Draconian standards in the name of security have the opposite of the intended effect, and are a waste of resources. One only needs to observe that attempts to control software are already in place by many companies, with little effect on the ability to prevent the installation of custom software. Most smartphones come with locked bootloaders and firmware, yet open source alternatives still exist. We should be encouraging the spread of valuable and quite frankly better alternatives to proprietary and closed software ecosystems. Without projects such as the Linux kernel and the GNU set of software the Internet as we know it would be vastly different. Manufacturers in China are starting to see the value of open source and free software, with companies such as Xiaomi embracing projects such as Cyanogen. I would hate to see our nation left behind because of stifling regulations.

Please do not criminalize and regulate such an important and vital feature of the nation as we know it.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Vyacheslav
Last Name: Subotin
Mailing Address: spam@jupeto.ru
City: Ykaterinburg
Country: Russia
State or Province: Sverdlovsk
ZIP/Postal Code: 620000
Email Address:
Organization Name:
Comment: ? ?

? ?

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: James
Last Name: Lyons
Mailing Address: 2707 Bruce Ter
City: Hollywood
Country: United States
State or Province: FL
ZIP/Postal Code: 33020
Email Address:
Organization Name:
Comment: Respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

* 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. (hello China!)

* 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.

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

* 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. (hello China!)

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Christopher
Last Name: Cote
Mailing Address: 31 Stratford Rd.
City: Natick
Country: United States
State or Province: MA
ZIP/Postal Code: 01760-1233
Email Address: mike@cotehome.com
Organization Name:
Comment: Please allow for an exemption for open source and crowd sourced modifications. I have used modified firmwares on my routers for over 10 years and not once have I violated FCC rules. There are existing rules in place for users and businesses who violate FCC rules when using a modified firmware.

Please allow for an exemption for open source and crowd sourced modifications. I have used modified firmwares on my routers for over 10 years and not once have I violated FCC rules. There are existing rules in place for users and businesses who violate FCC rules when using a modified firmware.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Dan
Last Name: Denson
Mailing Address: 15437 Cadoz Dr
City: Austin
Country: United States
State or Province: TX
ZIP/Postal Code: 78728
Email Address: pdenson@gmail.com
Organization Name:
Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install software of their choosing on their personal wireless computing devices.

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

Thank you,

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

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

Thank you,

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Michael
Last Name: Chaberski
Mailing Address: 483 Warren St #2F
City: Brooklyn
Country: United States
State or Province: NY
ZIP/Postal Code: 11217
Email Address: mchaberski@gmail.com
Organization Name:
Comment: Please do NOT prohibit people from installing custom software on devices they own.

Researchers and inventors depend upon the ability to evaluate and modify their devices. The next great technological shift, on the scale of the web in the 90s or the cell phone in the 2000s, may begin with someone with a curious mind tinkering with a device. From a different but equally important perspective, securing our devices requires the freedom to examine them in detail, a freedom the proposed rules would take away from us.

Please do NOT prohibit people from installing custom software on devices they own.

Researchers and inventors depend upon the ability to evaluate and modify their devices. The next great technological shift, on the scale of the web in the 90s or the cell phone in the 2000s, may begin with someone with a curious mind tinkering with a device. From a different but equally important perspective, securing our devices requires the freedom to examine them in detail, a freedom the proposed rules would take away from us.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Toke
Last Name: Hiland-Jrgensen
Mailing Address: Frdingshjd 12
City: Karlstad
Country: Sweden
State or Province: Vrmland
ZIP/Postal Code: 65637
Email Address: toke@toke.dk
Organization Name: null
Comment: To whom it may concern

I am writing this comment to urge the FCC not to implement regulation that will prevent users from modifying the firmware of their wireless devices.

I am a graduate student at Karlstad University in Sweden working on network research with a focus on wireless networks. In my work, having the ability to modify device firmware is of utmost importance, as this is the mechanism by which we are able to perform research with real-world hardware.

WiFi is a tremendously important technology for providing internet access to the ever increasing number of devices we surround ourselves with. And yet it has issues that need to be resolved to be able to continue to fill this role in the coming years. I believe academic research plays an important role in solving these problems, and ensuring that researches continue to have the ability to perform basic research on real-world WiFi platforms is of utmost importance. The thousands of published academic articles based on just this approach is an obvious testament to this.

Even being outside the United States, mine and other researchers' ability to perform our research is in risk of being severely hampered by the proposed regulation that would require manufacturers to lock down devices and prevent users from modifying the firmware. I therefore once again implore you to reconsider the proposed rules and ensure that users retain the ability to modify their devices.

To whom it may concern

I am writing this comment to urge the FCC not to implement regulation that will prevent users from modifying the firmware of their wireless devices.

I am a graduate student at Karlstad University in Sweden working on network research with a focus on wireless networks. In my work, having the ability to modify device firmware is of utmost importance, as this is the mechanism by which we are able to perform research with real-world hardware.

WiFi is a tremendously important technology for providing internet access to the ever increasing number of devices we surround ourselves with. And yet it has issues that need to be resolved to be able to continue to fill this role in the coming years. I believe academic research plays an important role in solving these problems, and ensuring that researches continue to have the ability to perform basic research on real-world WiFi platforms is of utmost importance.

The thousands of published academic articles based on just this approach is an obvious testament to this.

Even being outside the United States, mine and other researchers' ability to perform our research is in risk of being severely hampered by the proposed regulation that would require manufacturers to lock down devices and prevent users from modifying the firmware. I therefore once again implore you to reconsider the proposed rules and ensure that users retain the ability to modify their devices.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Raj
Last Name: Wurttemberg
Mailing Address: 5551 Clinchfield Trl.
City: Peachtree Corners
Country: United States
State or Province: GA
ZIP/Postal Code: 30092-2070
Email Address: rwurttem@gmail.com
Organization Name:
Comment: Please do not restrict the use of custom firmware on WiFi routers.

1) Many WiFi routers have security vulnerabilities from the original manufacturer. In many cases custom firmware is the only solution. Example Netgear routers. It has been six months and Netgear has not updated the firmware on the R8000 to fix its security issues.

2) The manufacturer provided firmware does not include many of the advanced features that the tech community desires. Custom firmware is the only option available to add the desired features.

Thank you for your time.

Kind regards,
Raj Wurttemberg

Please do not restrict the use of custom firmware on WiFi routers.

1) Many WiFi routers have security vulnerabilities from the original manufacturer. In many cases custom firmware is the only solution. Example Netgear routers. It has been six months and Netgear has not updated the firmware on the R8000 to fix its security issues.

2) The manufacturer provided firmware does not include many of the advanced features that the tech community desires. Custom firmware is the only option available to add the desired features.

Thank you for your time.

Kind regards,
Raj Wurttemberg

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Caio
Last Name: Machado
Mailing Address: Brazil
City: Brazil
Country: Brazil
State or Province: Brazil
ZIP/Postal Code: Iambrazil
Email Address:
Organization Name:
Comment: You should not take away users's ability to install the software they want in their hardware. This law would affect not only the USA, but also the whole world, as China won't have one standard for USA and another one for the rest.

You should not take away users's ability to install the software they want in their hardware. This law would affect not only the USA, but also the whole world, as China won't have one standard for USA and another one for the rest.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Brent
Last Name: Mehringer
Mailing Address: 11819 Bellhaven Dr.
City: Fishers
Country: United States
State or Province: IN
ZIP/Postal Code: 46038
Email Address: bmehringer@gmail.com
Organization Name:
Comment: Hello,

I would like to politely ask you, the FCC, to reconsider the proposed rule. I have been trying to think of how this rule would benefit the general population of the United States and I am unable to come up with any reasons on why we, the people, need this rule. This rules seems like it has been pushed and sponsored by corporations more so than any US citizen.

The part of this rule that bothers me the most is that this rule will make it illegal to modify property that was legally purchased. As far as I understand, purchasing an item makes you the legal owner of the item and you are allowed to do with it what you wish. Under this rule, you are allowed to purchase an item, but not change it. In my opinion, that is the equivalent of buying a car and then being told you can't modify it in any way.

Maybe I am missing the mark on this rule, but it seems like this serves no purpose. I think there are enough laws in this country that serve no purpose and we don't need to add another.

Thanks,

Brent

Hello,

I would like to politely ask you, the FCC, to reconsider the proposed rule. I have been trying to think of how this rule would benefit the general population of the United States and I am unable to come up with any reasons on why we, the people, need this rule. This rules seems like it has been pushed and sponsored by corporations more so than any US citizen.

The part of this rule that bothers me the most is that this rule will make it illegal to modify property that was legally purchased. As far as I understand, purchasing an item makes you the legal owner of the item and you are allowed to do with it what you wish. Under this rule, you are allowed to purchase an item, but not change it. In my opinion, that is the equivalent of buying a car and then being told you can't modify it in any way.

Maybe I am missing the mark on this rule, but it seems like this serves no purpose. I think there are enough laws in this country that serve no purpose and we don't need to add another.

Thanks,

Brent

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: David
Last Name: Goldberg
Mailing Address: 645 5th Ave New York
City: New York
Country: United States
State or Province: NY
ZIP/Postal Code: 10022
Email Address: ericgoldberg@mailinator.com
Organization Name: Broadcom
Comment: As an engineer active in the RF community, this is a really bad idea that will hinder innovation in the US while it will remain trivial to set up equipment that bypasses the technical restrictions that you are proposing.

As an engineer active in the RF community, this is a really bad idea that will hinder innovation in the US while it will remain trivial to set up equipment that bypasses the technical restrictions that you are proposing.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Faisal
Last Name: Shah
Mailing Address: 1414 S Dairy Ashford St.
City: Houston
Country: United States
State or Province: TX
ZIP/Postal Code: 77077
Email Address: Faisal.shah@gmail.com
Organization Name:
Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

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

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

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

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

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Claudio
Last Name: Pisa
Mailing Address: Via Portuense 1555
City: Rome
Country: Italy
State or Province: Rome
ZIP/Postal Code: 00100
Email Address:
Organization Name:
Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

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

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

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

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

Thanks for listening.

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

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

* Without the ability to modify the software running on these devices, nothing more than the very limited, more

lucrative use cases addressed by the manifacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: William
Last Name: O'Connor
Mailing Address: 8743 S Cicero Ave
City: Hometown
Country: United States
State or Province: IL
ZIP/Postal Code: 60456
Email Address:
Organization Name:
Comment: Please do NOT require device manufacturers to implement security restricting the flashing of firmware.

Please do NOT require device manufacturers to implement security restricting the flashing of firmware.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Marco
Last Name: Fichera
Mailing Address: Via Antonio Veranzio, 64
City: Roma
Country: Italy
State or Province: Lazio
ZIP/Postal Code: 00143
Email Address: emmeffe@marfi.it
Organization Name:
Comment: I ask the FCC to refrain from implementing such measures on restricting the modification of U-NII devices. It will hamper security, commerce, and innovation.

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

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

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

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

Thanks for listening.

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

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

* Without the ability to modify the software running on these devices, nothing more than the very limited, more

lucrative use cases addressed by the manifacturer would be implemented. This leaves behind advanced and/or custom scenarios which businesses could integrate on their services/products with very small costs by replacing the software.

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Vladimir
Last Name: Shapovalov
Mailing Address: vovasn@gmail.com
City: Kharkiv
Country: Ukraine
State or Province: Kharkiv
ZIP/Postal Code: 61000
Email Address:
Organization Name:
Comment: What about right of mine to upgrade devices? And right of setting up better sofware against default one?

Its not the best decision.

What about right of mine to upgrade devices? And right of setting up better sofware against default one?

Its not the best decision.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Benjamin
Last Name: Brown
Mailing Address: 308 N. Oak St.
City: Buchanan
Country: United States
State or Province: MI
ZIP/Postal Code: 49107
Email Address: ben.turbowizard@gmail.com
Organization Name: CreativePC
Comment: I Respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

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

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

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

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Lee
Last Name: Savoie
Mailing Address: 224 W Calle Cascara
City: Sahuarita
Country: United States
State or Province: AZ
ZIP/Postal Code: 85629
Email Address: lee.savoie@gmail.com
Organization Name:
Comment: I am concerned that the proposed changes to sections 2.1033(8)(e), and 2.1042(4)(i) are overly broad and will have unintended consequences while not fully achieving their goals. Specifically, the requirement that manufacturers must prevent system software from being modified by unauthorized parties will have at least the following undesired consequences:

1. Reduced security

Router manufacturers have been known to leave unpatched security vulnerabilities in devices for long periods of time, sometimes indefinitely. In cases where authorized parties do not patch security holes, or do not patch them quickly enough, end users (including government end users) will be completely unprotected, and will, in fact, be barred from taking any action to protect themselves short of acquiring a new device. This is a heavy and costly burden to place on end users, and it will necessarily result in reduced security.

2. Ineffective protections against modification

There is a long history of computer experts breaking software protections such as the protection that the FCC is considering mandating. There is no such thing as a completely secure system, and a sufficiently motivated individual will eventually find a way around any software protection that device manufacturers may implement. This will result in exactly the same situation that exists currently; despite these new rules, unauthorized parties will be able to modify firmware anyway.

3. Unnecessary restriction of freedom

I recognize that the FCC has a legitimate need to regulate wireless transmissions. It is not clear, however, that heavily regulating all software that might affect wireless transmission is necessary to achieve this goal. Hypothetically, a device with modifications by an unauthorized party could behave identically, in terms of wireless activity, to a device with no such modifications, and still run afoul of these rules. In the United States, laws and regulations should be written in a way that minimizes the impact of the rules and thus maximizes the freedom of individuals to act as they see fit. I do not believe these new rules pass that test; wireless transmissions can be regulated without preventing end users from modifying devices they own.

Recommendations:

I would suggest removing these rules. The FCC already has the authority to regulate wireless transmissions. Seeking to

also control the software that produces wireless transmissions is unnecessary, especially in cases where such transmissions fall within legal bounds. In cases where there is harmful interference, I believe a better path is to enforce the regulations that already exist, rather than impose new rules that have the deleterious consequences listed above.

I am concerned that the proposed changes to sections 2.1033(8)(e), and 2.1042(4)(i) are overly broad and will have unintended consequences while not fully achieving their goals. Specifically, the requirement that manufacturers must prevent system software from being modified by unauthorized parties will have at least the following undesired consequences:

1. Reduced security

Router manufacturers have been known to leave unpatched security vulnerabilities in devices for long periods of time, sometimes indefinitely. In cases where authorized parties do not patch security holes, or do not patch them quickly enough, end users (including government end users) will be completely unprotected, and will, in fact, be barred from taking any action to protect themselves short of acquiring a new device. This is a heavy and costly burden to place on end users, and it will necessarily result in reduced security.

2. Ineffective protections against modification

There is a long history of computer experts breaking software protections such as the protection that the FCC is considering mandating. There is no such thing as a completely secure system, and a sufficiently motivated individual will eventually find a way around any software protection that device manufacturers may implement. This will result in exactly the same situation that exists currently; despite these new rules, unauthorized parties will be able to modify firmware anyway.

3. Unnecessary restriction of freedom

I recognize that the FCC has a legitimate need to regulate wireless transmissions. It is not clear, however, that heavily regulating all software that might affect wireless transmission is necessary to achieve this goal. Hypothetically, a device with modifications by an unauthorized party could behave identically, in terms of wireless activity, to a device with no such modifications, and still run afoul of these rules. In the United States, laws and regulations should be written in a way that minimizes the impact of the rules and thus maximizes the freedom of individuals to act as they see fit. I do not believe these new rules pass that test; wireless transmissions can be regulated without preventing end users from modifying devices they own.

Recommendations:

I would suggest removing these rules. The FCC already has the authority to regulate wireless transmissions. Seeking to also control the software that produces wireless transmissions is unnecessary, especially in cases where such transmissions fall within legal bounds. In cases where there is harmful interference, I believe a better path is to enforce the regulations that already exist, rather than impose new rules that have the deleterious consequences listed above.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Ryan
Last Name: Erickson
Mailing Address: 11381 North Sampson Drive
City: Highland
Country: United States
State or Province: UT
ZIP/Postal Code: 84003
Email Address:
Organization Name:
Comment: Please do not implement rules which will keep Americans from being able to load custom firmware on their wireless devices (Cell Phones, Computers, Routers, etc.).

Being able to run custom non-manufacturer firmware is vital to:

Education: Being able to learn about programming, operating systems, wireless systems, etc. will come to a quick halt if it's not possible to install alternate software on devices.

Security: A large percentage of routers currently have vulnerable firmware. Allowing users to install their own firmware, such as OpenWRT or other firmware lets them have 'current' security, even with hardware that may be out of date and unsupported by the manufacturer anymore.

Commerce: Many companies rely on purchasing consumer wireless gear, and installing a firmware that is more secure, or more appropriate for their use. Restricting this usage of the gear will decrease income of those companies, and any that use those technologies.

Thank you.

Please do not implement rules which will keep Americans from being able to load custom firmware on their wireless devices (Cell Phones, Computers, Routers, etc.).

Being able to run custom non-manufacturer firmware is vital to:

Education: Being able to learn about programming, operating systems, wireless systems, etc. will come to a quick halt if it's not possible to install alternate software on devices.

Security: A large percentage of routers currently have vulnerable firmware. Allowing users to install their own firmware, such as OpenWRT or other firmware lets them have 'current' security, even with hardware that may be out of date and unsupported by the manufacturer anymore.

Commerce: Many companies rely on purchasing consumer wireless gear, and installing a firmware that is more secure, or more appropriate for their use. Restricting this usage of the gear will decrease income of those companies, and any that use those technologies.

Thank you.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: John
Last Name: Brownlee
Mailing Address: 1309 Merchant Street
City: Emporia
Country: United States
State or Province: KS
ZIP/Postal Code: 66801
Email Address:
Organization Name:
Comment: This rule stifles innovation.

This rule stifles innovation.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Saurabh
Last Name: Gupta
Mailing Address: 2151 nectarine drive
City: Santa rosa
Country: United States
State or Province: CA
ZIP/Postal Code: 95404
Email Address:
Organization Name:
Comment: Please understand that the proposed change to enforce the non-changeability of software/firmware in devices sporting a radio interface will be exceedingly disastrous for the security standards that these devices enjoy presently. Primarily owing to the quality of alternate software available and it acting as the yardstick by which original-manifacturers software is measured. The proposed rule will immediately put an end to this mass community effort to empower itself with better alternatives for the good of all. Not to mention the economic, monitory and competition as well as innovation stifeling ramifications of it.
I am a security expert and researcher who specialises in embedded hardware.
I can not begin to document here the huge discrepancy in the number of exploitable flaws that product manufacturers who enforce a closed firmware unwittingly leave in their embedded radio enabled devices vs the manufacturers who embrace an open software and firmware.
Even worse the setback to the general public who, today more than ever, has a fallback option and means to switch the software to a well known, open and peer reviewed, and therefore safer, version on their devices and thus save themselves from vulnerabilities that a hacker or a malicious entity can and will exploit which the equipment manufacturer is either too slow or unable or unwilling to fix in a timely manner, will be absolutely immense.
People have the right to empower themselves to thwart the attacks on their safety both in physical and digital realms, please don't undermine that.

Please understand that the proposed change to enforce the non-changeability of software/firmware in devices sporting a radio interface will be exceedingly disastrous for the security standards that these devices enjoy presently. Primarily owing to the quality of alternate software available and it acting as the yardstick by which original-manifacturers software is measured. The proposed rule will immediately put an end to this mass community effort to empower itself with better alternatives for the good of all. Not to mention the economic, monitory and competition as well as innovation stifeling ramifications of it.
I am a security expert and researcher who specialises in embedded hardware.
I can not begin to document here the huge discrepancy in the number of exploitable flaws that product manufacturers who enforce a closed firmware unwittingly leave in their embedded radio enabled devices vs the manufacturers who embrace an open software and firmware.
Even worse the setback to the general public who, today more than ever, has a fallback option and means to switch the software to a well known, open and peer reviewed, and therefore safer, version on their devices and thus save themselves from vulnerabilities that a hacker or a malicious entity can and will exploit which the equipment manufacturer is either too slow or unable or unwilling to fix in a timely manner, will be absolutely immense.
People have the right to empower themselves to thwart the attacks on their safety both in physical and digital realms, please don't undermine that.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Chris
Last Name: Smith
Mailing Address: 2343 NW Pettygrove St
City: Portland
Country: United States
State or Province: OR
ZIP/Postal Code: 97210
Email Address: chris@chrissmith.us
Organization Name:
Comment: Please preserve the opportunity for Open Source WiFi router software.

Please preserve the opportunity for Open Source WiFi router software.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: James
Last Name: Healzer
Mailing Address: 700 Lawrence Expwy
City: Santa Clara
Country: United States
State or Province: CA
ZIP/Postal Code: 95051
Email Address:
Organization Name:
Comment: I respectfully ask that this rule not be adopted, as it restricts many legitimate activities:

The rule prevents device owners from fixing their device in a case where the device is transmitting in an illegal manner. Since they are liable for operating a device that is violating the law, their only choice to is to stop using the device.
The rule prevents security fixes if a router is found to be insecure. This could manifest itself through intentionally created backdoors used for industrial and national espionage.
Firmware from manufacturers is often full of holes. Security experts recommend installing third-party firmware.
A manufacturer isn't required to provide fixes to the user even if the device is found to be insecure or operating outside of authorization
Manufacturers will often not patch routers with serious security holes.
Prevents companies from buying US routers and reflashing with custom firmware to then sell or rent to an end user, a somewhat common occurrence.
Discourages innovation and research in the US in wireless technologies, such as mesh networking

I respectfully ask that this rule not be adopted, as it restricts many legitimate activities:

The rule prevents device owners from fixing their device in a case where the device is transmitting in an illegal manner. Since they are liable for operating a device that is violating the law, their only choice to is to stop using the device.
The rule prevents security fixes if a router is found to be insecure. This could manifest itself through intentionally created backdoors used for industrial and national espionage.
Firmware from manufacturers is often full of holes. Security experts recommend installing third-party firmware.
A manufacturer isn't required to provide fixes to the user even if the device is found to be insecure or operating outside of authorization
Manufacturers will often not patch routers with serious security holes.
Prevents companies from buying US routers and reflashing with custom firmware to then sell or rent to an end user, a somewhat common occurrence.
Discourages innovation and research in the US in wireless technologies, such as mesh networking

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: R
Last Name: A
Mailing Address: PO BOX 6444
City: Columbia
Country: United States
State or Province: MD
ZIP/Postal Code: 21045
Email Address:
Organization Name:
Comment: Hello,
Wholesale firmware flashing restrictions would go against the American capitol of innovation. The ability to exchange parts of software is similar to owning a car and being able to change the brand of tires, or engine components.
If the intent is for security, firmware security on wireless routers is ineffective to secure systems. Non-standard home routers are more secure than device operating systems, and often patch the numerous security issues, and allowing more control and monitoring of those services.
Overall, wireless security is a concern for the world we live in, but restricting firmware on wireless will do nothing to further security or safety of our information.

Hello,
Wholesale firmware flashing restrictions would go against the American capitol of innovation. The ability to exchange parts of software is similar to owning a car and being able to change the brand of tires, or engine components.
If the intent is for security, firmware security on wireless routers is ineffective to secure systems. Non-standard home routers are more secure than device operating systems, and often patch the numerous security issues, and allowing more control and monitoring of those services.
Overall, wireless security is a concern for the world we live in, but restricting firmware on wireless will do nothing to further security or safety of our information.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Carl
Last Name: Conant
Mailing Address: 3207 NE 57TH TERRACE
City: GLADSTONE
Country: United States
State or Province: MO
ZIP/Postal Code: 64119
Email Address:
Organization Name:
Comment: Please do NOT require device manufacturers to implement security restricting the flashing of firmware. This type of thing will fundamentally break the users freedom to use alternate software on devices they own, and is a massive attack on US citizens freedoms.

Please do NOT require device manufacturers to implement security restricting the flashing of firmware. This type of thing will fundamentally break the users freedom to use alternate software on devices they own, and is a massive attack on US citizens freedoms.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Suren
Last Name: Ter-Saakov
Mailing Address: 12 callison ln.
City: Voorhees
Country: United States
State or Province: NJ
ZIP/Postal Code: 08043
Email Address: tersuren@gmail.com
Organization Name:
Comment: Limits are too strict. Paragraph 33 "Changes in certified equipment" is not good. WiFi radio module cannot do any bad. However, the suggested text forbids all changes. This is not good.

Limits are too strict. Paragraph 33 "Changes in certified equipment" is not good. WiFi radio module cannot do any bad. However, the suggested text forbids all changes. This is not good.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Joshua
Last Name: Franklin
Mailing Address: 12844 N Paradise Village Pkwy W #221
City: Phoenix
Country: United States
State or Province: AZ
ZIP/Postal Code: 85032
Email Address: joshua.a.franklin@gmail.com
Organization Name:
Comment: As an IT security professional this is a horrible idea, leaving home users at the mercy of router manufacturers on when and IF they get around to patching known security holes, along with limiting them to whatever features the manufacturer decides to implement in hardware you have paid for, leads to a bad hack prone network ecosystem.

As an IT security professional this is a horrible idea, leaving home users at the mercy of router manufacturers on when and IF they get around to patching known security holes, along with limiting them to whatever features the manufacturer decides to implement in hardware you have paid for, leads to a bad hack prone network ecosystem.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Jed
Last Name: Fonner
Mailing Address: 7516 Fisher Drive
City: Falls Church
Country: United States
State or Province: VA
ZIP/Postal Code: 22043
Email Address: fcc@jedfonner.com
Organization Name:
Comment: As an avid and completely law abiding user of technology, I am pleading with you to not take away the ability of users to install software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. Most importantly, user should have freedom and choice when it comes to the software they want to run on their own devices. Isn't that what America is all about?

As an avid and completely law abiding user of technology, I am pleading with you to not take away the ability of users to install software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. Most importantly, user should have freedom and choice when it comes to the software they want to run on their own devices. Isn't that what America is all about?

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Urias
Last Name: McCullough
Mailing Address: 14015 Live Oak Lane
City: Grass Valley
Country: United States
State or Province: CA
ZIP/Postal Code: 95945
Email Address: umccullough@gmail.com
Organization Name:
Comment: I urge you to not implement any rules that prevent me from reflashing my wireless devices with custom firmware. As a consumer, I am able to obtain end-of-life wireless networking hardware that is no longer supported and update it with custom 3rd party firmware (dd-wrt, openwrt, Tomato, etc) that brings new features and new life to hardware that would otherwise end up in a landfill. This is of great benefit to myself and my friends. It is also of great benefit to our environment as the useful life of these devices can be extended indefinitely. I have at least 7 or 8 devices running custom firmware in my possession. These allow me to create very useful wireless networks for my needs as I work from home in a location without physical network wiring.

Furthermore, by allowing the ability to update devices with custom firmware, I feel like I have full control over the security and functionality of my device beyond what the original manufacturer is willing to provide or support. I feel that I can actually trust my hardware to do what it is supposed to do, and feel like I have specific control over its functionality. As an owner of physical goods, it is also my right to modify them as I see fit. In many cases, the devices I own have been discovered to have major security holes that allows attackers to use them to infiltrate private networks, or use the devices to attack other internet services through distributed attacks with many thousands of vulnerable devices. In every case, the devices that I own which are reprogrammed with custom firmware do not exhibit the same vulnerabilities.

There are some vendors that provide specific support for custom firmware (I own at least 4 such devices). This is a great selling point and feature, and I specifically look for devices with this feature. By removing this ability, you will essentially be removing a very important selling feature and thus reducing the value of these products to a segment of the consumer market.

As a major advocate for open source and the ability to understand and modify critical infrastructure software that controls my daily life, I would be very upset if this was to no longer be possible. It means I would have to locate devices that are not FCC authorized and this would very likely put me in legal jeopardy. I would be forced to import devices manufactured and sold outside the U.S.

If anything, I think the opposite should be ordained by the FCC - manufacturers should be forced to allow their product software to be updated and repaired/replaced without locks and artificial limitations placed on them. This would allow consumers to take control of their infrastructure and secure their networks more effectively.

I urge you to not implement any rules that prevent me from reflashing my wireless devices with custom firmware. As a consumer, I am able to obtain end-of-life wireless networking hardware that is no longer supported and update it with custom 3rd party firmware (dd-wrt, openwrt, Tomato, etc) that brings new features and new life to hardware that would

otherwise end up in a landfill. This is of great benefit to myself and my friends. It is also of great benefit to our environment as the useful life of these devices can be extended indefinitely. I have at least 7 or 8 devices running custom firmware in my possession. These allow me to create very useful wireless networks for my needs as I work from home in a location without physical network wiring.

Furthermore, by allowing the ability to update devices with custom firmware, I feel like I have full control over the security and functionality of my device beyond what the original manufacturer is willing to provide or support. I feel that I can actually trust my hardware to do what it is supposed to do, and feel like I have specific control over its functionality. As an owner of physical goods, it is also my right to modify them as I see fit. In many cases, the devices I own have been discovered to have major security holes that allows attackers to use them to infiltrate private networks, or use the devices to attack other internet services through distributed attacks with many thousands of vulnerable devices. In every case, the devices that I own which are reprogrammed with custom firmware do not exhibit the same vulnerabilities.

There are some vendors that provide specific support for custom firmware (I own at least 4 such devices). This is a great selling point and feature, and I specifically look for devices with this feature. By removing this ability, you will essentially be removing a very important selling feature and thus reducing the value of these products to a segment of the consumer market.

As a major advocate for open source and the ability to understand and modify critical infrastructure software that controls my daily life, I would be very upset if this was to no longer be possible. It means I would have to locate devices that are not FCC authorized and this would very likely put me in legal jeopardy. I would be forced to import devices manufactured and sold outside the U.S.

If anything, I think the opposite should be ordained by the FCC - manufacturers should be forced to allow their product software to be updated and repaired/replaced without locks and artificial limitations placed on them. This would allow consumers to take control of their infrastructure and secure their networks more effectively.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Robert
Last Name: Larkin
Mailing Address: 40 Central Ave
City: Dalton
Country: United States
State or Province: MA
ZIP/Postal Code: 01226
Email Address:
Organization Name:
Comment: To whom it may concern.

I have recently come across this proposed legislation and I have a few concerns with it. The general impression that I have from this proposal is that it effectively bans changing or modifying the firmware and/or operating system from it's stock form on wireless device. Specifically, Wi-Fi and phone devices.

I would compare this to telling a home owner that they couldn't make changes or improvements to their home or a car owner that they couldn't make repairs/improvements to their vehicle they currently own.

Why would a person want to improve, change, or perform repairs on their home or vehicle? There may be several reasons for this, to me the biggest reason is to keep the home/vehicle in good efficient operating condition so they don't have to buy a new home/vehicle.

To bring this analogy to a wireless device (smart phone, wireless router, etc.), why would someone want to install a different firmware/OS on a wireless device? Because it adds more features and keeps the device system current after it is abandoned as end-of-life from the OEM so they don't have to buy a new one.

To me, the bottom line is the cost to the consumer. I personally keep all equipment in proper operating condition to insure my investment is said equipment is maximized. If I understand the proposed legislation correctly and I am unable to update my equipment with non-OEM firmware, this will force me to purchase new equipment in lieu of continuing to operate older functioning equipment when it reaches end-of-life or experience a risk in the integrity of my family's electronic and data security.

If I am interpreting this correctly, this legislation only benefits Big Business and not the consumer whom the FCC is supposed to protect.

Thank you for your consideration in this matter.

To whom it may concern.

I have recently come across this proposed legislation and I have a few concerns with it. The general impression that I have from this proposal is that it effectively bans changing or modifying the firmware and/or operating system from it's stock form on wireless device. Specifically, Wi-Fi and phone devices.

I would compare this to telling a home owner that they couldn't make changes or improvements to their home or a car owner that they couldn't make repairs/improvements to their vehicle they currently own.

Why would a person want to improve, change, or perform repairs on their home or vehicle? There may be several reasons for this, to me the biggest reason is to keep the home/vehicle in good efficient operating condition so they don't have to buy a new home/vehicle.

To bring this analogy to a wireless device (smart phone, wireless router, etc.), why would someone want to install a different firmware/OS on a wireless device? Because it adds more features and keeps the device system current after it is abandoned as end-of-life from the OEM so they don't have to buy a new one.

To me, the bottom line is the cost to the consumer. I personally keep all equipment in proper operating condition to insure my investment is said equipment is maximized. If I understand the proposed legislation correctly and I am unable to update my equipment with non-OEM firmware, this will force me to purchase new equipment in lieu of continuing to operate older functioning equipment when it reaches end-of-life or experience a risk in the integrity of my family's electronic and data security.

If I am interpreting this correctly, this legislation only benefits Big Business and not the consumer whom the FCC is supposed to protect.

Thank you for your consideration in this matter.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Da
Last Name: Ch
Mailing Address: 1234 Private Lane
City: Corporate
Country: United States
State or Province: CA
ZIP/Postal Code: 92345-4567
Email Address:
Organization Name:
Comment: The new rules effectively ban the installation of proven Open Source firmware on any WiFi router.

The new rules effectively ban the installation of proven Open Source firmware on any WiFi router.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Tom
Last Name: Neville
Mailing Address: 12025 Gray Eagle Drive
City: Fishers
Country: United States
State or Province: IN
ZIP/Postal Code: 46037
Email Address: tomn-fccwifi@sneaky.net
Organization Name: None
Comment: I am strongly against restricting users abilities to replace the firmware on their own equipment. I have several routers which use non-vendor developed firmware. These other firmwares provide additional features and security fixes that the original vendor is unwilling to provide. There is no financial benefit to them to release updated firmware, they would rather sell you a new router.

This will also result in additional e-waste going into landfills because the vendor won't update the firmware so the device becomes useless. (Yes, useless due to unpatched security flaws.)

For instance, how many router vendors patched their old routers against heartbleed and other recently released security issues. Again, there's no financial benefit to do so. In fact, there's incentive NOT to patch their firmware as they sell more routers and other devices.

This applies equally to mobile phones and laptop computers. In this specific situation, I purchased an HSPA WWAN card for my current laptop. Even though the laptop was designed to accept this card and others are using them with no problems (after modifying their firmware) I was unable to use this card. Dell/Ericsson has NO incentive to fix this - they want to sell you a NEW card.

To me, if the FCC approves this, it is doing a HUGE disservice to consumers of electronics and radio equipment. You are putting us at mercy of device manufacturers who won't update their software as needed. You are removing our ability to fix our own devices. You will be costing the consumers you're supposed to protect.

I am strongly against restricting users abilities to replace the firmware on their own equipment. I have several routers which use non-vendor developed firmware. These other firmwares provide additional features and security fixes that the original vendor is unwilling to provide. There is no financial benefit to them to release updated firmware, they would rather sell you a new router.

This will also result in additional e-waste going into landfills because the vendor won't update the firmware so the device becomes useless. (Yes, useless due to unpatched security flaws.)

For instance, how many router vendors patched their old routers against heartbleed and other recently released security issues. Again, there's no financial benefit to do so. In fact, there's incentive NOT to patch their firmware as they sell more routers and other devices.

This applies equally to mobile phones and laptop computers. In this specific situation, I purchased an HSPA WWAN card for my current laptop. Even though the laptop was designed to accept this card and others are using them with no problems (after modifying their firmware) I was unable to use this card. Dell/Ericsson has NO incentive to fix this - they want to sell you a NEW card.

To me, if the FCC approves this, it is doing a HUGE disservice to consumers of electronics and radio equipment. You are putting us at mercy of device manufacturers who won't update their software as needed. You are removing our ability to fix our own devices. You will be costing the consumers you're supposed to protect.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Harrison
Last Name: Metzger
Mailing Address: 2125 W Potomac Ave Apt 2
City: Chicago
Country: United States
State or Province: IL
ZIP/Postal Code: 60622
Email Address: harrisonmetz@gmail.com
Organization Name:
Comment: Don't lock down devices so we can't tinker. The freedom to tinker and innovate is what makes this country great. As long as people are doing nothing illegal with radios, it shouldn't matter what firmware it runs. This is a huge step backwards for the FCC which passed net neutrality.

Don't lock down devices so we can't tinker. The freedom to tinker and innovate is what makes this country great. As long as people are doing nothing illegal with radios, it shouldn't matter what firmware it runs. This is a huge step backwards for the FCC which passed net neutrality.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Paul
Last Name: Wyatt
Mailing Address: 6520 Roswell Rd Unit 99
City: Atlanta
Country: United States Minor Outlying Islands
State or Province: GA
ZIP/Postal Code: 30328
Email Address:
Organization Name:
Comment: Dear FCC,

From my point of view you should be doing the exact opposite. It should be illegal for OEMs and ISPs to lock down devices they sell to consumers. The fact that my phone's bootloader is locked, preventing me from updating my phone's OS with security patches, is asinine. You should be suing and fining the companies that do this because it's entirely anti-consumer.

This would more than likely restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc. And also prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes.
Moreover it will ban installation of custom firmware on your Android phone and surely discourage the development of alternative free and open source WiFi firmware, like OpenWrt.

Imagine in case of disaster it will infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel.

It's not only Anti-Consumer but also prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

Sincerely

Paul

Dear FCC,

From my point of view you should be doing the exact opposite. It should be illegal for OEMs and ISPs to lock down devices they sell to consumers. The fact that my phone's bootloader is locked, preventing me from updating my phone's OS with security patches, is asinine. You should be suing and fining the companies that do this because it's entirely anti-consumer.

This would more than likely restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc. And also prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes.
Moreover it will ban installation of custom firmware on your Android phone and surely discourage the development of

alternative free and open source WiFi firmware, like OpenWrt.

Imagine in case of disaster it will infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel.

It's not only Anti-Consumer but also prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

Sincerely

Paul

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Adam
Last Name: Evans
Mailing Address: 4308 S Abby Court
City: Taylorsville
Country: United States
State or Province: UT
ZIP/Postal Code: 84123
Email Address: arthurfelter@gmail.com
Organization Name:
Comment: This rule will have unintended consequences that will negatively affect our electronics. I implore the FCC to leave well enough alone.

This rule will have unintended consequences that will negatively affect our electronics. I implore the FCC to leave well enough alone.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Jason
Last Name: Gurley
Mailing Address: 1068 County Road 546
City: Greenway
Country: United States
State or Province: AR
ZIP/Postal Code: 72430
Email Address: kerashi@gmail.com
Organization Name: null
Comment: As someone who has in the past used ddwrt firmware distribution on routers that were no longer receiving firmware updates from manufacturers, I find it troubling that you would effectively outlaw the use of such alternative firmware. It is quite common for router vendors to stop updating firmware after a few years, resulting in hardware that has security vulnerabilities that may never be patched. Alternative firmware distributions from open-source firmware projects provide a means of getting updated firmware on at least some of these devices. Also, these alternative firmware versions often have more powerful features than stock firmware, in such areas as firewalls and network diagnostics. Please don't make it illegal to use such firmware distributions.

As someone who has in the past used ddwrt firmware distribution on routers that were no longer receiving firmware updates from manufacturers, I find it troubling that you would effectively outlaw the use of such alternative firmware. It is quite common for router vendors to stop updating firmware after a few years, resulting in hardware that has security vulnerabilities that may never be patched. Alternative firmware distributions from open-source firmware projects provide a means of getting updated firmware on at least some of these devices. Also, these alternative firmware versions often have more powerful features than stock firmware, in such areas as firewalls and network diagnostics. Please don't make it illegal to use such firmware distributions.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Michael
Last Name: Wiggins
Mailing Address: 12121 Winchester Rd
City: Ashville
Country: United States
State or Province: OH
ZIP/Postal Code: 43103
Email Address:
Organization Name:
Comment: These rules are being promulgated based on industry input, without consideration of unbiased expertise. The rules as proposed are clearly written by an industry seeking to protect corporate profits in the thin guise of aligning with the mission of the FCC. The unintended consequences of the proposed rules will criminalize legitimate actions and will harm efforts of citizens to improve compliance, security, and performance of broadcasting devices they own.

These rules are being promulgated based on industry input, without consideration of unbiased expertise. The rules as proposed are clearly written by an industry seeking to protect corporate profits in the thin guise of aligning with the mission of the FCC. The unintended consequences of the proposed rules will criminalize legitimate actions and will harm efforts of citizens to improve compliance, security, and performance of broadcasting devices they own.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Alan
Last Name: Somers
Mailing Address: 6463 Bluebird Ave
City: Longmont
Country: United States
State or Province: CO
ZIP/Postal Code: 80503
Email Address:
Organization Name:
Comment: Please don't pass this rule! As a wifi user, replacing the firmware on my consumer routers is extremely important to me. I don't care about being about to jack the power way up; I have only one house to cover. But I care about security (remember the "suprman" fiasco? The industry still hasn't learned: https://securityledger.com/2015/08/hardcoded-firmware-password-sinks-home-routers/) and I care about the flexibility to customize the software installed on my router. For example, I back up router settings with rsync. Not only does no off-the-shelf router OS install rsync, but rsync's GPLv3 license explicitly prohibits its distribution on "tivoized" platforms, which is just what this rule would require!

To give another example, my father is no networking expert. But he was able to quickly load DD-WRT onto two old routers and setup a wireless bridge between his house and an outbuilding. That capability is rare on OEM operating system.

Please don't take away our freedom to run the software of our choice on our own devices!

-Alan Somers, OpenWRT user since 2006

Please don't pass this rule! As a wifi user, replacing the firmware on my consumer routers is extremely important to me. I don't care about being about to jack the power way up; I have only one house to cover. But I care about security (remember the "suprman" fiasco? The industry still hasn't learned: https://securityledger.com/2015/08/hardcoded-firmware-password-sinks-home-routers/) and I care about the flexibility to customize the software installed on my router. For example, I back up router settings with rsync. Not only does no off-the-shelf router OS install rsync, but rsync's GPLv3 license explicitly prohibits its distribution on "tivoized" platforms, which is just what this rule would require!

To give another example, my father is no networking expert. But he was able to quickly load DD-WRT onto two old routers and setup a wireless bridge between his house and an outbuilding. That capability is rare on OEM operating system.

Please don't take away our freedom to run the software of our choice on our own devices!

-Alan Somers, OpenWRT user since 2006

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Jeffrey
Last Name: Miller
Mailing Address: 653 NW 80th Street
City: Seattle
Country: United States
State or Province: WA
ZIP/Postal Code: 98117
Email Address: jeffrey.miller@gmail.com
Organization Name:
Comment: To the FCC:

I am seriously concerned that this requirement for software-defined radios (including Wi-Fi networking equipment) will prevent its owners from upgrading and securing their devices. In an environment where exploits of routers have been demonstrated as a source of serious vulnerability in digital networking, exposing and compromising personal information, this requirement asserts the primacy of bureaucractic control to the direct detriment of the privacy and security interests of the owners and users of digital communication equipment.

Specifically this text is problematic:
"Also, an applicant for certification would have to specify which parties will be authorized to make software changes (e.g., the grantee, wireless service provider, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation."

unless the "authorized parties" is explicitly required to include the owner and operator of said equipment.

Regards,

Jeffrey S. Miller
Seattle, Washington

To the FCC:

I am seriously concerned that this requirement for software-defined radios (including Wi-Fi networking equipment) will prevent its owners from upgrading and securing their devices. In an environment where exploits of routers have been demonstrated as a source of serious vulnerability in digital networking, exposing and compromising personal information, this requirement asserts the primacy of bureaucractic control to the direct detriment of the privacy and security interests of the owners and users of digital communication equipment.

Specifically this text is problematic:
"Also, an applicant for certification would have to specify which parties will be authorized to make software changes (e.g., the grantee, wireless service provider, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation."

unless the "authorized parties" is explicitly required to include the owner and operator of said equipment.