require lockdown of the wifi radio, or it needs to provide additional means to hold manufacturers honest and accountable, and give users the right to request 'clean' installs which are guaranteed free of extraneous tracking and control software.

We've already seen what businesses will do when they think they can get away with it: root kits by Sony, benchmark cheats by Samsung, SSL disabling adware by Lenovo, tracking software by Verizon, and routers with wifi that cannot be turned off from Cablevision are just a few examples. So if businesses are legally required to protect the code which controls the wifi radio from user modifications, you can bet they'll just protect the entire system from user modifications, both because it gives them more leverage over the customer and it's the most reliable way to meet the legal requirements of this proposal. It means not only will it be impossible to hold them accountable for things like above, but it will be a crime to fix them yourself.

This goes beyond routers too, as cellphones, laptops, and even some desktop computers now come with software programmable wifi radios. And let me tell you, nothing would make the mobile OEMs and carriers happier than a law which makes rooting or jailbreaking your device illegal. So a proposal either needs to only require lockdown of the wifi radio, or it needs to provide additional means to hold manufacturers honest and accountable, and give users the right to request 'clean' installs which are guaranteed free of extraneous tracking and control software.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Daniel
Last Name: Sokolov
Mailing Address: 91 Nelsons Landing Blvd
City: Bedford
Country: Canada
State or Province: Nova Scotia
ZIP/Postal Code: B4A 3X4
Email Address: daniel@sokolov.eu.org
Organization Name:
Comment: Dear FCC,

please go back to the drawing board on this initiative. It has substantial negative side effects and is unnecessary.

The record does not show that there is actually a problem at such a massive scale, that the drastic results of the new rules would be warranted.

On the face of it, the proposed rules do not require a complete lock-down of the entire software of devices. However, this would be the exact side-effect your new rules would have. It is much easier for manufacturers to lock down the entire device's memory than to distinguish between wireless-related drivers and other software in a safe and reliable manner.

As we have seen with many consumer devices, manufacturers quickly abandon their product lines once they have been sold. However, some may still be in use decades later.

While normal users will be unable to update or reprogram their devices, criminals will find ways to do so quickly.

On the other hand, if users start to replace devices more quickly, it will have substantial negative effects on the environment. We should work towards longer usage cycles, not shorter ones. Thanks to Linux and other free and open source software, many a old hardware has found new meaning. But for this to work, it must be easy to reprogram it.

Another important aspect is the increasing mobility of users. They take their devices form one jurisdiction to another and use it there. Most users are not intent on breaking the law. They would install localized software, if it was available, in order to follow the local rules.

But that means that is must be easy to do so. Your proposed rules aim to make it difficult, which could lead to an opposite effect.

At the end of the day, the FCC should hold the end user accountable for any violations, not the manufacturer, as long as the end user was able to follow the rules with their very device. That means the user must be able to choose the correct, localized settings.

Also, alternate software helps to establish competition in the market for various wireless device categories. Additional functions and capabilities are often introduced into the market through free and open software. And competition is good for consumers and increases welfare for all customers.

Finally, a number of small and medium business use alternative software on wireless devices for security purposes. These businesses cannot afford to order custom builds from a large manufacturer. But they strive to eliminate their attack surface. So they choose alternate software for their devices whit as little as functions as they need. That can actually increase their security level.

Under the new rules, they would often be unable to do that. And this would result in reduced IT-security.

This can not be the aim of the FCC. Please reconsider your proposal.

Thank you for your attention and consideration.

Dear FCC,

please go back to the drawing board on this initiative. It has substantial negative side effects and is unnecessary.

The record does not show that there is actually a problem at such a massive scale, that the drastic results of the new rules would be warranted.

On the face of it, the proposed rules do not require a complete lock-down of the entire software of devices. However, this would be the exact side-effect your new rules would have. It is much easier for manufacturers to lock down the entire device's memory than to distinguish between wireless-related drivers and other software in a safe and reliable manner.

As we have seen with many consumer devices, manufacturers quickly abandon their product lines once they have been sold. However, some may still be in use decades later.

While normal users will be unable to update or reprogram their devices, criminals will find ways to do so quickly.

On the other hand, if users start to replace devices more quickly, it will have substantial negative effects on the environment. We should work towards longer usage cycles, not shorter ones. Thanks to Linux and other free and open source software, many a old hardware has found new meaning. But for this to work, it must be easy to reprogram it.

Another important aspect is the increasing mobility of users. They take their devices form one jurisdiction to another and use it there. Most users are not intent on breaking the law. They would install localized software, if it was available, in order to follow the local rules.

But that means that is must be easy to do so. Your proposed rules aim to make it difficult, which could lead to an opposite effect.

At the end of the day, the FCC should hold the end user accountable for any violations, not the manufacturer, as long as the end user was able to follow the rules with their very device. That means the user must be able to choose the correct, localized settings.

Also, alternate software helps to establish competition in the market for various wireless device categories. Additional functions and capabilities are often introduced into the market through free and open software. And competition is good for consumers and increases welfare for all customers.

Finally, a number of small and medium business use alternative software on wireless devices for security purposes. These businesses cannot afford to order custom builds from a large manufacturer. But they strive to eliminate their attack surface. So they choose alternate software for their devices whit as little as functions as they

need. That can actually increase their security level.

Under the new rules, they would often be unable to do that. And this would result in reduced IT-security.

This can not be the aim of the FCC. Please reconsider your proposal.

Thank you for your attention and consideration.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Nicholas
Last Name: Fries
Mailing Address: 4747 Atherton Ave Apt 1G
City: San Jose
Country: United States
State or Province: CA
ZIP/Postal Code: 95130
Email Address: nochristrequired@gmail.com
Organization Name:
Comment: I believe that if I have purchased the device, that it is my right to have control over the firmware (to install open source firmware replacement or fix bugs in the vendor provided firmware), and that I (the consumer) should be liable for any FCC rule violations as a result of making such modifications, not the OEM.

I believe that these proposed rules will cause technology to be less secure and limit consumer choice. Also, the inability to install an opensource firmware could make it more difficult for security researchers to conduct penetration testing.

I hope the FCC considers what this means for consumers as well as businesses.

I do not support these newly proposed rules.

I believe that if I have purchased the device, that it is my right to have control over the firmware (to install open source firmware replacement or fix bugs in the vendor provided firmware), and that I (the consumer) should be liable for any FCC rule violations as a result of making such modifications, not the OEM.

I believe that these proposed rules will cause technology to be less secure and limit consumer choice. Also, the inability to install an opensource firmware could make it more difficult for security researchers to conduct penetration testing.

I hope the FCC considers what this means for consumers as well as businesses.

I do not support these newly proposed rules.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Philip
Last Name: Karn
Mailing Address: 7431 Teasdale Ave
City: San Diego
Country: United States
State or Province: CA
ZIP/Postal Code: 92122-2830
Email Address: karn@ka9q.net
Organization Name:
Comment: In the mid 1980s I wrote and open-sourced KA9Q NOS, the first widely used Internet software package. It is long obsolete now but for many people it was their first exposure to the Internet. I originally wrote it to run TCP/IP (the Internet protocols) over Part 97 amateur packet radio but soon many non-hams ran it on their home PCs to gain dialup Internet access. Companies with Internet connections ran it, first to connect their own employees and eventually on a commercial basis. Today we call them "ISPs", and who knows how much that industry is worth?

Other than my ham license, which I needed to transmit on the air, I needed no permission to do this work, which I did as a hobby. I am very proud of my role in encouraging the wider use of the Internet, and I passionately want the next generation of open source authors and hobbyists to continue contributing to the development of the Internet.

Much of this development still takes place on radio, especially in developing countries without wire infrastructure. Hams are still active, aided considerably by the availability of inexpensive commercial WiFi devices easily modified to operate on the adjacent amateur bands.

Examples include Amateur HSMM (High Speed Multi Media) and the closely related AREDN (Amateur Radio Emergency Data Network) which will provide emergency Internet services to local governments in time of disaster -- one of the fundamental reasons amateur radio exists.

WiFi technology already uses several innovations first developed in ham radio, such as the low-level "collision avoidance" mechanism that I invented and published in 1990. I am personally interested in continuing to experiment in this area.

In principle we could build everything from scratch but that's simply not within our limited means as hams. By closing off our supply of inexpensive, easily modified hardware your proposed lock-out rule would simply shut us down. Please do not do that.

Respectfully submitted,

Phil Karn
Amateur Radio callsign KA9Q
San Diego, CA

In the mid 1980s I wrote and open-sourced KA9Q NOS, the first widely used Internet software package. It is long obsolete now but for many people it was their first exposure to the Internet. I originally wrote it to run TCP/IP (the Internet protocols) over Part 97 amateur packet radio but soon many non-hams ran it on their

home PCs to gain dialup Internet access. Companies with Internet connections ran it, first to connect their own employees and eventually on a commercial basis. Today we call them "ISPs", and who knows how much that industry is worth?

Other than my ham license, which I needed to transmit on the air, I needed no permission to do this work, which I did as a hobby. I am very proud of my role in encouraging the wider use of the Internet, and I passionately want the next generation of open source authors and hobbyists to continue contributing to the development of the Internet.

Much of this development still takes place on radio, especially in developing countries without wire infrastructure. Hams are still active, aided considerably by the availability of inexpensive commercial WiFi devices easily modified to operate on the adjacent amateur bands.

Examples include Amateur HSMM (High Speed Multi Media) and the closely related AREDN (Amateur Radio Emergency Data Network) which will provide emergency Internet services to local governments in time of disaster -- one of the fundamental reasons amateur radio exists.

WiFi technology already uses several innovations first developed in ham radio, such as the low-level "collision avoidance" mechanism that I invented and published in 1990. I am personally interested in continuing to experiment in this area.

In principle we could build everything from scratch but that's simply not within our limited means as hams. By closing off our supply of inexpensive, easily modified hardware your proposed lock-out rule would simply shut us down. Please do not do that.

Respectfully submitted,

Phil Karn
Amateur Radio callsign KA9Q
San Diego, CA

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Kevin
Last Name: Peng
Mailing Address: 40 Woodford Dr
City: Moraga
Country: United States
State or Province: CA
ZIP/Postal Code: 94556
Email Address: kpengboy@fastmail.fm
Organization Name:
Comment: Hi,

I would like to present my comment on these proposed regulations.

It is of utmost importance that Americans be not forbidden from performing modifications to the software of their wireless devices. While I do agree that it's very important to make sure people are not broadcasting on arbitrary frequencies, regulations to completely lock down wireless devices against their own owners is too heavy of a blow.

Firstly, if only a small class of people is able to develop software for wireless devices, that excludes the rest of the masses. Researchers will not be able to effectively test their new software and designs on existing hardware that they can procure. How would they then perform their research? They could only try to build their own hardware, which not many research group can realistically do. America needs the innovation that such research provides.

Also, ordinary people who use wireless devices ought to have control over them. If the stock firmware that arrives with their wireless devices does not allow them to make full use of those devices, they should by all rights be able to use another firmware that will. People should not be at the mercy of a few manufacturers who may not have their best interests in mind.

Furthermore, it is not necessarily the case that a few arbitrary manufacturers can always be trusted. Under the new proposal, a user who has discovered that their router has a security hole is at the mercy of the manufacturer, who may or may not choose to fix it. A user who doesn't want bloatware or spyware on their phones won't have a choice to remove it. If manufacturers engineer firmware that secretly contravenes laws or regulations, as Volkswagen recently did, the deviant misfeatures will never be discovered except by accident.

Therefore, the proposal in its current form is not good for America. While we do need to make sure people only broadcast on approved frequencies, this way is not the right way.

Thank you for your attention.

Hi,

I would like to present my comment on these proposed regulations.

It is of utmost importance that Americans be not forbidden from performing modifications to the software of their wireless devices. While I do agree that it's very important to make sure people are not broadcasting on arbitrary frequencies, regulations to completely lock down wireless devices against their own owners is too heavy of a blow.

Firstly, if only a small class of people is able to develop software for wireless devices, that excludes the rest of the masses. Researchers will not be able to effectively test their new software and designs on existing hardware that they can procure. How would they then perform their research? They could only try to build their own hardware, which not many research group can realistically do. America needs the innovation that such research provides.

Also, ordinary people who use wireless devices ought to have control over them.

If the stock firmware that arrives with their wireless devices does not allow them to make full use of those devices, they should by all rights be able to use another firmware that will. People should not be at the mercy of a few manufacturers who may not have their best interests in mind.

Furthermore, it is not necessarily the case that a few arbitrary manufacturers can always be trusted. Under the new proposal, a user who has discovered that their router has a security hole is at the mercy of the manufacturer, who may or may not choose to fix it. A user who doesn't want bloatware or spyware on their phones won't have a choice to remove it. If manufacturers engineer firmware that secretly contravenes laws or regulations, as Volkswagen recently did, the deviant misfeatures will never be discovered except by accident.

Therefore, the proposal in its current form is not good for America. While we do need to make sure people only broadcast on approved frequencies, this way is not the right way.

Thank you for your attention.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Michael
Last Name: Siepmann
Mailing Address: PO Box 270478
City: Louisville
Country: United States
State or Province: CO
ZIP/Postal Code: 80027
Email Address: MS@TechDesignPsych.com
Organization Name: The Tech Design Psychologist
Comment: I respectfully urge the FCC to avoid implementing rules that take away the ability of users to install the software of their choosing on their computing devices. The ability for citizens to choose the software that runs on their computing devices is critical to modern democratic society. Computing devices have become essential for all forms of information exchange, discussion, and debate. If users do not have the right to install software of their choosing, citizens have no reliable way to defend their political freedoms from powers that may, at any point in time, have or gain the leverage to control the software that runs on citizen's devices in ways that compromise political freedom.

I respectfully urge the FCC to avoid implementing rules that take away the ability of users to install the software of their choosing on their computing devices. The ability for citizens to choose the software that runs on their computing devices is critical to modern democratic society. Computing devices have become essential for all forms of information exchange, discussion, and debate. If users do not have the right to install software of their choosing, citizens have no reliable way to defend their political freedoms from powers that may, at any point in time, have or gain the leverage to control the software that runs on citizen's devices in ways that compromise political freedom.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Andrew
Last Name: Cosand
Mailing Address: 286 Florence St
City: Sunnyvale
Country: United States
State or Province: CA
ZIP/Postal Code: 94086
Email Address: fedreg@cosand.org.
Organization Name:
Comment: Hello, I am writing to request that the FCC NOT implement rules that could take away the ability of users to install the software of their choosing on their computing devices. Taking control of devices away from consumers and researchers would have serious deleterious effects on security and innovation.

Hello, I am writing to request that the FCC NOT implement rules that could take away the ability of users to install the software of their choosing on their computing devices. Taking control of devices away from consumers and researchers would have serious deleterious effects on security and innovation.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Kieron
Last Name: Gillespie
Mailing Address: 500 N. McBride
City: Syracuse
Country: United States
State or Province: NY
ZIP/Postal Code: 13203
Email Address: ciaran.gillespie@gmail.com
Organization Name:
Comment: As the chief software engineer for a Wireless software development team and also an expert in information security technology, embedded RF communication, and low power protocols, and Internet of Things (IoT) technology, this is the stupidest idea I have ever heard! This would only create barriers for businesses, small startups, IT organizations, and developers who are trying to legitimately operate, support, maintain and develop wireless technologies for the commercial sector.

Also forcing all low-power RF micro-controllers and systems to have to decrypt their firmware during every execution would lead to severe penalties to power performance and processor abilities. This would halt all activity in energy harvesting technology and would destroy the entire IoT business sector.

One other fact is that there would be no way for you to fully secure a system that someone has physical access too. Bus lines can be controlled externally, the simple cryptographic systems that will be used can be broken, and also no software executing on a micro-controller is going to be perfect against external attacks so compromising a system won't just be annoying it could be permanent. Once an attacker has exploited the software running thanks to your new regulation is will be almost impossible for a company to reissue/deploy and flash new firmware as the very security mechanisms that were required by this proposal suggests to use will be used against the manufacturer and customers only way to update and repair the system. Preventing customers from having any easy method to re-flash or repair their compromised system's software would be devastating the to the security of the nation. We would see an explosion of bot netted routers and other systems that are no longer in control of anyone but hacker. Taking away control from users doesn't not equate more security, in fact it almost always makes it easier for hackers to hide and exploit.

Also go ahead and approve this if you want to destroy any chance companies in the United States have in participating in the Internet of Thing revolution and watch the rest of the world take it over. With regulations like these we will see a clear decline in the number of businesses willing to participate in this sector, and also a vast majority of the very few options of low power RF protocols and chip set will be completely invalidated require total redesigns in most cases.

In short, this is a regulation that is obviously being written and thought up by people who are not technical or in this industry. Hopefully this is just a case of good intentions gone wrong and not with motives that do not have the best interests of our nation in mind.

As the chief software engineer for a Wireless software development team and also an expert in information security technology, embedded RF communication, and low power

protocols, and Internet of Things (IoT) technology, this is the stupidest idea I have ever heard! This would only create barriers for businesses, small startups, IT organizations, and developers who are trying to legitimately operate, support, maintain and develop wireless technologies for the commercial sector.

Also forcing all low-power RF micro-controllers and systems to have to decrypt their firmware during every execution would lead to severe penalties to power performance and processor abilities. This would halt all activity in energy harvesting technology and would destroy the entire IoT business sector.

One other fact is that there would be no way for you to fully secure a system that someone has physical access too. Bus lines can be controlled externally, the simple cryptographic systems that will be used can be broken, and also no software executing on a micro-controller is going to be perfect against external attacks so compromising a system won't just be annoying it could be permanent. Once an attacker has exploited the software running thanks to your new regulation is will be almost impossible for a company to reissue/deploy and flash new firmware as the very security mechanisms that were required by this proposal suggests to use will be used against the manufacturer and customers only way to update and repair the system. Preventing customers from having any easy method to re-flash or repair their compromised system's software would be devastating the to the security of the nation. We would see an explosion of bot netted routers and other systems that are no longer in control of anyone but hacker. Taking away control from users doesn't not equate more security, in fact it almost always makes it easier for hackers to hide and exploit.

Also go ahead and approve this if you want to destroy any chance companies in the United States have in participating in the Internet of Thing revolution and watch the rest of the world take it over. With regulations like these we will see a clear decline in the number of businesses willing to participate in this sector, and also a vast majority of the very few options of low power RF protocols and chip set will be completely invalidated require total redesigns in most cases.

In short, this is a regulation that is obviously being written and thought up by people who are not technical or in this industry. Hopefully this is just a case of good intentions gone wrong and not with motives that do not have the best interests of our nation in mind.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: William
Last Name: Farrow
Mailing Address: 3417 Savan Court
City: Raleigh
Country: United States
State or Province: NC
ZIP/Postal Code: 27613
Email Address: bill-fcc@arrowsreach.com
Organization Name:
Comment: Dear FCC,
I am writing to ask the FCC not to restrict the public from developing and installing custom software onto computing and networking devices that they own.

Wifi device manufacturers are well known for not releasing updated firmware to fix security flaws, leaving consumers and businesses vulnerable. Several Open Source Software projects like OpenWRT were created to replace the vendors software, fixing bugs, providing up to date security patches, and adding features like ipv6. There are entire ecosystems of small businesses that contribute and depend on these Open Source projects and the ability to customize networking equipment.

On a personal level, I am very concerned about the damage this would have on my professional career. I am an embedded software engineer who has developed products in the industrial, medical, and aerospace fields. This FCC proposal would degrade or prevent the continued development of the tools and software that I use for my trade.

Sincerely,
William F

Dear FCC,
I am writing to ask the FCC not to restrict the public from developing and installing custom software onto computing and networking devices that they own.

Wifi device manufacturers are well known for not releasing updated firmware to fix security flaws, leaving consumers and businesses vulnerable. Several Open Source Software projects like OpenWRT were created to replace the vendors software, fixing bugs, providing up to date security patches, and adding features like ipv6. There are entire ecosystems of small businesses that contribute and depend on these Open Source projects and the ability to customize networking equipment.

On a personal level, I am very concerned about the damage this would have on my professional career. I am an embedded software engineer who has developed products in the industrial, medical, and aerospace fields. This FCC proposal would degrade or prevent the continued development of the tools and software that I use for my trade.

Sincerely,
William F

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Michael
Last Name: Schultheiss
Mailing Address: PO Box 2112
City: Indianapolis
Country: United States
State or Province: IN
ZIP/Postal Code: 46206-2112
Email Address: schultmc@servingliberty.net
Organization Name:
Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Such rules will have a negative impact on several areas of computing:

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

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

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

* Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

* Users should be free to install whichever operating system, firmware, etc. on computing equipment they own

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

Such rules will have a negative impact on several areas of computing:

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

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

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

* Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

* Users should be free to install whichever operating system, firmware, etc. on computing equipment they own

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Christoph
Last Name: Franzen
Mailing Address: Schleckheimer Strasse 100
City: Aachen
Country: Germany
State or Province: Nordrhein-Westfalen
ZIP/Postal Code: 52076
Email Address: freifunk@alte-pflasterei.de
Organization Name: member of "Freifunk Rheinland e.V."
Comment: Firmware for wireless devices should be exchangeble by the user, at least the user must have the choice to buy a device which allows this due to the following reasons (just a few examples):

* It ist not a good idea to restrict users of mobile computers with built in wireless cards to the operating system it was initially bought with. It is also not a good idea to restrict the buyer to upgrades only from this one manufacturer. Because most Laptops are sold with a current version of Microsoft Windows, it could, for instance, become illegal to install free software later.

* The economic impact would be enormous: the competition is severely restricted; vendors of additional services ans modifications are removed from the market.

* Lack of competition leads to technological inferior products in the long run.

* Security holes will remain unfixed, and as a consequence, cyber threats increased, because buyers choose to live with the problem when the manufacturer refuses to fix them (you at least won't get fixes for older devices). Alternative software cannot be installed, and the users likely won't buy a new device just for this reason, and even if so, the result would be unnecessary electronic waste.

* Wireless networking reserch depends on the ability to reprogram devices and use alternative firmwares. The development of mesh routing protocols, for example, was mostly driven by a community of volunteers up to now, not by the "large players" on the hardware manufacturing market.

Firmware for wireless devices should be exchangeble by the user, at least the user must have the choice to buy a device which allows this due to the following reasons (just a few examples):

* It ist not a good idea to restrict users of mobile computers with built in wireless cards to the operating system it was initially bought with. It is also not a good idea to restrict the buyer to upgrades only from this one manufacturer. Because most Laptops are sold with a current version of Microsoft Windows, it could, for instance, become illegal to install free software later.

* The economic impact would be enormous: the competition is severely restricted; vendors of additional services ans modifications are removed from the market.

* Lack of competition leads to technological inferior products in the long run.

* Security holes will remain unfixed, and as a consequence, cyber threats increased, because buyers choose to live with the problem when the manufacturer refuses to fix them (you at least won't get fixes for older devices). Alternative software cannot

be installed, and the users likely won't buy a new device just for this reason, and even if so, the result would be unnecessary electronic waste.

* Wireless networking reserch depends on the ability to reprogram devices and use alternative firmwares. The development of mesh routing protocols, for example, was mostly driven by a community of volunteers up to now, not by the "large players" on the hardware manufacturing market.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Bobby
Last Name: Mohan
Mailing Address: 105 Thornhill Dr.
City: Chester
Country: United States
State or Province: VA
ZIP/Postal Code: 23836
Email Address:
Organization Name:
Comment: Please do not implement a rule preventing users from installing software of their choosing onto their devices such as routers and computers. While radio interference is bad, such a restriction will not effectively minimize such interference but will prevent the following:
1) hobbyists, tinkerers, and researchers of any size from investigating and modifying their devices and sharing their knowledge

2) people from fixing bugs and security holes when the manufacturer chooses to ignore or haphazardly fix them

3) people from using devices longer and more effectively than the manufacturer expected or intended, increasing electronic waste

4) availability of suitable products for secure wifi vendors or retail hotspot vendors.

I have benefittted from using such software with faster file and data transmission and fewer bugs, extending their useful life and with better functionality far beyond what Linksys/Cisco/Belkin planned and continue to learn from the updates provided.

Please do not implement a rule preventing users from installing software of their choosing onto their devices such as routers and computers. While radio interference is bad, such a restriction will not effectively minimize such interference but will prevent the following:
1) hobbyists, tinkerers, and researchers of any size from investigating and modifying their devices and sharing their knowledge

2) people from fixing bugs and security holes when the manufacturer chooses to ignore or haphazardly fix them

3) people from using devices longer and more effectively than the manufacturer expected or intended, increasing electronic waste

4) availability of suitable products for secure wifi vendors or retail hotspot vendors.

I have benefittted from using such software with faster file and data transmission and fewer bugs, extending their useful life and with better functionality far beyond what Linksys/Cisco/Belkin planned and continue to learn from the updates provided.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Brian
Last Name: Daniels
Mailing Address: 315 Montibello Dr
City: Cary
Country: United States
State or Province: NC
ZIP/Postal Code: 27513
Email Address:
Organization Name:
Comment: I would like to request that the FCC not implement rules that would prevent the loading of alternate software or firmware on consumer electronic devices that contain a wireless radio.

So-called "custom firmwares" have many legitimate uses. In a previous role as the IT manager of a small company, I used them to provide portable VPN devices to the employees of the firm. This gave non-technical personnel a plug-n-play device that was preconfigured for our network requirements. It would have been difficult to replicate our setup with off the shelf firmware.

Custom firmware is also crucial for being able to maintain and secure devices that are often poorly updated by the original manufacturer (if at all). It allows these devices to be updated, and keeps them out of the waste stream.

The proposed regulation would have many negative impacts. Please reconsider it.

Respectfully,
Brian Daniels

I would like to request that the FCC not implement rules that would prevent the loading of alternate software or firmware on consumer electronic devices that contain a wireless radio.

So-called "custom firmwares" have many legitimate uses. In a previous role as the IT manager of a small company, I used them to provide portable VPN devices to the employees of the firm. This gave non-technical personnel a plug-n-play device that was preconfigured for our network requirements. It would have been difficult to replicate our setup with off the shelf firmware.

Custom firmware is also crucial for being able to maintain and secure devices that are often poorly updated by the original manufacturer (if at all). It allows these devices to be updated, and keeps them out of the waste stream.

The proposed regulation would have many negative impacts. Please reconsider it.

Respectfully,
Brian Daniels

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Jonathan
Last Name: Schneider
Mailing Address: 333 Fawn Valley CT
City: Lansing
Country: United States
State or Province: KS
ZIP/Postal Code: 66043
Email Address: autlycus@gmail.com
Organization Name:
Comment: To whom it may concern,

Liberty is one of the strongest, if not the chief founding principle of this great nation. In preventing users from modifying the software which operates equipment that they have purchased, it is a direct assault on that tenure of our society. Many devices which are sold, only sell because of their ability to run modified firmware. Such firmware changes not only fix major security holes, but can increase stability and even add features that the OEM may not have thought to include. Regulating what someone does with their personal equipment, in the privacy of their own home, is akin to trying to regulate their sex life, or bathroom habits. Additionally, locking the firmware would essentially be like saying that once you bought a computer, could could only use the operating system that it came with, and could not install Linux. It could also be compared to saying that you cannot replace the oil your car, only rely on your existing oil's manufacturer to try to periodically clean it until the engine seizes, at which point you would need to replace that car.

Open source firmware for wireless devices have provided a myriad of improvements in the realm of consumer wifi products. The ability to create additional networks to partition your devices, giving you granular control over wifi security without having to maintain numerous devices or spend tens of thousands on enterprise level solutions alone is a miracle compared to this technology even 10 years ago.

As a consumer of electronics, and a liberty minded voter, please consider the needs of real american citizen's and how they prefer to use their own private property before trying to regulate liberty out of existence.

To whom it may concern,

Liberty is one of the strongest, if not the chief founding principle of this great nation. In preventing users from modifying the software which operates equipment that they have purchased, it is a direct assault on that tenure of our society. Many devices which are sold, only sell because of their ability to run modified firmware. Such firmware changes not only fix major security holes, but can increase stability and even add features that the OEM may not have thought to include. Regulating what someone does with their personal equipment, in the privacy of their own home, is akin to trying to regulate their sex life, or bathroom habits. Additionally, locking the firmware would essentially be like saying that once you bought a computer, could could only use the operating system that it came with, and could not install Linux. It could also be compared to saying that you cannot replace the oil your car, only rely on your existing oil's manufacturer to try to periodically clean it until the engine seizes, at which point you would need to replace that car.

Open source firmware for wireless devices have provided a myriad of improvements in the realm of consumer wifi products. The ability to create additional networks to partition your devices, giving you granular control over wifi security without having to maintain numerous devices or spend tens of thousands on enterprise level solutions alone is a miracle compared to this technology even 10 years ago.

As a consumer of electronics, and a liberty minded voter, please consider the needs of real american citizen's and how they prefer to use their own private property before trying to regulate liberty out of existence.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Sachin
Last Name: Bhale
Mailing Address: 539 Lanyard Dr
City: Redwood City
Country: United States
State or Province: CA
ZIP/Postal Code: 94065
Email Address:
Organization Name:
Comment: FCC please do not limit my ability to install software of my choosing on my computing devices.
We also need the ability to fix security holes without having to replace devices that manufacturers refuse to provide updates for. This has happened in the past and would be banned under these new rules.

This will cause extra e-waste to be generated and cost the average user lots of money.

FCC please do not limit my ability to install software of my choosing on my computing devices.
We also need the ability to fix security holes without having to replace devices that manufacturers refuse to provide updates for. This has happened in the past and would be banned under these new rules.

This will cause extra e-waste to be generated and cost the average user lots of money.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Brian
Last Name: Hall
Mailing Address: 11330 Cressman Drive
City: Peyton
Country: United States
State or Province: CO
ZIP/Postal Code: 80831-6802
Email Address:
Organization Name:
Comment: I always and only purchase wireless routers that I can install OpenWRT or other open-source firmware on. I strongly DISAGREE with the proposed rule and OPPOSE any mandatory locking-down of consumer hardware. The proper solution to abuse is stricter monitoring of emissions, not taking away my freedom to run the fully legal, open-source software of my choice on my own hardware.

I always and only purchase wireless routers that I can install OpenWRT or other open-source firmware on. I strongly DISAGREE with the proposed rule and OPPOSE any mandatory locking-down of consumer hardware. The proper solution to abuse is stricter monitoring of emissions, not taking away my freedom to run the fully legal, open-source software of my choice on my own hardware.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Tory
Last Name: Middlebrooks
Mailing Address: 928 s 8th ave
City: tucson
Country: United States
State or Province: AZ
ZIP/Postal Code: 85701
Email Address: undeckkid@yahoo.com
Organization Name:
Comment: Please keep the current rules for allowing consumers to modify their personal equipment.
The fears put forth about the current state of development is not disruptive and it's worthless to regulate it.

Please keep the current rules for allowing consumers to modify their personal equipment.
The fears put forth about the current state of development is not disruptive and it's worthless to regulate it.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Devon
Last Name: Vitkovsky
Mailing Address: 110 Simons Road
City: Greentown
Country: United States
State or Province: PA
ZIP/Postal Code: 18426
Email Address: nofewfudtefcity@gmail.com
Organization Name:
Comment: If owning a gun is illegal, only criminals will have guns. If owning custom firmware is illegal, only criminals will run it.

Throughout decades, the responsibility of fixing errors various big-name manufacturers have left in their devices has fallen to end-users. This practice is becoming more and more prevalent today, and while I see what you're trying to do to fix issues like this, I don't think this is the way to do it. Something's going to break on a large scale, and the few eyes allowed to look at the code won't be enough to fix it in a reasonable amount of time.

If this all started because someone brought up how everyone ignores the FCC rules on replacing antennas on routers, why not just require the FCC logo to be engraved on sanctioned antennas? Bam. Easy fix.

If owning a gun is illegal, only criminals will have guns. If owning custom firmware is illegal, only criminals will run it.

Throughout decades, the responsibility of fixing errors various big-name manufacturers have left in their devices has fallen to end-users. This practice is becoming more and more prevalent today, and while I see what you're trying to do to fix issues like this, I don't think this is the way to do it. Something's going to break on a large scale, and the few eyes allowed to look at the code won't be enough to fix it in a reasonable amount of time.

If this all started because someone brought up how everyone ignores the FCC rules on replacing antennas on routers, why not just require the FCC logo to be engraved on sanctioned antennas? Bam. Easy fix.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Eamon
Last Name: Dysinger
Mailing Address: 1608 E Edison Street
City: Tucson
Country: United States
State or Province: AZ
ZIP/Postal Code: 85719
Email Address: ejdysinger@gmail.com
Organization Name:
Comment: Limiting the ability of individuals to install software of their choice on computing devices is an affront to privacy, creativity and consumer choice. The sweeping changes proposed will have an adverse and needlessly and unjustly punitive effect on law-abiding American citizens. By constraining the right to configure, you will be impeding a generation of intelligent curious minds in their exploration of code. A generation of tinkers grew up taking apart microwaves and VCRs, and the next will take apart routers and smartphones in order to understand them. We need systems like this to move our economy forward. The ability to alter wireless firmware on a device is critical to research in these areas, research that contributes billions of dollars to this economy.
Further, in light of recent revelations concerning domestic surveillance we now know that the right to privacy is under attack. Free and Open-Source software stands as a set of tools for free people to control their digital fate. It may well be the case that such paternalist surveillance is benign in nature, but it is also open to abuse. Look at the persecution of homosexuals by the FBI during Herbert Hoover's administration. It is entirely conceivable that law-abiding people would wish to keep safe their identities to protect themselves from the injustice of society at large. Limiting these tools is a blow to liberty.
I respectfully urge the chairpersons of the FCC to reconsider this potentially disastrous regulation. Yes, those who use open source systems illegally should be punished, but those who use open source firmware with benign intent should be tolerated, even encouraged. If this great nation can endure the private ownership of weaponry for the sake of liberty, then why not the private ownership of the means of communication?

Limiting the ability of individuals to install software of their choice on computing devices is an affront to privacy, creativity and consumer choice. The sweeping changes proposed will have an adverse and needlessly and unjustly punitive effect on law-abiding American citizens. By constraining the right to configure, you will be impeding a generation of intelligent curious minds in their exploration of code. A generation of tinkers grew up taking apart microwaves and VCRs, and the next will take apart routers and smartphones in order to understand them. We need systems like this to move our economy forward. The ability to alter wireless firmware on a device is critical to research in these areas, research that contributes billions of dollars to this economy.
Further, in light of recent revelations concerning domestic surveillance we now know that the right to privacy is under attack. Free and Open-Source software stands as a set of tools for free people to control their digital fate. It may well be the case that such paternalist surveillance is benign in nature, but it is also open to abuse. Look at the persecution of homosexuals by the FBI during Herbert Hoover's administration. It is entirely conceivable that law-abiding people would wish to keep safe their identities to protect themselves from the injustice of society at large. Limiting these tools is a blow to liberty.
I respectfully urge the chairpersons of the FCC to reconsider this potentially

disastrous regulation. Yes, those who use open source systems illegally should be punished, but those who use open source firmware with benign intent should be tolerated, even encouraged. If this great nation can endure the private ownership of weaponry for the sake of liberty, then why not the private ownership of the means of communication?