

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: Brendan

Last Name: Lau

Mailing Address: 504 Lawrence Street

City: Ann Arbor

Country: United States

State or Province: MI

ZIP/Postal Code: 48104

Email Address:

Organization Name:

Comment: Hello, I am a creative person who uses computers daily, if not hourly, in order to execute my artistic vision on creative projects. Most of the time, software and hardware manufacturers who produce large scale operating systems and software on hardware systems (think iphone, android) are marketing their product towards the mass public, but there are times when hacking an item (my loose definition is taking something and repurposing it to do something else) can lend additional functionality that was not originally possible. Think of all the innovations that have come from experimentation and tinkering... if this freedom is revoked, the overall creativity and ingenuity of citizens all across the united states will be severely compromised, and that is not what I want for our country, which is why I am writing. I usually don't write, normally a very neutral person, but this issue is very much a personal matter to me, so i beg of you, please reconsider this decision. And I should also forewarn you, that people will always find ways around obstacles, no matter how high they might be.

Hello, I am a creative person who uses computers daily, if not hourly, in order to execute my artistic vision on creative projects. Most of the time, software and hardware manufacturers who produce large scale operating systems and software on hardware systems (think iphone, android) are marketing their product towards the mass public, but there are times when hacking an item (my loose definition is taking something and repurposing it to do something else) can lend additional functionality that was not originally possible. Think of all the innovations that have come from experimentation and tinkering... if this freedom is revoked, the overall creativity and ingenuity of citizens all across the united states will be severely compromised, and that is not what I want for our country, which is why I am writing. I usually don't write, normally a very neutral person, but this issue is very much a personal matter to me, so i beg of you, please reconsider this decision. And I should also forewarn you, that people will always find ways around obstacles, no matter how high they might be.

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: Sean
Last Name: Connelly
Mailing Address: 12910 stillwood dr
City: Savannah
Country: United States
State or Province: GA
ZIP/Postal Code: 31419
Email Address: edgeofadrenaline@gmail.com
Organization Name:

Comment: Current technology is moving forward in leaps and bounds by IT users like me being able to program pieces of equipment to be better than they would normally be.

Arduino, raspberry pi, routers, linux, all are platforms that are being built on, or developed on. Start ups and independant developers use these to jumpstart their businesses and revolutionize the IT industry with products that would otherwise be infeasible to develop on their own.

Current technology is moving forward in leaps and bounds by IT users like me being able to program pieces of equipment to be better than they would normally be.

Arduino, raspberry pi, routers, linux, all are platforms that are being built on, or developed on. Start ups and independant developers use these to jumpstart their businesses and revolutionize the IT industry with products that would otherwise be infeasible to develop on their 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: Matthew

Last Name: Hoffman

Mailing Address: 809 W Grove Parkway

City: Tempe

Country: United States

State or Province: AZ

ZIP/Postal Code: 85283

Email Address:

Organization Name:

Comment: This rule would stifle innovation, make us less secure, and set back progress in the United States decades.

Preventing the reverse engineering and close examination of various technology is only preventing the white-hat people from using it to prevent attacks. Malicious individuals will always try to exploit devices whether it is legal or not.

This rule would stifle innovation, make us less secure, and set back progress in the United States decades.

Preventing the reverse engineering and close examination of various technology is only preventing the white-hat people from using it to prevent attacks. Malicious individuals will always try to exploit devices whether it is legal or not.

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: Faurest

Last Name: Lupine

Mailing Address: 12 rue du 11 novembre

City: Beaurains

Country: France

State or Province: Pas-de-Calais

ZIP/Postal Code: 62217

Email Address:

Organization Name:

Comment: Fucking Shit idea !

Fucking Shit idea !

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: Brad
Last Name: Williamson
Mailing Address: 3101 West Broadway Ave.
City: Hopewell
Country: United States
State or Province: VA
ZIP/Postal Code: 23860
Email Address:
Organization Name:

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

Wireless device manufacturers have a defined product life cycle and do not always support their products after those devices are still useful and sometimes even during that time. End users need the ability to be able to fix security holes, especially in these cases. Users have fixed serious bugs in wifi drivers in the past and this would be banned under the NPRM. Not fixing security holes can feed cyberthreats and could increase electronic waste.

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

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

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

Wireless device manufacturers have a defined product life cycle and do not always support their products after those devices are still useful and sometimes even during that time. End users need the ability to be able to fix security holes, especially in these cases. Users have fixed serious bugs in wifi drivers in the past and this would be banned under the NPRM. Not fixing security holes can feed cyberthreats and could increase electronic waste.

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

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

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: Jonathan-Dsir

Last Name: GUIENNET

Mailing Address: 138 Boulevard de la Douronne

City: Auriol

Country: France

State or Province: PACA

ZIP/Postal Code: 13390

Email Address:

Organization Name:

Comment: Hi there,

I think preventing wireless hardware to be updated (flashed) is REALLY not a good idea.

Most of the time software needs to be updated for security purposes, or even to allow a certain kind of flexibility, adding functionalities and such.

Furthermore, what kind of ownership is this, if we can't even modify it.

Hi there,

I think preventing wireless hardware to be updated (flashed) is REALLY not a good idea.

Most of the time software needs to be updated for security purposes, or even to allow a certain kind of flexibility, adding functionalities and such.

Furthermore, what kind of ownership is this, if we can't even modify 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: Mark

Last Name: Hanna

Mailing Address: 421 s 43rd ave

City: Yuma

Country: United States

State or Province: AZ

ZIP/Postal Code: 85364

Email Address: Ddarthman@hotmail. Com

Organization Name:

Comment: What right does anyone have to tell me what OS I can run on a PC I bought if I want to change it that is my right.

What right does anyone have to tell me what OS I can run on a PC I bought if I want to change it that is my right.

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: Mike
Last Name: Hamerly
Mailing Address: 397 Koehler Road
City: Vadnais Heights
Country: United States
State or Province: MN
ZIP/Postal Code: 55127
Email Address: mhamerly@comcast.net
Organization Name:

Comment: I know you are considering a rule to force WiFi router manufacturers to encrypt their software that will prevent users from installing their own software on these devices.

I currently do this, not to circumvent power outputs, or to violate the intent of any ruling, but rather to keep the device I have current with the latest standards, and, more importantly, to keep up with the latest security threats. Once the devices leave the manufacturer, they typically do not offer firmware upgrades and make these devices more susceptible to attacks. I also use features to prevent phishing and other malicious activity on the router.

I have set up many elderly users with these devices, and the peace of mind I and they get is immeasurable.

Please allow free enterprise and innovation to continue here in America, and do not destroy the innovative spirit that got the airwaves to where they are today.

I know you are considering a rule to force WiFi router manufacturers to encrypt their software that will prevent users from installing their own software on these devices.

I currently do this, not to circumvent power outputs, or to violate the intent of any ruling, but rather to keep the device I have current with the latest standards, and, more importantly, to keep up with the latest security threats. Once the devices leave the manufacturer, they typically do not offer firmware upgrades and make these devices more susceptible to attacks. I also use features to prevent phishing and other malicious activity on the router.

I have set up many elderly users with these devices, and the peace of mind I and they get is immeasurable.

Please allow free enterprise and innovation to continue here in America, and do not destroy the innovative spirit that got the airwaves to where they are today.

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: John

Last Name: Arce

Mailing Address: 8422 WHELAN DR

City: SAN DIEGO

Country: United States

State or Province: CA

ZIP/Postal Code: 92119

Email Address: john.arce@gmail.com

Organization Name:

Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. I bought the hardware, I should be able to run what software I want.

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

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

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

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. I bought the hardware, I should be able to run what software I want.

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

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

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

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:=====

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: Wade

Last Name: Beinbrink

Mailing Address: 146 Dunnemann avenue

City: charleston

Country: United States

State or Province: SC

ZIP/Postal Code: 29403

Email Address: beinbrinkwade@yahoo.com

Organization Name:

Comment: Do not pass this. It will be a step backward for a internet system that is almost national monopolized by Comcast and AT&T.

Do not pass this. It will be a step backward for a internet system that is almost national monopolized by Comcast and AT&T.

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: Masha
Last Name: Thomas
Mailing Address: 16340 NE 83rd St #F138
City: Redmond
Country: United States
State or Province: WA
ZIP/Postal Code: 98052
Email Address: mat008work@gmail.com
Organization Name: null
Comment: To Whom It May Concern,

I would like to add my voice to the people who are opponents of this measure, the one that will restrict the installation of alternative operating systems on your devices. Once we purchase an item, we should have the ability to put on whatever software we want on it. We should not have to be restricted from our personal choices and our freedoms. If you bought a car, and you couldn't put a different bumper on it, how would you feel? We've paid our price for the device, now we should be able to make a choice for how we use it. The FCC is established to protect the freedoms and rights of individuals, and not to protect the interests of the mass corporations that take advantage of us. Enacting this proposal would strip us of those freedoms.

Other points of interest you should consider when denying this proposal:

- 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, as a consumer, and an individual who relies on my own ability to take action with my products, I beg you to deny this proposal.

Thank you for your time and consideration.

To Whom It May Concern,

I would like to add my voice to the people who are opponents of this measure, the one that will restrict the installation of alternative operating systems on your devices. Once we purchase an item, we should have the ability to put on whatever software we want on it. We should not have to be restricted from our personal choices and our freedoms. If you bought a car, and you couldn't put a different bumper on it, how would you feel? We've paid our price for the device, now we should be able to make a choice for how we use it. The FCC is established to protect the freedoms and rights of individuals, and not to protect the interests of the mass corporations that take advantage of us. Enacting this proposal

would
strip us of those freedoms.

Other points of interest you should consider when denying this proposal:

- 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, as a consumer, and an individual who relies on my own ability to take action with my products, I beg you to deny this proposal.

Thank you for your time 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: John
Last Name: Gotti
Mailing Address: 3715 Miramar St
City: La Jolla
Country: United States
State or Province: CA
ZIP/Postal Code: 92037
Email Address:
Organization Name:

Comment: As a US Citizen, I am absolutely against the provisions in this proposal. These regulations would severely hamper innovation in the field of technology. It would prohibit users from installing secure operating systems like GNU/Linux. Individuals should have the right to manipulate their devices in the way they see fit as long as by doing so they do not infringe on the rights of others. A blanket prohibition against the use of such hardware is not proportional to the security threats cited by the US Government. Furthermore, wireless networking research depends on the ability of researchers to investigate and modify devices. No one should have to rely on manufacturers to fix security holes in their devices. There is no harm done by modifying computing devices.

As a US Citizen, I am absolutely against the provisions in this proposal. These regulations would severely hamper innovation in the field of technology. It would prohibit users from installing secure operating systems like GNU/Linux. Individuals should have the right to manipulate their devices in the way they see fit as long as by doing so they do not infringe on the rights of others. A blanket prohibition against the use of such hardware is not proportional to the security threats cited by the US Government. Furthermore, wireless networking research depends on the ability of researchers to investigate and modify devices. No one should have to rely on manufacturers to fix security holes in their devices. There is no harm done by modifying computing devices.

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: Antonio

Last Name: DeFino

Mailing Address: 607 Leighton Rd

City: Augusta

Country: United States

State or Province: ME

ZIP/Postal Code: 04330

Email Address: definotony@gmail.com

Organization Name:

Comment: Do not allow this rule to pass, it will forever ruin the way people are able to manage and modify their own property after purchase. The company has sold a product, they cannot force you to keep it exactly the same way it was when purchased. They relinquished that right, just as I cannot tell someone they can't sell a gift I give them. It's their property, they have a right to do whatever they wish.

Do not allow this rule to pass, it will forever ruin the way people are able to manage and modify their own property after purchase. The company has sold a product, they cannot force you to keep it exactly the same way it was when purchased. They relinquished that right, just as I cannot tell someone they can't sell a gift I give them. It's their property, they have a right to do whatever they wish.

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: Jon
Last Name: Frisby
Mailing Address: 1201 Funston Ave. #305
City: San Francisco
Country: United States
State or Province: CA
ZIP/Postal Code: 94122
Email Address: jfrisby@mrjoy.com
Organization Name: null

Comment: While spectrum management is vital to a vibrant commercial ecosystem, history has shown that commercial vendors -- all of whom leech off the free software community, without giving anything back -- cannot be trusted to produce products that are secure, reliable, manageable or otherwise viable. They may appear to be reasonable products to consumers, but that's only because it's so difficult for consumers to judge the reliability or -- more importantly -- the security of complicated software products.

Protestations of the industry notwithstanding, the evidence clearly shows that the only path towards a more robust and secure future requires that the free software community continue to be able to play a role. That cannot happen under the proposed regulatory guidelines.

While spectrum management is vital to a vibrant commercial ecosystem, history has shown that commercial vendors -- all of whom leech off the free software community, without giving anything back -- cannot be trusted to produce products that are secure, reliable, manageable or otherwise viable. They may appear to be reasonable products to consumers, but that's only because it's so difficult for consumers to judge the reliability or -- more importantly -- the security of complicated software products.

Protestations of the industry notwithstanding, the evidence clearly shows that the only path towards a more robust and secure future requires that the free software community continue to be able to play a role. That cannot happen under the proposed regulatory guidelines.

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: Sean
Last Name: Duffy
Mailing Address: 2314 Rugby Row
City: Madison
Country: United States
State or Province: WI
ZIP/Postal Code: 53726
Email Address: SeanCollinDuffy@gmail.com
Organization Name: null
Comment: Good afternoon,

My name is Sean Duffy, I work in tech. Please do not allow the rights of small business' to be stripped by this rule, you shall not pass. A perfect example of how this would destroy emerging technologies is that of my work for MakerBot, a tech startup from NYC. If we had not been able to modify circuit boards for our developing 3D printers, we would have never come to market, this is just fact. Any person who has an idea needs to be able to express it for the good of the country. If you want technological advancement to stagnate, this rule would be a good way to do it.

TL;DR If this rule had existed 5 years ago, you never would have heard of 3D printing.

Good afternoon,

My name is Sean Duffy, I work in tech. Please do not allow the rights of small business' to be stripped by this rule, you shall not pass. A perfect example of how this would destroy emerging technologies is that of my work for MakerBot, a tech startup from NYC. If we had not been able to modify circuit boards for our developing 3D printers, we would have never come to market, this is just fact. Any person who has an idea needs to be able to express it for the good of the country. If you want technological advancement to stagnate, this rule would be a good way to do it.

TL;DR If this rule had existed 5 years ago, you never would have heard of 3D printing.

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: Charles

Last Name: Heaton

Mailing Address: 215 N Center St

City: San Antonio

Country: United States

State or Province: TX

ZIP/Postal Code: 78202

Email Address: gbear14275@gmail.com

Organization Name: Self

Comment: As a consumer I strongly appose rules which would prevent me from doing safe modifications to devices that are my property without some third parties permission. This is an extremely anti-consumer restriction and prevents both competition and freedom of choice. I'll give a few examples:

1. I suffered significantly after I chose to purchase a Playstation 3 (because it offered me the ability to run an "other OS") and subsequently was denied this feature when Sony modified the device removing this critical functionality and refusing to compensate me for it. Furthermore they aggressively prosecuted those consumers who sought to restore this functionality through modifications with 3rd party software which effectively killed any innovation or consumer freedom to use the devices in the manner of their choosing. This has led to me refusing to purchase Sony products in the future and has also reduced my confidence that the products I buy are mine. Instead I've realized that through software controls such as Digital Restrictions Management (DRM) that I do NOT own those devices that I buy because my use and freedom to use them is restricted to only that which the original manufacturer chooses to allow.

2. I also greatly benefited from use of 3rd party software when I was able to significantly upgrade the functionality of a Linksys WRT54G I had purchased. The WRT54G was a consumer product who utilized free software and, because of consumer friendly copyleft licensing of its components, was forced to disclose its software to consumers. Consumers then were able to vastly improve the product, share these modifications and extend the useful life of their WRT54G products significantly. In fact I still own a 3rd party compatible wifi router for just this reason. Further, this release of vastly improved 3rd party software raised the quality of every consumer wifi product on the market when companies could no longer sell products competitively that did not at least match this level of functionality. In effect, the rising tide (of functionality) floated all boats. A HUGE consumer win! These products actually continue to sell on the 2nd hand market for significantly more than if this had never happened.

3. Another case of companies using FCC regulations (either appropriately or not) for anti-competitive reasons is the case of white-listing laptop WIFI cards. WIFI cards in laptops were designed to use industry standard interfaces so that they are interchangeable. This improves competition and improves consumer choice. Unfortunately, companies have been claiming that the FCC requires them to "whitelist" specific certified cards as being good and blocks laptops from being able to use any others. See this forum reference: <https://forums.lenovo.com/t5/General-Discussion/WWAN-and-wireless-card-BIOS-whitelists-Lenovo-COME-ON/td-p/952681>. This excuse by vendors MAY be legitimate but I have strong doubts that this is required. I was forced to located 3rd party BIOS images in order to install a card (with it's own FCC ID) that was compatible with my operating system (Linux). Furthermore their "compatible/certified" cards were marked up significantly in price compared to other offerings which says to me that these types of things are used for vendor lock-in, not legitimate consumer or public safety. If vendors were further required to lock down software changes then I would not have been able to do this, which would have further restricted competition and would have

further limited my effective ownership of the things that I bought.

4. Lastly, in my profession as a cyber security engineer I have witnessed the difference in the security of open/modifiable products vs closed/proprietary/"locked down" products and there is a significantly increased risk for public safety and consumer safety with closed/locked down products. As they say, locks only keep honest people honest. Open modifiable products are FAR safer as they are inspectable and fixable. Open products are safe products.

I hope that the above examples are considered during your rule making as both good and poor examples of the effects of restrictions on consumers ability to modify the products they purchase.

In closing I would urge the Commission to take careful consideration of consumers choice, freedom and protection into account with this rule making. I fully support ensuring that manufacturers carefully test their devices for proper operation and safety during the manufacturing and design process but having them "lock them down" would be the equivalent of welding the car hoods shut on cars so that people don't modify their engines.

Please don't weld shut the hoods of information technology.

As a consumer I strongly appose rules which would prevent me from doing safe modifications to devices that are my property without some third parties permission. This is an extremely anti-consumer restriction and prevents both competition and freedom of choice. I'll give a few examples:

1. I suffered significantly after I chose to purchase a Playstation 3 (because it offered me the ability to run an "other OS") and subsequently was denied this feature when Sony modified the device removing this critical functionality and refusing to compensate me for it. Furthermore they aggressively prosecuted those consumers who sought to restore this functionality through modifications with 3rd party software which effectively killed any innovation or consumer freedom to use the devices in the manner of their choosing. This has led to me refusing to purchase Sony products in the future and has also reduced my confidence that the products I buy are mine. Instead I've realized that through software controls such as Digital Restrictions Management (DRM) that I do NOT own those devices that I buy because my use and freedom to use them is restricted to only that which the original manufacturer chooses to allow.

2. I also greatly benefited from use of 3rd party software when I was able to significantly upgrade the functionality of a Linksys WRT54G I had purchased. The WRT54G was a consumer product who utilized free software and, because of consumer friendly copyleft licensing of its components, was forced to disclose its software to consumers. Consumers then were able to vastly improve the product, share these modifications and extend the useful life of their WRT54G products significantly. In fact I still own a 3rd party compatible wifi router for just this reason. Further, this release of vastly improved 3rd party software raised the quality of every consumer wifi product on the market when companies could no longer sell products competitively that did not at least match this level of functionality. In effect, the rising tide (of functionality) floated all boats. A HUGE consumer win! These products actually continue to sell on the 2nd hand market for significantly more than if this had never happened.

3. Another case of companies using FCC regulations (either appropriately or not) for anti-competitive reasons is the case of white-listing laptop WIFI cards. WIFI cards in laptops were designed to use industry standard interfaces so that they are interchangeable. This improves competition and improves consumer choice. Unfortunately, companies have been claiming that the FCC requires them to "whitelist" specific certified cards as being good and blocks laptops from being able to use any others. See this forum reference: <https://forums.lenovo.com/t5/General-Discussion/WWAN-and-wireless-card-BIOS-whitelists-Lenovo-COME-ON/td-p/952681>. This excuse by vendors MAY be legitimate but I have strong doubts that this is required. I was forced to located 3rd party BIOS images in order to install a card (with it's own FCC ID) that was compatible with my operating system (Linux). Furthermore their "compatible/certified" cards were marked up significantly in price compared to other offerings which says to me that these types of things are used for vendor lock-in, not legitimate consumer or public safety. If vendors were further required to lock down software changes then I would not have been able to do this, which would have further restricted competition and would have further limited my effective ownership of the things that I bought.

4. Lastly, in my profession as a cyber security engineer I have witnessed the difference in the security of open/modifiable products vs closed/proprietary/"locked down" products and there is a significantly increased risk for public safety and consumer safety with closed/locked down products. As they say, locks only keep honest people honest. Open modifiable products are FAR safer as they are inspectable and fixable. Open products are safe products.

I hope that the above examples are considered during your rule making as both good and poor examples of the effects of restrictions on consumers ability to modify the products they purchase.

In closing I would urge the Commission to take careful consideration of consumers choice, freedom and protection into account with this rule making. I fully support ensuring that manufacturers carefully test their devices for proper operation and safety during the manufacturing and design process but having them "lock them down" would be the equivalent of welding the car hoods shut on cars so that people don't modify their engines.

Please don't weld shut the hoods of information technology.

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: Paul
Last Name: Tousignant
Mailing Address: 426 Sommerset Drive
City: Grayslake
Country: United States
State or Province: IL
ZIP/Postal Code: 60030
Email Address: null
Organization Name: null

Comment: Given the proliferation of wireless devices, and the increasing flexibility of how those devices use spectrum through software and firmware updates, it is understandable and desirable that the FCC improve the agility and flexibility of its certification process, which originates from times when there were fewer devices entering the market and their configuration was much more static in nature.

However, I believe it is important that, as the FCC adapts its certification process, it does not create rules which allow *only* certified vendors to update their radio software/firmware, in effect creating a federally mandated ban on consumers updating their devices with third-party (often open-source) software.

Setting aside possibly contentious assertions about whether consumers should be permitted to change software on physical hardware which they have purchased, there is another sensible reason to allow consumers to update such devices. Specifically, for many consumer devices, the viable lifespan of the physical device is typically much shorter than the period of time where device vendors provide software/firmware updates.

This is increasingly critical for devices such as WiFi routers and smartphones, where security vulnerabilities are rampant, and addressing them for any device or platform is an ongoing battle. In my experience, once a device is more than a couple of years old vendors will no longer provide software/firmware updates for even the most severe, publicly-known vulnerabilities. To a point, this is understandable. Vendors constantly produce newer, better devices, and sustaining support for older devices is, after a point, impractical. However, this leaves those consumers even aware of the problem in a difficult situation.

Once a vendor stops providing updates, replacing the software/firmware of these devices with actively maintained third-party alternatives is one of the only ways to retain use of devices while attempting to address known vulnerabilities. The only other alternative is to replace the device well before its physical and electronic components are defunct, which just begins the cycle anew.

Vendors, of course, are probably quite happy for consumers to buy replacements, but I question whether consumers should, in effect, be forced to take this course when they would, barring regulatory limits, have viable, if technical, alternatives.

While end users who have the technical skills to perform such replacements on their wireless devices are a minority, I believe this capability is useful to those with the right skills, important as a way to support the existence of such skills in the broader populace, and in line with consumer expectations regarding the right to use or modify of physical devices they own. For these reasons, I would like to see this ability protected under the updated FCC rules.

Please seek a means of increasing the FCC's agility and flexibility that does not have the result of disallowing American consumers from this existing ability to update and manage devices they have purchased.

Given the proliferation of wireless devices, and the increasing flexibility of how those devices use spectrum through software and firmware updates, it is understandable and desirable that the FCC improve the agility and flexibility of its certification process, which originates from times when there were fewer devices entering the market and their configuration was much more static in nature.

However, I believe it is important that, as the FCC adapts its certification process, it does not create rules which allow *only* certified vendors to update their radio software/firmware, in effect creating a federally mandated ban on consumers updating their devices with third-party (often open-source) software.

Setting aside possibly contentious assertions about whether consumers should be permitted to change software on physical hardware which they have purchased, there is another sensible reason to allow consumers to update such devices. Specifically, for many consumer devices, the viable lifespan of the physical device is typically much shorter than the period of time where device vendors provide software/firmware updates.

This is increasingly critical for devices such as WiFi routers and smartphones, where security vulnerabilities are rampant, and addressing them for any device or platform is an ongoing battle. In my experience, once a device is more than a couple of years old vendors will no longer provide software/firmware updates for even the most severe, publicly-known vulnerabilities. To a point, this is understandable. Vendors constantly produce newer, better devices, and sustaining support for older devices is, after a point, impractical. However, this leaves those consumers even aware of the problem in a difficult situation.

Once a vendor stops providing updates, replacing the software/firmware of these devices with actively maintained third-party alternatives is one of the only ways to retain use of devices while attempting to address known vulnerabilities. The only other alternative is to replace the device well before its physical and electronic components are defunct, which just begins the cycle anew.

Vendors, of course, are probably quite happy for consumers to buy replacements, but I question whether consumers should, in effect, be forced to take this course when they would, barring regulatory limits, have viable, if technical, alternatives.

While end users who have the technical skills to perform such replacements on their wireless devices are a minority, I believe this capability is useful to those with the right skills, important as a way to support the existence of such skills in the broader populace, and in line with consumer expectations regarding the right to use or modify of physical devices they own. For these reasons, I would like to see this ability protected under the updated FCC rules.

Please seek a means of increasing the FCC's agility and flexibility that does not have the result of disallowing American consumers from this existing ability to update and manage devices they have purchased.

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: Thomas
Last Name: Sanjurjo
Mailing Address: 1010 Estatewood Dr.
City: Brandon
Country: United States
State or Province: FL
ZIP/Postal Code: 33510
Email Address:
Organization Name:

Comment: There are a myriad of ways this law will be abused to lock consumers in to products that are damaging to their privacy, economic independence, and technical ability. This legislation is poorly thought out, and needs another look from people who understand the deeper implications of shackling firmware decisions to businesses rather than consumers. What little protection that is gained from this legislation will be vastly counter balanced by a concerned citizenship being made into criminals for wanting to learn, research, and help improve technology.

The burden of regulation of the airwaves falls to the FCC, but to regulate the software interface is to over step the bounds of the purpose of the FCC, and to penalize research and non-corporate entities from experimentation which may yield vastly improved RF and WiFi components. This regulation would certainly stifle innovation, and be costly to the American consumer.

As an advocate for Free and Open Source software, this is the wrong direction to go with regulation on these issues. The better option would be to encourage firmware manufacturers to produce APIs for their firmware that are easily understood, and well scrutinized. From that, they would need to go back and work on securing those parts of their code that need to be contained, and they would benefit from the process, as would the consumers.

The recent failure of certain RF / WiFi connected devices to separate core functionality from communications pieces is not a failure of firmware, but of software and programming. It is systemic, and dependent on lazy protectionism and refusal to acknowledge and promote discovery of potential flaws from independent contractors. The way this regulation is written will just increase that laziness and strain.

There are a myriad of ways this law will be abused to lock consumers in to products that are damaging to their privacy, economic independence, and technical ability. This legislation is poorly thought out, and needs another look from people who understand the deeper implications of shackling firmware decisions to businesses rather than consumers. What little protection that is gained from this legislation will be vastly counter balanced by a concerned citizenship being made into criminals for wanting to learn, research, and help improve technology.

The burden of regulation of the airwaves falls to the FCC, but to regulate the software interface is to over step the bounds of the purpose of the FCC, and to penalize research and non-corporate entities from experimentation which may yield vastly improved RF and WiFi components. This regulation would certainly stifle innovation, and be costly to the American consumer.

As an advocate for Free and Open Source software, this is the wrong direction to go with regulation on these issues. The better option would be to encourage firmware manufacturers to produce APIs for their firmware that are easily

understood, and well scrutinized. From that, they would need to go back and work on securing those parts of their code that need to be contained, and they would benefit from the process, as would the consumers.

The recent failure of certain RF / WiFi connected devices to separate core functionality from communications pieces is not a failure of firmware, but of software and programming. It is systemic, and dependent on lazy protectionism and refusal to acknowledge and promote discovery of potential flaws from independent contractors. The way this regulation is written will just increase that laziness and strain.