

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: Hrishenko

Mailing Address: 321 N Fox Ridge Dr.

City: Raymore

Country: United States

State or Province: MO

ZIP/Postal Code: 64083

Email Address:

Organization Name:

Comment: Regarding the following clause and related articles:

(10) Applications for certification of U-NII devices in the 5.15-5.35 GHz and the 5.47-5.85 GHz bands must include a high level operational description of the security procedures that control the radio frequency operating parameters and ensure that UNAUTHORIZED MODIFICATIONS cannot be made.

Please do not restrict the public use and innovation of such devices. If our government were a socialist state where only one manufacturer existed to produce any operable system capable of communications over the 5 GHz range, such a law might serve well. To my everpresent relief we DO NOT live in such a state, and in fact some of the best and most innovative products are developed by communities of free-thinking, unpaid individuals worldwide. That you would curb this development and cripple the U.S. in an already escalating cyber-war is a disservice to every man and woman who contributed to make this nation the foundation of the digital age. Please let me secure my wireless router with open-source code. Let Google and Apple continue using open-source code on their devices. Give us the freedom to respond in real-time to the security threats that have become so common in this information era. Wifi is a very small freedom granted to us in a domain so extremely regulated already, please don't take it away.

Regarding the following clause and related articles:

(10) Applications for certification of U-NII devices in the 5.15-5.35 GHz and the 5.47-5.85 GHz bands must include a high level operational description of the security procedures that control the radio frequency operating parameters and ensure that UNAUTHORIZED MODIFICATIONS cannot be made.

Please do not restrict the public use and innovation of such devices. If our government were a socialist state where only one manufacturer existed to produce any operable system capable of communications over the 5 GHz range, such a law might serve well. To my everpresent relief we DO NOT live in such a state, and in fact some of the best and most innovative products are developed by communities of free-thinking, unpaid individuals worldwide. That you would curb this development and cripple the U.S. in an already escalating cyber-war is a disservice to every man and woman who contributed to make this nation the foundation of the digital age. Please let me secure my wireless router with open-source code. Let Google and Apple continue using open-source code on their devices. Give us the freedom to respond in real-time to the security threats that have become so common in this information era. Wifi is a very small freedom granted to us in a domain so extremely regulated already, please don't take it away.

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: Wong

Mailing Address: 523 64 Avenue Northwest

City: Calgary

Country: Canada

State or Province: Alberta

ZIP/Postal Code: T2K0M3

Email Address:

Organization Name:

Comment: This isn't right, you're attempting to help us but you're hurting us even further if this goes through.

This isn't right, you're attempting to help us but you're hurting us even further if this goes through.

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: Lane

Mailing Address: 1339 146th PL A8

City: Whitestone

Country: United States

State or Province: NY

ZIP/Postal Code: 11568

Email Address: mikeurl@gmail.com

Organization Name: none

Comment: I hope the Commission can clarify. Is the intention to require manufacturers to show that the device can't be modified *beyond* it's approved limits? Meaning that you can't flash a router to pump out 500 watts of RF (to use an extreme example).

Or is it the Commission's intention to, for example, outlaw something like DD-WRT entirely?

If the intention is just to make sure that software can't modify the settings that the device maker indicated are the "limits" of the proposed operation I hope the Commission can make that more clear.

The cost of compliance with this reg is estimated to be almost none. If device lockdown is the intention then every device maker would be forced to implement some kind of "trusted computing" model and the costs of compliance would be enormous. Every chip/software would have to be redesigned to include an encrypted connection that only "authorized parties" have access to.

I certainly hope the intention of the regulation is NOT to remove the ability of consumers to use custom firmware to improve their end-user experience.

I hope the Commission can clarify. Is the intention to require manufacturers to show that the device can't be modified *beyond* it's approved limits? Meaning that you can't flash a router to pump out 500 watts of RF (to use an extreme example).

Or is it the Commission's intention to, for example, outlaw something like DD-WRT entirely?

If the intention is just to make sure that software can't modify the settings that the device maker indicated are the "limits" of the proposed operation I hope the Commission can make that more clear.

The cost of compliance with this reg is estimated to be almost none. If device lockdown is the intention then every device maker would be forced to implement some kind of "trusted computing" model and the costs of compliance would be enormous. Every chip/software would have to be redesigned to include an encrypted connection that only "authorized parties" have access to.

I certainly hope the intention of the regulation is NOT to remove the ability of consumers to use custom firmware to improve their end-user experience.

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: Mark

Last Name: Rand

Mailing Address: Rustler Lane

City: Folsom

Country: United States

State or Province: CA

ZIP/Postal Code: 95639

Email Address:

Organization Name:

Comment: I write to request that the FCC not implement rules that would deprive users of the ability to install software of their own choosing on their computing devices.

As a user of a wifi device which I needed to patch with third-party open source firmware drivers to maintain the security and reliability of my communications, I have experienced first-hand the vital importance of end user's ability to secure their own equipment.

Such a ruling would also serve to further undermine the competitiveness of American communications products and services both at home and abroad.

I write to request that the FCC not implement rules that would deprive users of the ability to install software of their own choosing on their computing devices.

As a user of a wifi device which I needed to patch with third-party open source firmware drivers to maintain the security and reliability of my communications, I have experienced first-hand the vital importance of end user's ability to secure their own equipment.

Such a ruling would also serve to further undermine the competitiveness of American communications products and services both at home and abroad.

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: Darrin

Last Name: Rogers

Mailing Address: 83 Maple Avenue

City: Fredonia

Country: United States

State or Province: NY

ZIP/Postal Code: 14063

Email Address: petitions@darrinrogers.com

Organization Name:

Comment: This proposal, while draped in the language of technical necessity, is a handout to the companies who make wireless devices and the security industry that regularly errs on the side of restriction of citizen freedom in its zeal to make its job easier and garner federal funds.

This proposal would create regulations to strangle innovation and handicap ongoing (and future) projects demonstrating exactly why America has traditionally kept up, technologically, with other nations even while suffering demographic and infrastructure challenges in doing so. This proposal is the equivalent of prohibiting ham radio operators from fiddling with their sets to increase range, or criminalizing auto aficionados trying to squeeze more speed or efficiency from their engines.

Please stop this silly proposal. I am one of many people who would be negatively affected. I use Linux on three or more computers, I root my tablets, I have aftermarket firmware on my router, and I have even replaced my mp3 player's operating system with a better open-source option. These alternatives increase my productivity and enjoyment, and it's extremely difficult to see how anything I do with them (like millions of other technology users) constitutes any kind of threat as mentioned in the proposal's introduction.

This proposal is nothing but a method of giving a few companies even more control over the formerly-free market. Please kill the proposal.

This proposal, while draped in the language of technical necessity, is a handout to the companies who make wireless devices and the security industry that regularly errs on the side of restriction of citizen freedom in its zeal to make its job easier and garner federal funds.

This proposal would create regulations to strangle innovation and handicap ongoing (and future) projects demonstrating exactly why America has traditionally kept up, technologically, with other nations even while suffering demographic and infrastructure challenges in doing so. This proposal is the equivalent of prohibiting ham radio operators from fiddling with their sets to increase range, or criminalizing auto aficionados trying to squeeze more speed or efficiency from their engines.

Please stop this silly proposal. I am one of many people who would be negatively affected. I use Linux on three or more computers, I root my tablets, I have aftermarket firmware on my router, and I have even replaced my mp3 player's operating system with a better open-source option. These alternatives increase my productivity and enjoyment, and it's extremely difficult to see how anything I do with them (like millions of other technology users) constitutes any kind of threat as mentioned in the proposal's introduction.

This proposal is nothing but a method of giving a few companies even more control over the formerly-free market.
Please kill the proposal.

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: Theodore

Last Name: Pepe

Mailing Address: 40 Walnut St. Apt 1

City: Belmont

Country: United States

State or Province: MA

ZIP/Postal Code: 02478

Email Address: cykros@lycos.com

Organization Name: null

Comment: I've no doubt you've received comment from folks more eloquent than I detailing exactly why this is an overreaching regulation that would result in absurd amounts of waste, both material and in labor, and meanwhile not actually achieve the goal it sets out with due to issues stemming from the fact that it is particularly easy to circumvent, as any computer can be made to operate as one of these devices, given that computers are, at the end of the day, computers, rather than the highly specialized machines they may be marketed as in stores for the sake of drumming up profits. It stifles innovation, and ultimately seeks to pointlessly criminalize harmless behavior while not having the teeth it would need to address the issues it seeks to. While there may be very real issues here that should be addressed, this is most certainly not the way forward, and if passed, will be seen as no less short sighted than the Computer Fraud and Abuse Act or the Digital Millenium Copyright Act, both of which have become synonymous with governmental inability to grasp technology.

I seek only to add my comment here to ensure that the numbers do not appear inconsequential. Seek some expert advice, go back to the drawing board, and put forth something a bit more polished. Or don't. Doing nothing would be less problematic than allowing this regulation to move forward.

I've no doubt you've received comment from folks more eloquent than I detailing exactly why this is an overreaching regulation that would result in absurd amounts of waste, both material and in labor, and meanwhile not actually achieve the goal it sets out with due to issues stemming from the fact that it is particularly easy to circumvent, as any computer can be made to operate as one of these devices, given that computers are, at the end of the day, computers, rather than the highly specialized machines they may be marketed as in stores for the sake of drumming up profits. It stifles innovation, and ultimately seeks to pointlessly criminalize harmless behavior while not having the teeth it would need to address the issues it seeks to. While there may be very real issues here that should be addressed, this is most certainly not the way forward, and if passed, will be seen as no less short sighted than the Computer Fraud and Abuse Act or the Digital Millenium Copyright Act, both of which have become synonymous with governmental inability to grasp technology.

I seek only to add my comment here to ensure that the numbers do not appear inconsequential. Seek some expert advice, go back to the drawing board, and put forth something a bit more polished. Or don't. Doing nothing would be less problematic than allowing this regulation to move forward.

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: Smith

Mailing Address: 1175 Homeward Lane

City: Altamonte Springs

Country: United States

State or Province: FL

ZIP/Postal Code: 32714

Email Address:

Organization Name:

Comment: Access to the bootloader of devices allows ingenuity beyond the original ideas of the manufacturer. It provides flexibility in scenarios that could not have been predicted. I am an engineer with an optical research group out of the University of Central Florida and we heavily rely on flash-able wireless routers for experimentation purposes. We would not be successful without the ability to interconnect atmospheric instruments, data collection computers, and tracker pedestals wirelessly. There are legitimate uses for unlocked bootloaders on wireless devices and the benefits far outweigh the risks.

Access to the bootloader of devices allows ingenuity beyond the original ideas of the manufacturer. It provides flexibility in scenarios that could not have been predicted. I am an engineer with an optical research group out of the University of Central Florida and we heavily rely on flash-able wireless routers for experimentation purposes. We would not be successful without the ability to interconnect atmospheric instruments, data collection computers, and tracker pedestals wirelessly. There are legitimate uses for unlocked bootloaders on wireless devices and the benefits far outweigh the risks.

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: Brad

Last Name: Miller

Mailing Address: 1213 W Oklahoma St

City: Appleton

Country: United States

State or Province: WI

ZIP/Postal Code: 54914

Email Address: cpdevnull@gmail.com

Organization Name:

Comment: This change would have severe unintended consequences for the open source community. It should not be passed as is.

This change would have severe unintended consequences for the open source community. It should not be passed as is.

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: Anonymous

Last Name: Anonymous

Mailing Address: 801 Culver St.

City: Commerce

Country: United States

State or Province: TX

ZIP/Postal Code: 75428

Email Address: null

Organization Name: null

Comment: As a Computer Information Systems student and part-time hardware support technician, I ask that the FCC reconsider the implementation of this proposed rule in order to safeguard the rights of the end-user to install whatever software they choose onto their computing and networking devices.

I've used an open-source firmware, DD-WRT, in all of my routers for the last five years, and it has given me a greater amount of control over security and performance than limited OEM-issued firmware. Custom firmware has assisted me in creating a RADIUS-secured VPN for remote access to my personal server, as well as a VPN designed for pooling of remote resources that my colleagues and I use for resource-intensive computing projects. When the NIC failed in one of my computers, I used custom firmware to turn an old router I hadn't used for years into a WiFi adapter, keeping my computer connected and recycling an outdated device in the process. Under the proposed rule, the installation of custom firmware such as DD-WRT would be illegal on these devices.

What's more, I fear that this proposed rule may have unintentional consequences to the public. Wireless networking research is highly dependent on the ability to modify wireless devices. Additional restrictions to the modifications that can be performed on these devices could have a detrimental effect of wireless research that can be performed in the US. In addition, continuing to allow users to modify or replace the existing firmware on their devices means that users can continue to fix security exploits and other bugs in their device's firmware that the manufacturer is either unwilling or unable to fix themselves, as well as keep aging networking technology, which may no longer have official support, up-to-date with more current devices.

I also feel that the proposed rule has too wide of a scope. Preventing modification to all computing devices with an "electronic label"* or "modular transmitter"*** could unintentionally restrict the ability of the end-user to install open-source operating systems such as Linux onto their PCs or alternative firmware on smartphone and tablet devices. Enacting this rule would also heavily discourage development of open-source WiFi firmware such as the aforementioned DD-WRT and OpenWrt, the latter of which is developed by an enthusiast community that relies on the ability to modify routers to further develop their software. Considering that OpenWrt is used by several networking hardware manufacturers such as Linksys**** and MediaTek***** as a basis for their own router software, stifling its development could increase the cost of developing router software for these companies; a cost which would likely be passed on to the consumer.

It is my hope that the FCC will continue to respect the right of the end-user to tailor their devices to better suit their needs by installing the software of their choosing, rather than require manufacturers to lock out their devices from modification by the public.

*Section 2.935(d) on page 46918

**Sections 2.1033(4i) on page 46919 and 2.1042(e) on page 46922

***<http://www.linksys.com/us/wireless-routers/c/wrt-wireless-routers/#fullstory>

****<http://mediatek.com/en/news-events/mediatek-news/mediatek-launches-mt7628-industrys-first-80211n-2t2r-ap-soc-for-home-router-smart-router-and-iot-gateway/>

As a Computer Information Systems student and part-time hardware support technician, I ask that the FCC reconsider the implementation of this proposed rule in order to safeguard the rights of the end-user to install whatever software they choose onto their computing and networking devices.

I've used an open-source firmware, DD-WRT, in all of my routers for the last five years, and it has given me a greater amount of control over security and performance than limited OEM-issued firmware. Custom firmware has assisted me in creating a RADIUS-secured VPN for remote access to my personal server, as well as a VPN designed for pooling of remote resources that my colleagues and I use for resource-intensive computing projects. When the NIC failed in one of my computers, I used custom firmware to turn an old router I hadn't used for years into a WiFi adapter, keeping my computer connected and recycling an outdated device in the process. Under the proposed rule, the installation of custom firmware such as DD-WRT would be illegal on these devices.

What's more, I fear that this proposed rule may have unintentional consequences to the public. Wireless networking research is highly dependent on the ability to modify wireless devices. Additional restrictions to the modifications that can be performed on these devices could have a detrimental effect of wireless research that can be performed in the US. In addition, continuing to allow users to modify or replace the existing firmware on their devices means that users can continue to fix security exploits and other bugs in their device's firmware that the manufacturer is either unwilling or unable to fix themselves, as well as keep aging networking technology, which may no longer have official support, up-to-date with more current devices.

I also feel that the proposed rule has too wide of a scope. Preventing modification to all computing devices with an "electronic label"* or "modular transmitter"*** could unintentionally restrict the ability of the end-user to install open-source operating systems such as Linux onto their PCs or alternative firmware on smartphone and tablet devices. Enacting this rule would also heavily discourage development of open-source WiFi firmware such as the aforementioned DD-WRT and OpenWrt, the latter of which is developed by an enthusiast community that relies on the ability to modify routers to further develop their software. Considering that OpenWrt is used by several networking hardware manufacturers such as Linksys*** and MediaTek**** as a basis for their own router software, stifling its development could increase the cost of developing router software for these companies; a cost which would likely be passed on to the consumer.

It is my hope that the FCC will continue to respect the right of the end-user to tailor their devices to better suit their needs by installing the software of their choosing, rather than require manufacturers to lock out their devices from modification by the public.

*Section 2.935(d) on page 46918

**Sections 2.1033(4i) on page 46919 and 2.1042(e) on page 46922

***<http://www.linksys.com/us/wireless-routers/c/wrt-wireless-routers/#fullstory>

****<http://mediatek.com/en/news-events/mediatek-news/mediatek-launches-mt7628-industrys-first-80211n-2t2r-ap-soc-for-home-router-smart-router-and-iot-gateway/>

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Gary

Last Name: Travis

Mailing Address: 136 E 8th St.

City: Port Angeles

Country: United States

State or Province: WA

ZIP/Postal Code: 98362

Email Address: garyt@satyr.com

Organization Name: null

Comment: The re-certification clause in B38, etc, is burdensome for individuals or organizations who wish to re-purpose previously certified equipment. It is especially a non-issue when it comes to devices that are already designed to have relatively low power output on bands that are also occupied by "garbage" transmitters like microwave ovens and low-cost telemetry devices (the 2.4GHz band).

It is understandable that you don't want devices tampered-with to the point that they become interferers, but the wording put forth in this document is over-generalized and can be a huge hindrance to open-source developers of networking and SDR products.

The re-certification clause in B38, etc, is burdensome for individuals or organizations who wish to re-purpose previously certified equipment. It is especially a non-issue when it comes to devices that are already designed to have relatively low power output on bands that are also occupied by "garbage" transmitters like microwave ovens and low-cost telemetry devices (the 2.4GHz band).

It is understandable that you don't want devices tampered-with to the point that they become interferers, but the wording put forth in this document is over-generalized and can be a huge hindrance to open-source developers of networking and SDR products.

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: Allegretti

Mailing Address: 337 AP Newcomb Rd

City: Brewster

Country: United States

State or Province: MA

ZIP/Postal Code: 02631

Email Address: rob.allegretti@gmail.com

Organization Name: null

Comment: To whom it may concern:

Please do not proceed with the implementation of the Equipment Authorization and Electronic Labeling for Wireless Devices FCC-2015-0262-0001, or of any rules which prevent consumers or professionals from installing software of their choosing on their computing devices.

This will prevent technological advancement which is beneficial to society as a whole, and will cause considerable waste in the form of hardware which is no longer serviceable and cannot be upgraded. It also has the decidedly harmful side-effect of preventing competition among hardware, software, and operating system vendors by disallowing private development of software for specific hardware devices.

These regulations will also hamper device and network security, as it will become significantly more difficult, costly, or time-consuming to patch security vulnerabilities within network and cellular hardware. This will ultimately lead to more cyber-crime events and other intrusion-related problems as the criminal element exploits these unaddressed security holes.

Many research projects will also be affected, including development of mobile applications and newer, better forms of wireless communication, as these rules would prevent individuals from experimenting with new settings and configurations of their hardware. Technologies such as long-range or low-power Bluetooth, and higher speed WiFi communication would not be possible today without such experimentation in the past.

In addition to the hindrance of future development, this would prevent security or bug fixes from being properly addressed in existing hardware by hardware manufacturers, or would require undue burden to the consumer to have the manufacturer or another 'authorized' person perform these upgrades. In the worst case scenario, this would require a new purchase for every software iteration, which is quantifiably wasteful and harmful to the consumer.

Furthermore, there is no reason for these regulations. Customized firmware does not present a threat to existing or future technology, and existing modified devices do not contribute additional interference or

Finally, billions of dollars of present and future commerce would be impeded by these regulations, such as from WiFi vendors, retail hotspot vendors, and anyone creating or selling customized wireless hardware for public consumption. These technologies and programming abilities are crucial to this industry and the proposed regulations would prevent the resellers or installers from customizing this hardware to suit its intended purpose correctly.

Please reconsider these regulations, and do not proceed with implementation of these rules.

Thank you,

Rob Allegretti
rob.allegretti@gmail.com

To whom it may concern:

Please do not proceed with the implementation of the Equipment Authorization and Electronic Labeling for Wireless Devices FCC-2015-0262-0001, or of any rules which prevent consumers or professionals from installing software of their choosing on their computing devices.

This will prevent technological advancement which is beneficial to society as a whole, and will cause considerable waste in the form of hardware which is no longer serviceable and cannot be upgraded. It also has the decidedly harmful side-effect of preventing competition among hardware, software, and operating system vendors by disallowing private development of software for specific hardware devices.

These regulations will also hamper device and network security, as it will become significantly more difficult, costly, or time-consuming to patch security vulnerabilities within network and cellular hardware. This will ultimately lead to more cyber-crime events and other intrusion-related problems as the criminal element exploits these unaddressed security holes.

Many research projects will also be affected, including development of mobile applications and newer, better forms of wireless communication, as these rules would prevent individuals from experimenting with new settings and configurations of their hardware. Technologies such as long-range or low-power Bluetooth, and higher speed WiFi communication would not be possible today without such experimentation in the past.

In addition to the hindrance of future development, this would prevent security or bug fixes from being properly addressed in existing hardware by hardware manufacturers, or would require undue burden to the consumer to have the manufacturer or another 'authorized' person perform these upgrades. In the worst case scenario, this would require a new purchase for every software iteration, which is quantifiably wasteful and harmful to the consumer.

Furthermore, there is no reason for these regulations. Customized firmware does not present a threat to existing or future technology, and existing modified devices do not contribute additional interference or

Finally, billions of dollars of present and future commerce would be impeded by these regulations, such as from WiFi vendors, retail hotspot vendors, and anyone creating or selling customized wireless hardware for public consumption. These technologies and programming abilities are crucial to this industry and the proposed regulations would prevent the resellers or installers from customizing this hardware to suit its intended purpose correctly.

Please reconsider these regulations, and do not proceed with implementation of these rules.

Thank you,

Rob Allegretti
rob.allegretti@gmail.com

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: chase

Last Name: barber

Mailing Address: 1580 E Route 66

City: flagstaff

Country: United States

State or Province: AZ

ZIP/Postal Code: 86001

Email Address:

Organization Name:

Comment: These regulations are especially oppressive to small companies and to free software developers. Individuals and small companies that want to make changes to their own products, to build custom devices, or to provide custom services will be forced out of the market if they don't use proprietary software or if they are required to pay licensing fees to those who control the DRM signing keys that allow the upgrading of software and firmware on encrypted devices.

These regulations are especially oppressive to small companies and to free software developers. Individuals and small companies that want to make changes to their own products, to build custom devices, or to provide custom services will be forced out of the market if they don't use proprietary software or if they are required to pay licensing fees to those who control the DRM signing keys that allow the upgrading of software and firmware on encrypted 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: James

Last Name: Patrick

Mailing Address: 201 South 10th St

City: Richmond

Country: United States

State or Province: IN

ZIP/Postal Code: 47374

Email Address: jamesepatrick@gmail.com

Organization Name: null

Comment: I'm really hoping this doesn't disappear into some mailbag. My name is James Patrick, I'm a software developer, and system admin for a start up in Richmond Indiana. I adamantly hope this proposal does not pass. Over the past years I've personally had to develop and deploy fixes for both current and legacy hardware. Most currently supported hardware are slow to respond to security CVE items. Significant vulnerabilities be actively being exploded for months before a vendor will respond with a firmware patch, and legacy hardware is lucky if it ever receives a patch. More and more router's are becoming commodity item, firmware patches are either uncommon or poorly written. Having a secure and verifiable alternative to known vulnerabilities instantly is needed in general but also specifically for me and my work. Major vendors have a disincentive to support legacy devices while the needs are something that haven't changed. Additionally having the vendors being the only gatekeeper for feature sets means that we could easy be paying a premium for feature sets that would otherwise be supported (see Linksys in the early 2000's). There are some vendors that do support opensource firmware, the regulation we should still be dependent on the company it self to insure that the firmware for our LAN and WLAN connects are secure, and support for legacy hardware will still have the same issue.

For an example of this exact issue on simply has to look at the cell phones in the US. Devices that are 2 years or older often aren't supported, patches do not come out or are so slow to come out that exploits will have been actively exploded for months. Both the use of unsigned open source alternatives to router firmware, and open source alternatives to partially deprecated or legacy phones stem void that is not filled by the vendors themselves.

I'm really hoping this doesn't disappear into some mailbag. My name is James Patrick, I'm a software developer, and system admin for a start up in Richmond Indiana. I adamantly hope this proposal does not pass. Over the past years I've personally had to develop and deploy fixes for both current and legacy hardware. Most currently supported hardware are slow to respond to security CVE items. Significant vulnerabilities be actively being exploded for months before a vendor will respond with a firmware patch, and legacy hardware is lucky if it ever receives a patch. More and more router's are becoming commodity item, firmware patches are either uncommon or poorly written. Having a secure and verifiable alternative to known vulnerabilities instantly is needed in general but also specifically for me and my work. Major vendors have a disincentive to support legacy devices while the needs are something that haven't changed. Additionally having the vendors being the only gatekeeper for feature sets means that we could easy be paying a premium for feature sets that would otherwise be supported (see Linksys in the early 2000's). There are some vendors that do support opensource firmware, the regulation we should still be dependent on the company it self to insure that the firmware for our LAN and WLAN connects are secure, and support for legacy hardware will still have the same issue.

For an example of this exact issue one simply has to look at the cell phones in the US. Devices that are 2 years or older often aren't supported, patches do not come out or are so slow to come out that exploits will have been actively exploited for months. Both the use of unsigned open source alternatives to router firmware, and open source alternatives to partially deprecated or legacy phones stem from a void that is not filled by the vendors themselves.

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: Philip

Last Name: Dorr

Mailing Address: 804 Lexington

City: Pleasant Hill

Country: United States

State or Province: MO

ZIP/Postal Code: 64080

Email Address: tagno25@gmail.com

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Hanson

Mailing Address: 4032 Burton Place West

City: Seattle

Country: United States

State or Province: WA

ZIP/Postal Code: 98199

Email Address:

Organization Name:

Comment: Please do not take away the ability of users to install software on computing or communication devices.

* We need to be able to fix security issues and repair errors, even if the manufacturer does not chose to maintain or support their device.

Allowing users to apply fixes will also help reduce e-waste.

* Researchers need to be able to investigate and modify devices in order to help detect and correct problems in operation or in security.

* Innovation and education requires the ability to access and modify devices. If we preclude such access, then the focus for innovation will move overseas, and the US will be left even further behind in technology and engineering, relegated to simply using the devices and services invented elsewhere.

* Manufacturers or third parties could install software that changes a devices function - removing features, making it inoperable, or even making it work in a harmful manner. Restricting the users right to install software on the device could make it illegal for the user to restore the device to a previously operating state. So they could be held hostage - either having to pay ransome to some third party to undo the damage, or having to dispose of the device. As more devices incorporate communication technology (the Internet of things), this leaves users increasingly vulnerable to remote manipulation.

Please do not take away the ability of users to install software on computing or communication devices.

* We need to be able to fix security issues and repair errors, even if the manufacturer does not chose to maintain or support their device.

Allowing users to apply fixes will also help reduce e-waste.

* Researchers need to be able to investigate and modify devices in order to help detect and correct problems in operation or in security.

* Innovation and education requires the ability to access and modify devices. If we preclude such access, then the focus for innovation will move overseas, and the US will be left even further behind in technology and engineering, relegated to simply using the devices and services invented elsewhere.

* Manufacturers or third parties could install software that changes a devices function - removing features, making it inoperable, or even making it work in a harmful manner. Restricting the users right to install software on the device could make it illegal for the user to restore the device to a previously operating state. So they could be held hostage - either having to pay ransome to some third party to undo the damage, or having to dispose of the device. As more devices incorporate communication technology (the Internet of things), this leaves users increasingly vulnerable to remote manipulation.

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: Weinstein

Mailing Address: 2132 Idaho Falls Drive

City: Henderson

Country: United States

State or Province: NV

ZIP/Postal Code: 89044-0150

Email Address:

Organization Name:

Comment: 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 do not patch routers with serious security holes.

This rule would prevent 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 Community implemented the fq_codel algorithm for eliminating bufferbloat-based network congestion by using a version of OpenWrt. The fixes for this are now in the Linux kernel.

Mesh networking research depends on low-level access and modification of kernel on the router.

Vendors have not developed mesh networking support; instead it's been done primarily by the community on open and modifiable drivers and firmware.

Research into wireless networking requires low-level access to drivers and firmware.

Nearly 7,200 academic articles related to open drivers and firmware. The research cannot occurred without the ability to modify the device's software.

I believe that, Ham radio operators are allowed to operate at a higher power in portions of the unlicensed spectrum than non-licensed operators. This requirement prevents them from modifying low cost routers for operating long range wifi networks, such as would be useful in a disaster situation.

The law permits amateur radio operators to increase the transmit power on commercial routers beyond its regular limits, where the wifi frequencies overlap with frequencies. This system works particularly well for emergency communication. See Broadband-Hamnet.

Broadband-Hamnet uses a mesh networking protocol so this interacts with the issues on innovation

No FCC complaints about improper usage of routers were related to flashing third-party firmware. Most were related to commercial wifi providers breaking the law. In some cases, the official router web administration for the routers used in the complaint had a UI for operating in an illegal fashion. For example, it was possible to turn off all DFS or allow test operation on all possible channels which are both wildly irresponsible to place in a standard router UI.

The key problem necessitating the rule change, the need to make sure DFS is running near airports with Terminal-area Doppler Weather Radar (TDWR), is primarily relevant for those operating a wifi router outside within a mile or so of 45 airports in the US.

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 do not patch routers with serious security holes.

This rule would prevent 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 Community implemented the fq_codel algorithm for eliminating bufferbloat-based network congestion by using a version of OpenWrt. The fixes for this are now in the Linux kernel.

Mesh networking research depends on low-level access and modification of kernel on the router.

Vendors have not developed mesh networking support; instead it's been done primarily by the community on open and modifiable drivers and firmware.

Research into wireless networking requires low-level access to drivers and firmware.

Nearly 7,200 academic articles related to open drivers and firmware. The research cannot occurred without the ability to modify the device's software.

I believe that, Ham radio operators are allowed to operate at a higher power in portions of the unlicensed spectrum than non-licensed operators. This requirement prevents them from modifying low cost routers for operating long range wifi networks, such as would be useful in a disaster situation.

The law permits amateur radio operators to increase the transmit power on commercial routers beyond its regular limits, where the wifi frequencies overlap with frequencies. This system works particularly well for emergency communication. See Broadband-Hamnet.

Broadband-Hamnet uses a mesh networking protocol so this interacts with the issues on innovation

No FCC complaints about improper usage of routers were related to flashing third-party firmware. Most were related to commercial wifi providers breaking the law. In some cases, the official router web administration for the routers used in the complaint had a UI for operating in an illegal fashion. For example, it was possible to turn off all DFS or allow test operation on all possible channels which are both wildly irresponsible to place in a standard router UI.

The key problem necessitating the rule change, the need to make sure DFS is running near airports with Terminal-area Doppler Weather Radar (TDWR), is primarily relevant for those operating a wifi router outside within a mile or so of 45 airports in the US.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ryan

Last Name: Nelson

Mailing Address: 611 Foxbury Ct Apt B

City: Columbus

Country: United States

State or Province: OH

ZIP/Postal Code: 43228

Email Address: ryan@ryannelson.us

Organization Name:

Comment: I am asking for this to never go into effect. By taking this away you are harming the open source community. A lot of DIYers mod there own purchased wireless routers because the firmware that come stock either sucks or does not work half the time. I personally mod mine to open features that allow me to run features that would otherwise not be available to me. A lot of wireless router manufactures have gaping security holes in the software that they will not patch either as it is not cost effective or they do not believe it to be a sever enough issue to warrant it. Taking this away from the people would set back the open source community a great deal.

Ryan Nelson

I am asking for this to never go into effect. By taking this away you are harming the open source community. A lot of DIYers mod there own purchased wireless routers because the firmware that come stock either sucks or does not work half the time. I personally mod mine to open features that allow me to run features that would otherwise not be available to me. A lot of wireless router manufactures have gaping security holes in the software that they will not patch either as it is not cost effective or they do not believe it to be a sever enough issue to warrant it. Taking this away from the people would set back the open source community a great deal.

Ryan Nelson

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: Timothy

Last Name: Parrotte

Mailing Address: 472 Shawmont Avenue, Apt C

City: Philadelphia

Country: United States

State or Province: PA

ZIP/Postal Code: 19128

Email Address:

Organization Name:

Comment: It is extremely important to a capitalist society that we be able to do whatever we wish to our possessions so long as we don't harm others in the process.

The freedom to flash custom firmware to wireless routers and other devices is very important to myself and to society at large.

Banning custom firmware would make us legally subject to the whims of corporations, which limits our First Amendment right to free speech.

It is extremely important to a capitalist society that we be able to do whatever we wish to our possessions so long as we don't harm others in the process.

The freedom to flash custom firmware to wireless routers and other devices is very important to myself and to society at large.

Banning custom firmware would make us legally subject to the whims of corporations, which limits our First Amendment right to free speech.

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: Forest

Last Name: Wilkinson

Mailing Address: 1436 8th st

City: Berkeley

Country: United States

State or Province: CA

ZIP/Postal Code: 94710

Email Address:

Organization Name:

Comment: You must not make any rules that interfere with equipment owners' ability to modify or replace the software or firmware in their devices. Such modifications are critical to the security of individuals' communications and networks, the security of the internet as a whole, and to the innovations made possible by both hobbyists and trained engineers. Any attempt to prevent radio interference by way of disabling such critical functionality is horribly misguided; essentially throwing the baby out with the bathwater.

You must not make any rules that interfere with equipment owners' ability to modify or replace the software or firmware in their devices. Such modifications are critical to the security of individuals' communications and networks, the security of the internet as a whole, and to the innovations made possible by both hobbyists and trained engineers. Any attempt to prevent radio interference by way of disabling such critical functionality is horribly misguided; essentially throwing the baby out with the bathwater.

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: Deven

Last Name: Hubbard

Mailing Address: 5176 Bootlegger Ave

City: Las Vegas

Country: United States

State or Province: NV

ZIP/Postal Code: 89141

Email Address: devenhubbard@yahoo.com

Organization Name:

Comment: I am writing to request that the FCC not implement rules that would take away the ability of users to install software of their choosing on devices they own.

I use DDWRT, Linux, and other computing software that is not developed, or offered by as a corporate product on a device, and thus requires that the devices that these softwares run on must be updated during the installation. I do this to get better performance, better reliability, more features, and through the open source community a practical method of getting bugs fixed.

Commercial products primarily serve the financial bottom line of the manufacturer, and thus bugs, poor user interfaces, lack of features, and security concerns are a lower, and sometimes nonexistent priority.

The FCC's proposal is far too broad, and has widespread consequences beyond the direct interest of the FCC to be reasonable.

It's not in the public interest to cripple open source development on products that happen to have the ability to broadcast. A certain amount of personel responsiblity and enforcement is a much more appropriate balance in a demacracy than physically preventing all possible undesirable circumstances to occur.

I am writing to request that the FCC not implement rules that would take away the ability of users to install software of their choosing on devices they own.

I use DDWRT, Linux, and other computing software that is not developed, or offered by as a corporate product on a device, and thus requires that the devices that these softwares run on must be updated during the installation. I do this to get better performance, better reliability, more features, and through the open source community a practical method of getting bugs fixed.

Commercial products primarily serve the financial bottom line of the manufacturer, and thus bugs, poor user interfaces, lack of features, and security concerns are a lower, and sometimes nonexistent priority.

The FCC's proposal is far too broad, and has widespread consequences beyond the direct interest of the FCC to be reasonable.

It's not in the public interest to cripple open source development on products that happen to have the ability to broadcast.

A certain amount of personal responsibility and enforcement is a much more appropriate balance in a democracy than physically preventing all possible undesirable circumstances to occur.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Daniel

Last Name: Dobkin

Mailing Address: 877 Sutter Ave.

City: Sunnyvale

Country: United States

State or Province: CA

ZIP/Postal Code: 94086-7549

Email Address: dan@enigmatic-consulting.com

Organization Name: Enigmatics

Comment: Folks: with regard to 2.1033...

The FCC should move very cautiously in requiring that manufacturers block third-party access to equipment. Open-source software is one of the most important social and commercial trends of the last two decades, and one of the few trends that does not enhance concentration of wealth. Legal purchasers of equipment should have legal access to that equipment's capabilities.

I am old enough to remember the days when "non-standard" connectors were required on antennas in a futile attempt to prevent field modification. Field modifications occurred, but catastrophes did not result. Most user equipment to which the proposed standards would apply will be operating in the 2.4 GHz or 5 GHz unlicensed bands, and is under 1 W transmitted power. Propagation characteristics in most environments limit range to a few tens of meters, and thus the possibility of interference with other users is modest and localized. The necessity for any regulatory intervention under these circumstances is questionable. Make sure there is a problem before you impose a drastic and inappropriate solution.

Thanks for your consideration.

--Daniel M. Dobkin

Folks: with regard to 2.1033...

The FCC should move very cautiously in requiring that manufacturers block third-party access to equipment. Open-source software is one of the most important social and commercial trends of the last two decades, and one of the few trends that does not enhance concentration of wealth. Legal purchasers of equipment should have legal access to that equipment's capabilities.

I am old enough to remember the days when "non-standard" connectors were required on antennas in a futile attempt to prevent field modification. Field modifications occurred, but catastrophes did not result. Most user equipment to which the proposed standards would apply will be operating in the 2.4 GHz or 5 GHz unlicensed bands, and is under 1 W transmitted power. Propagation characteristics in most environments limit range to a few tens of meters, and thus the possibility of interference with other users is modest and localized. The necessity for any regulatory intervention under these circumstances is questionable. Make sure there is a problem before you impose a drastic and inappropriate solution.

Thanks for your consideration.

--Daniel M. Dobkin

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: Maxwell

Last Name: Brickner

Mailing Address: 520 Clifton Ave

City: Findlay

Country: United States

State or Province: OH

ZIP/Postal Code: 45840

Email Address:

Organization Name:

Comment: Please do not implement restrictions on general computing devices in ways which are intrusive and harm user freedom. It's very important to keep our wireless devices operating as intended and prevent interference with emergency infrastructure, but this is not the way to do it. It currently takes a knowledgeable and determined individual to modify their devices to create interference. I do not believe these restrictions on the general population will deter these people at all. It may even goad them to create interference and break the law on purpose. Punish those who break the law, not innocent people.

Please do not implement restrictions on general computing devices in ways which are intrusive and harm user freedom. It's very important to keep our wireless devices operating as intended and prevent interference with emergency infrastructure, but this is not the way to do it. It currently takes a knowledgeable and determined individual to modify their devices to create interference. I do not believe these restrictions on the general population will deter these people at all. It may even goad them to create interference and break the law on purpose. Punish those who break the law, not innocent people.

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: Soley

Mailing Address: 1190 Archer Way

City: Campbell

Country: United States

State or Province: CA

ZIP/Postal Code: 95008

Email Address: n6igf@wrs.soley.org

Organization Name: null

Comment: Some accommodation needs to be made to allow end users to replace or modify software that controls the non-regulated functionality of devices such as wireless routers provided that the modification does not alter the behavior of the regulated functions. For example, I should be able to add new features to the user interface or firewall of my wireless router, since these functions are not regulated and do not affect regulated functions.

The problem is that many devices combine the software the controls regulated functions with that which controls non-regulated functions. If the manufacturer incorporates technical controls (such as strictly enforced code signing) that prevents all modification then this will have a chilling effect on innovation and infringe on the rights of the property owner.

Some accommodation needs to be made to allow end users to replace or modify software that controls the non-regulated functionality of devices such as wireless routers provided that the modification does not alter the behavior of the regulated functions. For example, I should be able to add new features to the user interface or firewall of my wireless router, since these functions are not regulated and do not affect regulated functions.

The problem is that many devices combine the software the controls regulated functions with that which controls non-regulated functions. If the manufacturer incorporates technical controls (such as strictly enforced code signing) that prevents all modification then this will have a chilling effect on innovation and infringe on the rights of the property owner.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Cornwall

Mailing Address: 1243 E Sunburst Ln

City: Tempe

Country: United States

State or Province: AZ

ZIP/Postal Code: 85284

Email Address:

Organization Name:

Comment: See attached file(s)

See attached file(s)

I am concerned that parts of this NPRM are over-broad, and might have unintended consequences that result in a loss of technical ability in the United States.

Section 2.1033 Application for grant of certification. Paragraph 4(i), states "The description must state which parties will be authorized to make software changes (e.g., the grantee, wireless service providers, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation."

Such a complete lockdown on part 15 devices would preclude part 97 experimentation with devices, such as the current Broadband-Hamnet project. It would also in all likelihood prevent users from changing non-RF-specific parts of the firmware for reasons unrelated to the FCC (for example, by flashing a router with DD-WRT - which might not affect any RF).

Further, section 2.1042 Certified modular transmitters states that "Manufacturers of any radio including certified modular transmitters which includes a software defined radio must take steps to ensure that only software that has been approved with a particular radio can be loaded into that radio." This appears to mean that open source development of (for instance) drivers for wifi chipsets that are included in a modular device would be prohibited. The current state of open source wifi development is done on a per-chip basis rather than a per-device basis. This would appear to stifle such development except by the vendor.

This NPRM seems to be taking a "throw the baby out with the bathwater" approach. It's understandable that the FCC doesn't want people to use the 2.4 GHz wifi channel 14, but doing that by locking down all hardware and preventing anyone but the vendor from modifying it seems like a recipe for fiasco an order of magnitude larger than the ban of DA 97-1440, and will result in increased cost for manufacturers, decreased choice for American consumers, and further use of unregulated devices imported via the grey market - precisely not what the FCC presumably intends.

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: Barecki

Mailing Address: 2015 Lee

City: Wyoming

Country: United States

State or Province: MI

ZIP/Postal Code: 49519

Email Address: shoot40@gmail.com

Organization Name: N/A

Comment: WiFi technology should be kept unrestricted as it is.

WiFi technology should be kept unrestricted as it is.

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: maxwell

Last Name: bryan

Mailing Address: 1510 lakeside ridge drive

City: sand springs

Country: United States

State or Province: OK

ZIP/Postal Code: 74063

Email Address: maxad11@live.com

Organization Name:

Comment: Please do not implement changes that would take away a users ability to change the software of a device that they own. It would be a tragic blow the freedoms we have in the U.S. 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 changes that would take away a users ability to change the software of a device that they own. It would be a tragic blow the freedoms we have in the U.S. 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: David

Last Name: Kochendorfer

Mailing Address: 4285 Boulder Creek Circle

City: Stockton

Country: United States

State or Province: CA

ZIP/Postal Code: 95219

Email Address: david.kochendorfer@gmail.com

Organization Name: Self

Comment: I am very disturbed at this ruling which will severely constrain or prohibit my ability to load new or updated firmware on the devices that I own.

This is simply unacceptable.

Thank you

I am very disturbed at this ruling which will severely constrain or prohibit my ability to load new or updated firmware on the devices that I own.

This is simply unacceptable.

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: Paul

Last Name: Mullin

Mailing Address: PO Box 348

City: Maunaloa

Country: United States

State or Province: HI

ZIP/Postal Code: 96770-0348

Email Address: wh7qq.hi@gmail.com

Organization Name:

Comment: I am an amateur radio operator, callsign WH7QQ and I use personal computers on a network in my home which are connected to a satellite internet provider. As a ham, I am very aware that use of unnecessary transmitting power provides little/no help in improving communications because it does nothing to enhance the ability to receive and both transmission and reception are the basis of two way communication. It also raises the likelihood of creating harmful interference to other legitimate operators. Out of band transmission is unacceptable due to the potential for interference to other services.

As a computer user, I am painfully aware of the need for constantly maintaining updated firmware in my router to keep ahead of hackers who would compromise the security of my network. I am also aware that router manufacturers are frequently lax in providing firmware updates that address security flaws such as the OpenSSL bug of recent notoriety. Further, router manufacturers often do not provide firmware that addresses many needs such as adequate monitoring of data usage. These inadequacies make it necessary for router owners to upgrade the firmware in these small computers to keep them current and to address needs not served by the manufacturer. I own an ageing Belkin router that has never received a firmware upgrade after its release to sales. Belkin is not unique in totally abandoning their products after sales.

This proposed rule has the potential to prohibit firmware upgrades by users or to restrict them to the manufacturer's provided firmware when available. Manufacturers will take the path of least resistance to compliance with FCC regulation and that will result in locking out open source firmware altogether, whether or not it even addresses power output or frequency.

This proposed rule is overly broad and not sufficiently specific to keep from prohibiting any open source upgrades. It will adversely effect the security of my home network and prevent me from properly monitoring my data usage to stay within my ISP mandated usage cap.

I am an amateur radio operator, callsign WH7QQ and I use personal computers on a network in my home which are connected to a satellite internet provider. As a ham, I am very aware that use of unnecessary transmitting power provides little/no help in improving communications because it does nothing to enhance the ability to receive and both transmission and reception are the basis of two way communication. It also raises the likelihood of creating harmful interference to other legitimate operators. Out of band transmission is unacceptable due to the potential for interference to other services.

As a computer user, I am painfully aware of the need for constantly maintaining updated firmware in my router to keep ahead of hackers who would compromise the security of my network. I am also aware that router manufacturers are

frequently lax in providing firmware updates that address security flaws such as the OpenSSL bug of recent notoriety. Further, router manufacturers often do not provide firmware that addresses many needs such as adequate monitoring of data usage. These inadequacies make it necessary for router owners to upgrade the firmware in these small computers to keep them current and to address needs not served by the manufacturer. I own an ageing Belkin router that has never received a firmware upgrade after its release to sales. Belkin is not unique in totally abandoning their products after sales.

This proposed rule has the potential to prohibit firmware upgrades by users or to restrict them to the manufacturer's provided firmware when available. Manufacturers will take the path of least resistance to compliance with FCC regulation and that will result in locking out open source firmware altogether, whether or not it even addresses power output or frequency.

This proposed rule is overly broad and not sufficiently specific to keep from prohibiting any open source upgrades. It will adversely effect the security of my home network and prevent me from properly monitoring my data usage to stay within my ISP mandated usage cap.

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: Brennan

Last Name: Fee

Mailing Address: 12224 NE 8TH ST APT 304

City: BELLEVUE

Country: United States

State or Province: WA

ZIP/Postal Code: 98005

Email Address:

Organization Name:

Comment: I have long believed that in order to curb peoples rights we need a compelling reason. So, my only question to the FCC and those proposing laws like this is: why? I see benefits to the business who will be able to control and monopolize their customers more. I see governments being able to control the populace more. But what benefit to the users? None that I can see. When we curb rights it needs to be for the benefit of the many not the few. It needs to benefit the interests of the people not the interests of business or government.

So, in short please think and answer why should we do this? We should ALWAYS air on the side of openness and transparency unless there is a compelling reason that benefits all (not just some).

I have long believed that in order to curb peoples rights we need a compelling reason. So, my only question to the FCC and those proposing laws like this is: why? I see benefits to the business who will be able to control and monopolize their customers more. I see governments being able to control the populace more. But what benefit to the users? None that I can see. When we curb rights it needs to be for the benefit of the many not the few. It needs to benefit the interests of the people not the interests of business or government.

So, in short please think and answer why should we do this? We should ALWAYS air on the side of openness and transparency unless there is a compelling reason that benefits all (not just some).

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: London

Mailing Address: 321 Park Ave.

City: Salt Lake City

Country: United States

State or Province: UT

ZIP/Postal Code: 84111

Email Address:

Organization Name:

Comment: I have a Netgear 6200 wireless router, and I had problems with it crashing. Waited a full year for Netgear to fix it after I complained. They never addressed the problem. I switched to DD-WRT on that same piece of hardware. It fixed the problem and I have more features. I love DD-WRT.

I want the freedom to reprogram my devices to serve MY needs. ATT only sells phones that come with bloatware and spyware. Where is the freedom in that?

Please choose to empower the individual by supporting the reprogramming of our devices.

I have a Netgear 6200 wireless router, and I had problems with it crashing. Waited a full year for Netgear to fix it after I complained. They never addressed the problem. I switched to DD-WRT on that same piece of hardware. It fixed the problem and I have more features. I love DD-WRT.

I want the freedom to reprogram my devices to serve MY needs. ATT only sells phones that come with bloatware and spyware. Where is the freedom in that?

Please choose to empower the individual by supporting the reprogramming of our 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: Robert

Last Name: Jones

Mailing Address: 2393 Dusan St.

City: Simi Valley

Country: United States

State or Province: CA

ZIP/Postal Code: 93065

Email Address:

Organization Name:

Comment: I am writing to voice my opposition to the proposed rule that would disallow the use of custom firmware on wireless enabled devices. As an amateur license holder, I understand that the obligation to operate within the FCC rules falls to the owner/operator of the radio device, and as such, so does the ability to experiment on that device while staying within the rules. A blanket ban on the use of experimental software on a radio device violates the spirit that has made amateur radio such a benefit to the communications world, and would greatly hamper the development of new and exciting technologies. Please leave the current rules in place, and continue to let the operator of radio devices bear the responsibility of operating legally.

I am writing to voice my opposition to the proposed rule that would disallow the use of custom firmware on wireless enabled devices. As an amateur license holder, I understand that the obligation to operate within the FCC rules falls to the owner/operator of the radio device, and as such, so does the ability to experiment on that device while staying within the rules. A blanket ban on the use of experimental software on a radio device violates the spirit that has made amateur radio such a benefit to the communications world, and would greatly hamper the development of new and exciting technologies. Please leave the current rules in place, and continue to let the operator of radio devices bear the responsibility of operating legally.

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: Bryant

Mailing Address: 21530 Pine Arbor Way

City: Cypress

Country: United States

State or Province: TX

ZIP/Postal Code: 77433

Email Address:

Organization Name:

Comment: Against regulating WIFI routers, endpoints, devices.

It is unconscionable that the FCC would consider this level of regulation. However well intended the agency may be, this regulation will put a regulatory burden on many devices unintentionally. This type of regulation can lead to ambiguity in the internet device market and will drive out innovation as some developers may choose to leave this space rather than need to comply with unnecessary regulation.

Stop now...

No need to regulate, dangerous to regulate.

Against regulating WIFI routers, endpoints, devices.

It is unconscionable that the FCC would consider this level of regulation. However well intended the agency may be, this regulation will put a regulatory burden on many devices unintentionally. This type of regulation can lead to ambiguity in the internet device market and will drive out innovation as some developers may choose to leave this space rather than need to comply with unnecessary regulation.

Stop now...

No need to regulate, dangerous to regulate.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eric

Last Name: Driggs

Mailing Address: 21200 Kittridge Street

City: Canoga Park

Country: United States

State or Province: CA

ZIP/Postal Code: 91303

Email Address: edriggs@gmail.com

Organization Name:

Comment: Please do not prevent flashing of custom firmware onto routers.

The router software which comes by default on most routers is lacking both in functionality and security. A router is another type of computer. Preventing people from loading their own firmware on their router is like prevent people from installing their own operating system on their computer.

This is an especially bad law because it is proscribing a tool instead of prohibiting an action. If there are concerns about behavior in the 5ghz spectrum, simply make clear what rules have to obeyed. This would be consistent which the regulations the FCC has in place for other electronic devices.

Don't ban the tool. Regulate behavior.

Please do not prevent flashing of custom firmware onto routers.

The router software which comes by default on most routers is lacking both in functionality and security. A router is another type of computer. Preventing people from loading their own firmware on their router is like prevent people from installing their own operating system on their computer.

This is an especially bad law because it is proscribing a tool instead of prohibiting an action. If there are concerns about behavior in the 5ghz spectrum, simply make clear what rules have to obeyed. This would be consistent which the regulations the FCC has in place for other electronic devices.

Don't ban the tool. Regulate behavior.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Brian

Last Name: Cohen

Mailing Address: 9800 Bridleridge Ct

City: Vienna

Country: United States

State or Province: VA

ZIP/Postal Code: 22181

Email Address: brian.cohen.88@gmail.com

Organization Name: Independent Contractor

Comment: I work with wireless technologies, and fear that the current version of this proposal would negatively affect innovation, as preventing modifying software carries with it great costs for the end-user, and limits the repurposing existing technologies. It would be extremely wasteful for hardware to die with the firmware it was installed with in a fast-paced world. And it won't be long until proof-carrying code checked by hardware makes it possible to accomplish the same goals as these proposed rules without the need of additional certification and explicit permission, which slows the process of experimentation to a halt.

I work with wireless technologies, and fear that the current version of this proposal would negatively affect innovation, as preventing modifying software carries with it great costs for the end-user, and limits the repurposing existing technologies. It would be extremely wasteful for hardware to die with the firmware it was installed with in a fast-paced world. And it won't be long until proof-carrying code checked by hardware makes it possible to accomplish the same goals as these proposed rules without the need of additional certification and explicit permission, which slows the process of experimentation to a halt.

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: Matthew

Last Name: Hirsch

Mailing Address: 18 Mansfield St. Apt. 2

City: Somerville

Country: United States

State or Province: MA

ZIP/Postal Code: 02143

Email Address: matthew.hirsch@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. I am the founder of a technology company, and creating additional barriers to innovation in a fast-paced field is bad for American interests, and bad for technological progress.

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. I am the founder of a technology company, and creating additional barriers to innovation in a fast-paced field is bad for American interests, and bad for technological progress.

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: John

Last Name: Pell

Mailing Address: PO Box 94047

City: Pasadena

Country: United States

State or Province: CA

ZIP/Postal Code: 91109

Email Address: John+FCC@gaelicWizard.net

Organization Name: gaelicWizard.llc

Comment: I strongly object to this proposal. I am an Information Technology administrator for several small/medium healthcare providers and I regularly install "modified" firmware on my WiFi devices at work and at home. The manufacturer-provided firmware is often sorely lacking in several dimensions, not least of which is security. By using open-source firmware, I can ensure that my businesses do not leak Patient Health Information through improper/unpatched security failures. Often, I seek to *reduce* the transmission power of my access points to improve interoperability within the facility. Banning firmware modification is short-sighted and quite-frankly unacceptable.

I strongly object to this proposal. I am an Information Technology administrator for several small/medium healthcare providers and I regularly install "modified" firmware on my WiFi devices at work and at home. The manufacturer-provided firmware is often sorely lacking in several dimensions, not least of which is security. By using open-source firmware, I can ensure that my businesses do not leak Patient Health Information through improper/unpatched security failures. Often, I seek to *reduce* the transmission power of my access points to improve interoperability within the facility. Banning firmware modification is short-sighted and quite-frankly unacceptable.

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: george

Last Name: walton

Mailing Address: 29309 204th pl se

City: kent

Country: United States

State or Province: WA

ZIP/Postal Code: 98042

Email Address: georgeawalton@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: Martin

Last Name: Fried

Mailing Address: 768 Duke Circle

City: Pleasant Hill

Country: United States

State or Province: CA

ZIP/Postal Code: 94523

Email Address: martinjfried@gmail.com

Organization Name: retired

Comment: I am writing to urge you not to take away my ability to use my wireless devices in the way I see fit, assuming I do not break any laws in doing so.

I personally use 3rd party firmware in my router now for a few reasons.

1. The router itself was a very good price, but the existing firmware was almost painful to use. Some pages would constantly refresh, causing information being entered to disappear, and making the page "flash" repeatedly. I have found that many time, a hardware manufacturer might make a fine piece of hardware, but fail at making good software for the device.
2. Some of the advertised features did not work very well.
3. For a while, there was a bug that allowed unauthorized third-party users to gain control of the device, and it took a while for the manufacturer to come out with a fix.

By installing open-source firmware (DD-WRT) on my router (TP-Link), I now have a very usable router rather than a big disappointment and waste of money. Please don't take this feature away from me.

I am writing to urge you not to take away my ability to use my wireless devices in the way I see fit, assuming I do not break any laws in doing so.

I personally use 3rd party firmware in my router now for a few reasons.

1. The router itself was a very good price, but the existing firmware was almost painful to use. Some pages would constantly refresh, causing information being entered to disappear, and making the page "flash" repeatedly. I have found that many time, a hardware manufacturer might make a fine piece of hardware, but fail at making good software for the device.
2. Some of the advertised features did not work very well.
3. For a while, there was a bug that allowed unauthorized third-party users to gain control of the device, and it took a while for the manufacturer to come out with a fix.

By installing open-source firmware (DD-WRT) on my router (TP-Link), I now have a very usable router rather than a big disappointment and waste of money. Please don't take this feature away from me.

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: Jonathan

Last Name: Younessian

Mailing Address: 1310 K Street S.E.

City: Washington

Country: United States

State or Province: DC

ZIP/Postal Code: 20003

Email Address: jon.youne@gmail.com

Organization Name:

Comment: Software defined radios are too vaguely defined. The concept of a wireless device is not limited to wireless internet access points.

Mobile ad hoc network seen in areas where governments have disrupted normal Wi-Fi and GSM communications rely on open hardware and software defined radios to restore communication.

Without these ad hoc mesh networks the disruption of free speech is just as simple as turning off the devices protected in this proposal.

Within the scope proposed I believe Equipment Authorization and Electronic Labeling for Wireless Devices will violate the First and Second Amendments of the US Constitution in even the lightest restrictions.

Our ability peacefully assemble, report on actions taken by governments, and communicate to our loved ones depend on protecting the use of software defined radios from US government restrictions.

Software defined radios are too vaguely defined. The concept of a wireless device is not limited to wireless internet access points.

Mobile ad hoc network seen in areas where governments have disrupted normal Wi-Fi and GSM communications rely on open hardware and software defined radios to restore communication.

Without these ad hoc mesh networks the disruption of free speech is just as simple as turning off the devices protected in this proposal.

Within the scope proposed I believe Equipment Authorization and Electronic Labeling for Wireless Devices will violate the First and Second Amendments of the US Constitution in even the lightest restrictions.

Our ability peacefully assemble, report on actions taken by governments, and communicate to our loved ones depend on protecting the use of software defined radios from US government restrictions.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Samiul

Last Name: Islam

Mailing Address: Fulbari Gate

City: Khulna

Country: Bangladesh

State or Province: Khulna

ZIP/Postal Code: 9203

Email Address: samikuet10@gmail.com

Organization Name: KUET

Comment: "I object this because security and privacy is *important* to me."

"I object this because security and privacy is *important* to me."

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: Brooks

Last Name: Clemans

Mailing Address: 59 Peabody Drive

City: brentwood

Country: United States

State or Province: NH

ZIP/Postal Code: 03833

Email Address:

Organization Name:

Comment: I, Brooks Clemans, 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. Additionally:

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 for your time.

I, Brooks Clemans, 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. Additionally:

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 for your time.