

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: Aaron

Last Name: Curley

Mailing Address: 2676 Newhall St, Apt 25

City: Santa Clara

Country: United States

State or Province: CA

ZIP/Postal Code: 95050

Email Address: accwebs@gmail.com

Organization Name: N/A

Comment: Good afternoon,

I respectfully and strongly request that the FCC avoid implementing any rules that take away the rights of individuals to manage and control the computing devices that they have purchased and own. This includes allowing users to install the software of their choosing on equipment such routers, laptops, cellular phones, etc.

In particular, I am gravely concerned that the proposed rules would ban all custom open source firmwares for home networked (e.g. Wi-Fi) devices. This would result in a substantial increase in network device manufacturers' power over their customers' security and data.

As you are aware, many home network device manufacturers presently do a VERY poor job of securing the default firmware on the home network devices they sell. Worse still, in the past (and likely still continuing in the present) many manufacturers have shipped devices with firmware containing deliberate "back doors" (e.g. hard-coded passwords, hidden listening services, and services with silent "phone home" logic) that allow attackers to silently enter and compromise a user's systems and personal data. Such security issues (whether they are deliberate or accidental) are frequently easy to discover, making the issues ripe for exploitation by malicious parties. In addition to having security problems, the default network device firmwares are frequently of poor quality & reliability (e.g. randomly requiring power-cycles when they "lock up", or not supporting commonly-required features).

Up until now, Americans have had the ability to solve the aforementioned issues by switching to an alternative firmware for many common devices. The open source community has been especially helpful in this regard, producing many quality projects (e.g. OpenWRT, Tomato) that give users an alternative choice of software for the devices they have purchased.

The widespread availability of custom home network device firmware has substantially improved a major imbalance of power between the buyer and the home network device manufacturer. Due to the rapid device model turnover in the current market, when a buyer is initially purchasing a home network device, it is VERY difficult for that buyer to judge the security and functionality of the devices that are available at that time. This is because such issues (security ones, especially) are frequently not known yet. At present, when issues are inevitably discovered, should manufacturers be unwilling or unable to solve the issues, users are able to solve those problems on their own by switching to an alternative software. I, personally, have used this approach many times.

If this ability is now taken away through the banning of custom firmwares, once the buyer has purchased the device (and security/functionality issues are identified later), they are now at the "mercy" of the device manufacturer, who may not

(and likely will not) actually care to fix such issues, especially after the devices are a few years old.

Most (if not all) third party network device firmware projects promote lawful use of the devices using their software. I would like to reiterate that the consumers of these open source firmwares are generally NOT deviants trying to abuse the wireless spectrum in their vicinity at the expense of all others; instead, consumers of third party firmwares are typically individuals trying to improve upon the reliability, security, and functionality of the computing devices they own.

Please amend the proposed rules to ensure that users retain the ability to control and choose the software they run on their personally-owned devices.

Thank you for your time and attention to my concerns.

Respectfully,  
Aaron Curley

Good afternoon,

I respectfully and strongly request that the FCC avoid implementing any rules that take away the rights of individuals to manage and control the computing devices that they have purchased and own. This includes allowing users to install the software of their choosing on equipment such routers, laptops, cellular phones, etc.

In particular, I am gravely concerned that the proposed rules would ban all custom open source firmwares for home networked (e.g. Wi-Fi) devices. This would result in a substantial increase in network device manufacturers' power over their customers' security and data.

As you are aware, many home network device manufacturers presently do a VERY poor job of securing the default firmware on the home network devices they sell. Worse still, in the past (and likely still continuing in the present) many manufacturers have shipped devices with firmware containing deliberate "back doors" (e.g. hard-coded passwords, hidden listening services, and services with silent "phone home" logic) that allow attackers to silently enter and compromise a user's systems and personal data. Such security issues (whether they are deliberate or accidental) are frequently easy to discover, making the issues ripe for exploitation by malicious parties. In addition to having security problems, the default network device firmwares are frequently of poor quality & reliability (e.g. randomly requiring power-cycles when they "lock up", or not supporting commonly-required features).

Up until now, Americans have had the ability to solve the aforementioned issues by switching to an alternative firmware for many common devices. The open source community has been especially helpful in this regard, producing many quality projects (e.g. OpenWRT, Tomato) that give users an alternative choice of software for the devices they have purchased.

The widespread availability of custom home network device firmware has substantially improved a major imbalance of power between the buyer and the home network device manufacturer. Due to the rapid device model turnover in the current market, when a buyer is initially purchasing a home network device, it is VERY difficult for that buyer to judge the security and functionality of the devices that are available at that time. This is because such issues (security ones, especially) are frequently not known yet. At present, when issues are inevitably discovered, should manufacturers be unwilling or unable to solve the issues, users are able to solve those problems on their own by switching to an alternative software. I, personally, have used this approach many times.

If this ability is now taken away through the banning of custom firmwares, once the buyer has purchased the device (and security/functionality issues are identified later), they are now at the "mercy" of the device manufacturer, who may not (and likely will not) actually care to fix such issues, especially after the devices are a few years old.

Most (if not all) third party network device firmware projects promote lawful use of the devices using their software. I would like to reiterate that the consumers of these open source firmwares are generally NOT deviants trying to abuse the wireless spectrum in their vicinity at the expense of all others; instead, consumers of third party firmwares are typically

individuals trying to improve upon the reliability, security, and functionality of the computing devices they own.

Please amend the proposed rules to ensure that users retain the ability to control and choose the software they run on their personally-owned devices.

Thank you for your time and attention to my concerns.

Respectfully,  
Aaron Curley

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: Parker

Last Name: Mathews

Mailing Address: 2110 James St

City: Bellingham

Country: United States

State or Province: WA

ZIP/Postal Code: 98248

Email Address:

Organization Name:

Comment: Please DO NOT require device manufacturers to implement security restricting the flashing of firmware. This would likely prevent consumers from being able to install alternative operating systems on the computers they own among many other reasons.

Again I'm asking you not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Please DO NOT require device manufacturers to implement security restricting the flashing of firmware. This would likely prevent consumers from being able to install alternative operating systems on the computers they own among many other reasons.

Again I'm asking you not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Richard

Last Name: Brown

Mailing Address: 84 Orford Road

City: Lyme

Country: United States

State or Province: NH

ZIP/Postal Code: 03768

Email Address: richb.hanover@gmail.com

Organization Name: Blueberry Hill Software

Comment: I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for "consumer routers."

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This "lock down" would prevent modification to the radio's power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168>. The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturer's seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq\_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt>. The result of this multi-year effort was a major advance in performance for all routers. The fq\_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as

test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) I would incorporate into my comments all the other "talking points" listed on the Save WiFi page at: [https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi)

5) Finally, I want to address the FCC's original concern - that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused any actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve America's airwaves.

I recommend that the FCC RESCIND its Proposed Rule, Document number 2015-18402 regarding wireless devices. The Proposed Rule is overbroad, would harm many communities of Americans, and is not warranted by the facts on the ground.

Although the FCC has the power to regulate equipment that generates radio frequencies, this is a heavy-handed rule that could be addressed other ways. Specifically, I am concerned about the ability of third parties to modify and create new firmware for "consumer routers."

The proposed rule would require that router manufacturers lock down the RF portion of the router to obtain FCC approval. This "lock down" would prevent modification to the radio's power, frequencies, etc to prevent it from radiating outside the specified limits. This is a laudable goal, but the application of this rule as written would result in undesirable consequences.

In practice, most radio functions are very tightly wedded to all the other factors of the hardware/software. The most likely way manufacturers would likely lock down the RF operation would be to make it impossible to modify any of the code in the routers.

There would be a number of adverse consequences both for me personally, to consumers in the US, and the networking industry. These consequences can be ameliorated by allowing the owners of routers to install their own code.

1) Security of the router. It is well known that vendor-supplied firmware for consumer routers often contain flaws. Just last week, the CERT released knowledge of a vulnerability to Belkin routers. See <http://www.kb.cert.org/vuls/id/201168>. The ability to install well-tested, secure firmware into a router benefits all consumers. The ability for a person to update their own router on a regular basis (as opposed to many manufacturer's seemingly lackadaisical schedule) preserves security.

2) Research into the field of computer networking. Non-traditional research efforts (outside academia) lead to real improvements in the state of computer networking. An example is the CeroWrt project that developed the fq\_codel algorithm. <http://www.bufferbloat.net/projects/cerowrt> The result of this multi-year effort was a major advance in performance for all routers. The fq\_codel code has been accepted into the Linux kernel and now runs in hundreds of millions of devices. As a member of the team that worked on this, I assert that without the ease of modification of a consumer router to prove out the ideas, this improvement would not have occurred.

3) Personal learning environments. Individuals, as well as network professionals, often use these consumer routers as test beds for increased understanding of network operation. Losing the ability to reprogram the router would make it more expensive, if not prohibitive, for Americans to improve their knowledge and become more competitive.

4) I would incorporate into my comments all the other "talking points" listed on the Save WiFi page at:

[https://libreplanet.org/wiki/Save\\_WiFi](https://libreplanet.org/wiki/Save_WiFi)

5) Finally, I want to address the FCC's original concern - that these consumer routers are SDRs, and they must not be operated outside their original design parameters. While the goal of reducing radio frequency interference is important, the FCC has failed to demonstrate that the widespread practice of installing/updating firmware in consumer routers has caused any actual problems. Furthermore, the FCC can use its current enforcement powers to monitor and shut down equipment that is interfering.

Creating a broad, wide-ranging rule to address a theoretical problem harms industry and individuals, and is an overreach of the rules necessary to preserve America's airwaves.

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: Erin

Last Name: DeSpain

Mailing Address: 10828 Marsha Kaye Circle

City: Sandy

Country: United States

State or Province: UT

ZIP/Postal Code: 84070-5277

Email Address:

Organization Name:

Comment: As a user and advocate of open-source WiFi software for both myself and the businesses with whom I have relationships, I find the FCC's new proposed regulations quite worrying.

Open source software on WiFi devices is critical to meet the very specific software needs of individuals and businesses with whom I work. The functionality and flexibility the seek to have on their devices is available nowhere else to meet their specific needs.

These businesses rely on the security, transparency, and flexibility of open-source software, which can be found nowhere else, in order to help manage their businesses and better serve their customers.

Surely any unilateral ban on open-source software for WiFi devices would impose a huge cost on individuals, businesses, hobbyists, researchers, and innovators for a VERY, VERY small potential gain in standardization and functional limitation for a VERY narrowly defined purpose. A poorly written rule would be FAR FAR more harmful in the long run than the present condition of no rule at all!

Limiting the ability of users to apply open-source software to devices they own will create further risks that it will resolve because manufacturers often provide shoddy and insecure software on their WiFi devices. Some of this software contains gaping security holes that manufacturers have little and/or no incentive to fix--because consumers and manufacturers make little-nothing for providing ongoing support for devices consumers have already purchased. Even when manufacturers do have an incentive to provide limited support, there may be significant problems: 1) they may be slow in doing so--exposing the data of users to misappropriation or harm--while they wait for updates and software patches to be applied; 2) they may address some issues but may fail to resolve others that might be significantly more important to a certain segment consumers--leaving those consumers without the improvements they seek.

To prevent individuals, businesses, hobbyists, researchers and innovators from applying software updates to these devices would expose users to great harm without the ability to fix them. Furthermore manufacturers now depend heavily on the innovations, improvements, and bug-fixes that open-source software provides for their own systems--therefore limiting the application of these improvements will only damage the same manufacturers with which the FCC has relationships.

On the whole the desire to bottle-up patches, fixes, and innovations by preventing the application of open-source software improvements or updates to WiFi devices will greatly harm consumers, businesses, researchers, and innovators and eventually the manufactures themselves FAR FAR more than the harms these rules and provisions seek to prevent. A short-sighted application of draconian provisions does no good.

As a user and advocate of open-source WiFi software for both myself and the businesses with whom I have relationships, I find the FCC's new proposed regulations quite worrying.

Open source software on WiFi devices is critical to meet the very specific software needs of individuals and businesses with whom I work. The functionality and flexibility they seek to have on their devices is available nowhere else to meet their specific needs.

These businesses rely on the security, transparency, and flexibility of open-source software, which can be found nowhere else, in order to help manage their businesses and better serve their customers.

Surely any unilateral ban on open-source software for WiFi devices would impose a huge cost on individuals, businesses, hobbyists, researchers, and innovators for a VERY, VERY small potential gain in standardization and functional limitation for a VERY narrowly defined purpose. A poorly written rule would be FAR FAR more harmful in the long run than the present condition of no rule at all!

Limiting the ability of users to apply open-source software to devices they own will create further risks that it will resolve because manufacturers often provide shoddy and insecure software on their WiFi devices. Some of this software contains gaping security holes that manufacturers have little and/or no incentive to fix--because consumers and manufacturers make little-thing for providing ongoing support for devices consumers have already purchased. Even when manufacturers do have an incentive to provide limited support, there may be significant problems: 1) they may be slow in doing so--exposing the data of users to misappropriation or harm--while they wait for updates and software patches to be applied; 2) they may address some issues but may fail to resolve others that might be significantly more important to a certain segment consumers--leaving those consumers without the improvements they seek.

To prevent individuals, businesses, hobbyists, researchers and innovators from applying software updates to these devices would expose users to great harm without the ability to fix them. Furthermore manufacturers now depend heavily on the innovations, improvements, and bug-fixes that open-source software provides for their own systems--therefore limiting the application of these improvements will only damage the same manufacturers with which the FCC has relationships.

On the whole the desire to bottle-up patches, fixes, and innovations by preventing the application of open-source software improvements or updates to WiFi devices will greatly harm consumers, businesses, researchers, and innovators and eventually the manufacturers themselves FAR FAR more than the harms these rules and provisions seek to prevent. A short-sighted application of draconian provisions does no good.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Peter

Last Name: Masterson

Mailing Address: 940 E Arthur ST

City: Warsaw

Country: United States

State or Province: IN

ZIP/Postal Code: 46580

Email Address: shadowwalker78@gmail.com

Organization Name:

Comment: I am very displeased at the notion of the FCC harshly regulating a piece of consumer home electronics in this fashion. Whenever I buy something like a router, I expect the ability to be able to modify and otherwise improve the software on said device.

Commercial producers of these wireless routing devices very regularly do not put much effort into making the software of said devices open, secure, or as useful as possible to the end user. With the right to modify the software, I retain the ability to make my home network as secure as possible from those who may wish me, or my family harm and / or inconvenience / harassment from outside agencies.

Please do not go forward with these proposed rules - they are incredibly anti-consumer and take many rights and freedoms away from citizens.

Thank you for your time.

I am very displeased at the notion of the FCC harshly regulating a piece of consumer home electronics in this fashion. Whenever I buy something like a router, I expect the ability to be able to modify and otherwise improve the software on said device.

Commercial producers of these wireless routing devices very regularly do not put much effort into making the software of said devices open, secure, or as useful as possible to the end user. With the right to modify the software, I retain the ability to make my home network as secure as possible from those who may wish me, or my family harm and / or inconvenience / harassment from outside agencies.

Please do not go forward with these proposed rules - they are incredibly anti-consumer and take many rights and freedoms away from citizens.

Thank you for your time.

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: jack

Last Name: mehoff

Mailing Address: 111 ne 2nd

City: portland

Country: United States

State or Province: OR

ZIP/Postal Code: 97030

Email Address:

Organization Name:

Comment: disgusting... when government becomes a dictatorship, it is time we shut the entire thing down.

disgusting... when government becomes a dictatorship, it is time we shut the entire thing down.

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: Andy

Last Name: Yuergens

Mailing Address: 241 Wolfberry path

City: Buda

Country: United States

State or Province: TX

ZIP/Postal Code: 78610

Email Address:

Organization Name:

Comment: Please permit wireless radios to remain modifiable. Modifications can enhance specs of oem devices in ways that may not thought of during development and extends the life of older devices so no additional money may need to be specified to unnecessarily.

Thanks

Please permit wireless radios to remain modifiable. Modifications can enhance specs of oem devices in ways that may not thought of during development and extends the life of older devices so no additional money may need to be specified to unnecessarily.

Thanks

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: Berger

Mailing Address: 112 NC HWY 54

City: Carrboro

Country: United States

State or Province: NC

ZIP/Postal Code: 27510

Email Address:

Organization Name:

Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Eric

Last Name: Johansson

Mailing Address: 54 Salem St

City: Woburn

Country: United States

State or Province: MA

ZIP/Postal Code: 01801

Email Address: eric@in3x.io

Organization Name: in3x inc.

Comment: I'm an IT professional and deploy wireless access points as part of my responsibilities. For years, I've had to suffer from numerous problems caused because of buggy, unreliable vendor supplied software.

when projects such as dd-wrt and openwrt came around, I was finally able to get higher reliability and more secure software on a number of access points. This third-party software became the major deciding factor in which hardware I would purchase for personal and professional uses.

I hope the commission will not Lock up the hardware from end-user modifications but instead head the other direction. Make it possible for projects such as openwrt to get all of the information they need in order to make high-quality software with greater functionality than that provided by the hardware vendor.

I'm an IT professional and deploy wireless access points as part of my responsibilities. For years, I've had to suffer from numerous problems caused because of buggy, unreliable vendor supplied software.

when projects such as dd-wrt and openwrt came around, I was finally able to get higher reliability and more secure software on a number of access points. This third-party software became the major deciding factor in which hardware I would purchase for personal and professional uses.

I hope the commission will not Lock up the hardware from end-user modifications but instead head the other direction. Make it possible for projects such as openwrt to get all of the information they need in order to make high-quality software with greater functionality than that provided by the hardware vendor.

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: Nicolas

Last Name: Dufour

Mailing Address: 11 Burnett Terrace

City: West Orange

Country: United States

State or Province: NJ

ZIP/Postal Code: 07052

Email Address: nrdufour@gmail.com

Organization Name:

Comment: I use a router that I flashed myself with an opensource firmware. It doesn't make any sense to me to forbid this usage. It makes me safer and more aware of what the router can and can't do.

The same thing applies for any device like arduino based ones.

This non sense has to be stopped now!

I use a router that I flashed myself with an opensource firmware. It doesn't make any sense to me to forbid this usage. It makes me safer and more aware of what the router can and can't do.

The same thing applies for any device like arduino based ones.

This non sense has to be stopped now!

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: Dennis

Last Name: Cioffi

Mailing Address: 119 Walker Ave

City: West Berlin

Country: United States

State or Province: NJ

ZIP/Postal Code: 08091

Email Address: concretemannj@comcast.net

Organization Name:

Comment: I want to be able to control my own computing devices

I want to be able to control my own computing devices

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Miller, Jr.

Mailing Address: 750 Passaic Ave

City: Kearny

Country: United States

State or Province: NJ

ZIP/Postal Code: 07032

Email Address: jim@jimandbrandi.com

Organization Name:

Comment: I am writing to oppose the proposed rules as written. The ubiquity of WiFi devices in the 5Ghz range means that manufacturers widely vary in their level of support, willingness to provide timely updates, and even their continued existence to provide such support.

Most importantly, wireless networking research depends on the ability of researchers to investigate and modify their devices. Inevitable discovery of security and operating flaws mean that Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

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

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

I am writing to oppose the proposed rules as written. The ubiquity of WiFi devices in the 5Ghz range means that manufacturers widely vary in their level of support, willingness to provide timely updates, and even their continued existence to provide such support.

Most importantly, wireless networking research depends on the ability of researchers to investigate and modify their devices. Inevitable discovery of security and operating flaws mean that 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: Ashkan

Last Name: Jazayeri

Mailing Address: 2nd floor, #37, Madayen St,Khaje'abdollah, Seyedkhandan

City: Tehran

Country: Iraq

State or Province: Iran

ZIP/Postal Code: 1661777555

Email Address: ashkan@jazayeri.net

Organization Name:

Comment: Hi

As a software company we're working on opensource software projects to provide Hotspot solutions to our customers. We need to be able to maintain our devices and install our own software based on our end users needs. We're asking the FCC not to implement rules that take away our ability to install the software of our choosing on our computing devices.

Hi

As a software company we're working on opensource software projects to provide Hotspot solutions to our customers. We need to be able to maintain our devices and install our own software based on our end users needs. We're asking the FCC not to implement rules that take away our ability to install the software of our choosing on our computing devices.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Shield

Last Name: Anderson

Mailing Address: 125 West Mariposa St

City: Altadena

Country: United States

State or Province: CA

ZIP/Postal Code: 91001-4719

Email Address:

Organization Name:

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

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

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

1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Not fixing security holes either feeds cyberthreats or increases electronic waste.
5. 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: Jason

Last Name: Mervyn

Mailing Address: 22 Presidential Way

City: Hopewell Junction

Country: United States

State or Province: NY

ZIP/Postal Code: 12533

Email Address: jhmervyn@yahoo.com

Organization Name: Private citizen (Dept of Defense Education Activity)

Comment: Please strike or re-write any portions of III.B.3.b. (or related portions of the proposal) which would either:

A. criminalize so-called "jailbreaking"

or

B. infer that manufacturers must prevent modification of devices by unregistered third parties

Decisions to lock down devices should be left in the hands of the manufacturer. It ought to be up to them if they wish to allow Open Source modification to their devices. Harnessing the labor of Open Source is one of the best ways in which disadvantaged manufacturers can compete in the marketplace.

Please strike or re-write any portions of III.B.3.b. (or related portions of the proposal) which would either:

A. criminalize so-called "jailbreaking"

or

B. infer that manufacturers must prevent modification of devices by unregistered third parties

Decisions to lock down devices should be left in the hands of the manufacturer. It ought to be up to them if they wish to allow Open Source modification to their devices. Harnessing the labor of Open Source is one of the best ways in which disadvantaged manufacturers can compete in the marketplace.

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: Grinkevich

Mailing Address: 138 71ST ST APT F5

City: Brooklyn

Country: United States

State or Province: NY

ZIP/Postal Code: 11209

Email Address: danielgrinkevich@gmail.com

Organization Name: null

Comment: Public servants of the Federal Communications Commission,

I respectfully ask that the FCC does not implement this NPRM. The rules would take away the ability of Americans to install the software of their choosing on their computing devices.

There are many reasons why we need the ability to modify the software on wireless devices. Americans need the ability to fix security holes in their devices when the manufacturer stops supporting the device. In the past users have fixed serious security flaws in WiFi devices which would not be possible under this NPRM. Wireless network research depends on the ability of researchers modify and experiment their devices.

Community WiFi mesh networks would be more difficult, if not impossible to implement under these new laws. To effectively and efficiently implement a mesh network you need to load your own firmware onto devices. Mesh networks help responders in emergencies, create anonymity, and allows for a backup / alternative communications network. For example, Red Hook WiFi was able to keep users connected during hurricane Sandy.

The financial impact would be billions of dollars of commerce. There are many vendors that depend on the user's ability to install software of their choosing; secure WiFi vendors, retail hotspot vendors, and small ISPs for example.

Device manufacturers will likely take the easiest route to lock down the device to comply with the law instead of just securing the radio. Locking the user out of the device will prevent the discovery of security flaws and checking for backdoors.

I am a firmware developer for the NYC Mesh and amateur radio operator. This NOPR would make the NYC Mesh cease to exist. The project utilizes a modified version of OpenWRT that runs on low cost consumer hardware. These modifications are absolutely necessary for the NYC Mesh to exist. The radio firmware/baseband is already locked down and cannot be modified, further restrictions serve no purpose.

I urge the FCC to not adopt the NPRM as written and to explicitly allow 3rd party firmware on wireless devices.

Public servants of the Federal Communications Commission,

I respectfully ask that the FCC does not implement this NPRM. The rules would take away the ability of Americans to install the software of their choosing on their computing devices.

There are many reasons why we need the ability to modify the software on wireless devices. Americans need the ability to fix security holes in their devices when the manufacturer stops supporting the device. In the past users have fixed serious security flaws in WiFi devices which would not be possible under this NPRM. Wireless network research depends on the ability of researchers modify and experiment their devices.

Community WiFi mesh networks would be more difficult, if not impossible to implement under these new laws. To effectively and efficiently implement a mesh network you need to load your own firmware onto devices. Mesh networks help responders in emergencies, create anonymity, and allows for a backup / alternative communications network. For example, Red Hook WiFi was able to keep users connected during hurricane Sandy.

The financial impact would be billions of dollars of commerce. There are many vendors that depend on the user's ability to install software of their choosing; secure WiFi vendors, retail hotspot vendors, and small ISPs for example.

Device manufacturers will likely take the easiest route to lock down the device to comply with the law instead of just securing the radio. Locking the user out of the device will prevent the discovery of security flaws and checking for backdoors.

I am a firmware developer for the NYC Mesh and amateur radio operator. This NOPR would make the NYC Mesh cease to exist. The project utilizes a modified version of OpenWRT that runs on low cost consumer hardware. These modifications are absolutely necessary for the NYC Mesh to exist. The radio firmware/baseband is already locked down and cannot be modified, further restrictions serve no purpose.

I urge the FCC to not adopt the NPRM as written and to explicitly allow 3rd party firmware on wireless 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: Richard

Last Name: Maio

Mailing Address: 25 Warehouse Creek Lane

City: Edgewater

Country: United States

State or Province: MD

ZIP/Postal Code: 21037

Email Address: ww3r,maio@gmail.com

Organization Name: Anne Arundel Radio Club

Comment: In general, there is no recognition of legitimate changes to equipment for licensed services, particularly amateur radio. Since the frequencies between 5.65 and 5.85 GHz in section 2.1033(b)(10) fall within the 5.65 to 5.925 GHz amateur allocation, it is important to note the differences between these rules and allowed activities under Part 97. Many innovations in communications have been started in the amateur community as part of our activities to advance the art and science of wireless communications. The ability to add functionality via a software download allows end users to improve capabilities without replacing hardware. For wireless devices, this means, among other things, the ability to fix or improve security to ensure that others can't access the equipment, or to create new capabilities where none existed before. For amateur operators in particular, the inability to download new firmware to a device would prevent using existing hardware for experimentation or advancing the art and science of wireless communications. These are core tenets of the amateur radio community and would cause undue hardship in that portion of our allocated spectrum. Streamlining the rules is good as is responding to new technologies, but it should not be at the expense of creating future capabilities.

In general, there is no recognition of legitimate changes to equipment for licensed services, particularly amateur radio. Since the frequencies between 5.65 and 5.85 GHz in section 2.1033(b)(10) fall within the 5.65 to 5.925 GHz amateur allocation, it is important to note the differences between these rules and allowed activities under Part 97. Many innovations in communications have been started in the amateur community as part of our activities to advance the art and science of wireless communications. The ability to add functionality via a software download allows end users to improve capabilities without replacing hardware. For wireless devices, this means, among other things, the ability to fix or improve security to ensure that others can't access the equipment, or to create new capabilities where none existed before. For amateur operators in particular, the inability to download new firmware to a device would prevent using existing hardware for experimentation or advancing the art and science of wireless communications. These are core tenets of the amateur radio community and would cause undue hardship in that portion of our allocated spectrum. Streamlining the rules is good as is responding to new technologies, but it should not be at the expense of creating future capabilities.

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: Hovemeyer

Mailing Address: 357 Edgehill Rd

City: York

Country: United States

State or Province: PA

ZIP/Postal Code: 17403

Email Address: david.hovemeyer@gmail.com

Organization Name:

Comment: Please do not prohibit users of wireless devices from installing their own firmware. For example, the firmware provided by vendors of wireless routers often is buggy, has security vulnerabilities, and lacks features such as QoS. Allowing users of these devices to install custom firmware (such as DD-WRT) allows them to address these limitations.

The security issues with vendor firmware are a particularly important issue, leaving users exposed to online attacks which could lead to exposure of personal and financial information.

Please do not prohibit users of wireless devices from installing their own firmware. For example, the firmware provided by vendors of wireless routers often is buggy, has security vulnerabilities, and lacks features such as QoS. Allowing users of these devices to install custom firmware (such as DD-WRT) allows them to address these limitations.

The security issues with vendor firmware are a particularly important issue, leaving users exposed to online attacks which could lead to exposure of personal and financial information.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Whipple

Mailing Address: 92 river dr

City: Naples

Country: United States

State or Province: FL

ZIP/Postal Code: 34112

Email Address: cm0n3y34@gmail.com

Organization Name:

Comment: Please do not implement this proposed rule. This is far too widely restrictive and honestly, frightening. Wireless networking research depends on the ability of researchers to investigate and modify their devices, meaning progress in wireless technology will come to a complete stop.

We also need the ability to fix security holes in our 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 these rules. Not fixing security holes either feeds cyber-threats or increases electronic waste. Both are less than ideal.

Billions of dollars of commerce, such as secure WiFi vendors, retail hotspot vendors, depend on the ability of users and companies to install the software of their choosing. Without this ability, these technologies could not exist any longer.

Furthermore, these rules will restrict activities such as the installation custom firmware and operating systems on computers and phones, which add features, fix problems, etc. Without this, computer's potential, and by proxy, their ownership will be limited to the company providing the operating system. With Microsoft Windows 10's issues and telemetry, this proposed rule will effectively make Microsoft a spying organization, with total control of all non-apple computers.

I have moved Windows from all of my systems to a secondary role, under various Linux-based OSes. (This made them faster, and more capable, on top of the fact that Microsoft doesn't get to see every keystroke, every click, every file on my computer and storage devices. )

Open source is what has, and continues to, make the technology industries what they are today. Even now, Apple and Microsoft increasingly rely on open source software to improve their own software. These rules would effectively kill open source. (At least on anything with WiFi, which is most computers and all portable devices.) It is important to note that many industries rely on open-source to some degree, and this proposed rule would destroy this, potentially having a severe effect on those industries and even our economy as a whole.

I would sooner remove all of my wireless cards than give my ownership of my devices to the government, Microsoft, etc. And I'm sure many feel the same.

One key aspect of owning a device is the ability to make changes to it, modify it at the hardware and software levels, provided the device is kept within the restrictions of regulations (many of which are currently in place to prevent health issues, interference, and interrupting important communications, such as those by police, military, medical, etc. By implementing this rule, you would be taking ownership of every phone, computer, router, modem, tablet, even modern versions of appliances such as refrigerators and washing machines, away from Americans.

As a technician, network support student, and software/hardware design hobbyist, I humbly ask that you reconsider this rule. It will have severe repercussions in the technology industry, and by proxy, every other industry that uses some kind of electronic device.

Please do not destroy wireless technology with this rule.

Please do not implement this proposed rule. This is far too widely restrictive and honestly, frightening. Wireless networking research depends on the ability of researchers to investigate and modify their devices, meaning progress in wireless technology will come to a complete stop.

We also need the ability to fix security holes in our 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 these rules. Not fixing security holes either feeds cyber-threats or increases electronic waste. Both are less than ideal.

Billions of dollars of commerce, such as secure WiFi vendors, retail hotspot vendors, depend on the ability of users and companies to install the software of their choosing. Without this ability, these technologies could not exist any longer.

Furthermore, these rules will restrict activities such as the installation custom firmware and operating systems on computers and phones, which add features, fix problems, etc. Without this, computer's potential, and by proxy, their ownership will be limited to the company providing the operating system. With Microsoft Windows 10's issues and telemetry, this proposed rule will effectively make Microsoft a spying organization, with total control of all non-apple computers.

I have moved Windows from all of my systems to a secondary role, under various Linux-based OSes. (This made them faster, and more capable, on top of the fact that Microsoft doesn't get to see every keystroke, every click, every file on my computer and storage devices. )

Open source is what has, and continues to, make the technology industries what they are today. Even now, Apple and Microsoft increasingly rely on open source software to improve their own software. These rules would effectively kill open source. (At least on anything with WiFi, which is most computers and all portable devices.) It is important to note that many industries rely on open-source to some degree, and this proposed rule would destroy this, potentially having a severe effect on those industries and even our economy as a whole.

I would sooner remove all of my wireless cards than give my ownership of my devices to the government, Microsoft, etc. And I'm sure many feel the same.

One key aspect of owning a device is the ability to make changes to it, modify it at the hardware and software levels, provided the device is kept within the restrictions of regulations (many of which are currently in place to prevent health issues, interference, and interrupting important communications, such as those by police, military, medical, etc. By implementing this rule, you would be taking ownership of every phone, computer, router, modem, tablet, even modern versions of appliances such as refrigerators and washing machines, away from Americans.

As a technician, network support student, and software/hardware design hobbyist, I humbly ask that you reconsider this rule. It will have severe repercussions in the technology industry, and by proxy, every other industry that uses some kind of electronic device.

Please do not destroy wireless technology with this rule.

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: Roby

Last Name: Nattas

Mailing Address: plinio69@email.it

City: New york

Country: United States

State or Province: AK

ZIP/Postal Code: 1000

Email Address:

Organization Name:

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

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Paolo

Last Name: Andreozzi

Mailing Address: Via Lecco 154

City: Monza

Country: Italy

State or Province: MB

ZIP/Postal Code: 20900

Email Address: paolo.andi@gmail.com

Organization Name:

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

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jeffrey

Last Name: Dileo

Mailing Address: 220 E 26th St #1C

City: New York

Country: United States

State or Province: NY

ZIP/Postal Code: 10010

Email Address: jtdileo@gmail.com

Organization Name:

Comment: Please see the attached comment.txt. For some reason, the submission form kept saying that my (slightly less than 5000 characters) comment (as typed in this form) was greater than the 5000 character limit.

Please see the attached comment.txt. For some reason, the submission form kept saying that my (slightly less than 5000 characters) comment (as typed in this form) was greater than the 5000 character limit.

Hi, I'm Jeff. I'm a senior security consultant at a major computer (cyber) security consultancy (but I'm just representing myself right now). I also do security research in my spare time. I know a lot about Android firmware security and have done a lot of work and research on embedded devices, such as IoT [Internet of Things] "things" ;) and home WiFi routers. I've heard a bunch of disturbing things in the news lately about new FCC rules to regulate electronic devices, and while much of the media seems to be hyping up a bunch of FUD about what the rules would actually mean, I would just like to pass on some information that may help with your rulemaking processes.

Whether or not you plan to require WiFi router manufacturers to try and implement "security" measures to prevent "flashing" unapproved software/operating systems to the devices, I think it would be good to describe the current device landscape a bit and what I predict it would be like if such requirements were put to OEMs. So, first off, things are pretty bad already. Like really bad. You may have read stories about how Android device fragmentation hurts security and leaves millions and millions of phones unpatched; this is worse. Home WiFi routers these days can generally be put into 2 groups, ones that run some sort of Linux, and ones that run an embedded OS generally referred to as a "real time operating system" (RTOS). The ones that run Linux have pretty constrained specs (like your smartphone probably is 2 orders of magnitude more powerful); the ones that run RTOSes are so resource constrained that you wouldn't imagine them to be able to do much. In both cases, the OS itself is very minimal, and there are a variety of tools and software installed to do the the stuff that WiFi routers are supposed to do (like provide Internet access and stuff ;). That "stuff" part is actually pretty scary, but I'll get to that a bit later. The OSes themselves are generally so resource constrained that they, and the software running on them, have almost no modern security mechanisms enabled. I'm talking about all the features that protect you from things like "buffer overflows." So basically, any security bug that would otherwise be much harder to exploit on your desktop/laptop computer is trivial to exploit on these devices. And that's just the "low-level" bugs occurring in bad "C" (programming language) code. Home WiFi routers also have configuration web apps. They tend to be written in a mix of C and "Lua" (another programming language). This is where some of the really scary bugs live. The sorts that can compromise and backdoor your router just from visiting a website. I've found those sorts of bugs before. They're super scary and I hope vendors fix them when people like me report them. But over time I've seen a trend. Many devices have these types of flaws and are easily compromised. And chances are, if you can compromise the web app or any other program on the device, you'll find that it's running as the most powerful admin account (or something similar, but where "account" isn't the right word) on the device. If you exploit such flaws, you can co-opt that level of privilege to do arbitrary things, the sorts of things that the device normally does, like manage/instruct the radio chips. And you can do the sorts of things that unapproved OSes (e.g. OpenWrt, DD-WRT) can do when instructed by users that don't know better (like mess with the radio to make it more powerful or use those "secret" JP channels for better WiFi bandwidth). That's bad, and also illegal. But that's not really the worst part.

The worst part is that a large majority of home WiFi routers are already compromised by "the bad guys." Recent news suggests that those "Lizard Squad" distributed denial of service (DDoS) attacks are actually perpetrated by a vast

botnet formed from compromised home WiFi routers. Also, there was this thing called the "Internet Census of 2012" that scanned the entire IPv4 address space (for most purposes, this is literally the entire public Internet) for all sorts of statistics. The "census" results came out of nowhere. The reason for this is that some random person (or people) did the entire thing in a clandestine manner by performing all of the scans from one of the world's largest botnets. But it wasn't only one of the largest, it was also formed by compromised home WiFi routers. If the people running these botnets bothered to care, and if the router radios let them, they could probably cause mass havoc and do all sorts of bad things to the radio spectrum to disrupt critical services.

Right now, the OpenWrt's of the world are much more secure. If people can't use them, the poor security we have gets worse. And the bad guys can still do the bad radio frequency stuff. Please don't require or guide device OEMs to try and block "flashing." Require them to block bad behavior at the radio level, because I doubt their devices will stop getting mass hacked.

I hope this helps,  
-Jeff

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: Derek

Last Name: Linz

Mailing Address: 517 Everett Ln

City: Chapel Hill

Country: United States

State or Province: NC

ZIP/Postal Code: 27516

Email Address: freerangeservers@gmail.com

Organization Name:

Comment: Esteemed FCC,

I implore you to consider the ramifications of this proposal, not only in terms of the limitations it places on individual freedoms--i.e. the right to choose the software they run on their electronic devices-- but also in terms of damage to the anti-trust impact of opensource software development.

If such regulations were to be implemented, it would effectively create an FCC endorsement for software giants like Apple and further solidifying the monopolistic nature of this sector.

Thank you for considering my comment,  
Derek Linz

Esteemed FCC,

I implore you to consider the ramifications of this proposal, not only in terms of the limitations it places on individual freedoms--i.e. the right to choose the software they run on their electronic devices-- but also in terms of damage to the anti-trust impact of opensource software development.

If such regulations were to be implemented, it would effectively create an FCC endorsement for software giants like Apple and further solidifying the monopolistic nature of this sector.

Thank you for considering my comment,  
Derek Linz

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: Jack

Last Name: Coats

Mailing Address: 2004 Girl Scout Rd

City: Ashland City

Country: United States

State or Province: TN

ZIP/Postal Code: 37015

Email Address: jack@coats.org

Organization Name: Personal user, not affiliated with any organization.

Comment: I understand wanting to dis-allow misuse of equipment that generates radio radiation, but this proposed regulation will keep people from being able to update their equipment for necessary maintenance especially for the installation of 3rd party software that is needed in much wireless equipment to provide enhanced features, security, or, most often, to fix security problems.

<p>

Many vendors have a VERY poor track record about fixing security issues, especially for non-leading edge equipment. Back generations of equipment that has significant useful life left is ignored by several vendors. There are more than one or two stories of the proper 'support' line response for people wanting a current security enhancement for a new WIFI router less than 6 months old being told 'it is too old to fix. Buy a new one.' This is unacceptable to most of us on fixed or lower incomes.

<p>

Yes, I understand, there will be some people that modify software to allow the software controlled transmitters to provide higher power than the hardware is registered for.

<p>

One option is to require vendors to make equipment that cannot generate excess power rather than hamstringing users into not being able to keep the equipment more than a few months or live with security problems.

<p>

Please help the good user community to keep being able to use their consumer grade equipment without resorting to 'jail breaking' or 'hacking' it, making its use technically illegal.

<p>

Thank you for your understanding.

<p>Sorry for the poor formatting, I was not able to determine how to format this document in a more effective method.

I understand wanting to dis-allow misuse of equipment that generates radio radiation, but this proposed regulation will keep people from being able to update their equipment for necessary maintenance especially for the installation of 3rd party software that is needed in much wireless equipment to provide enhanced features, security, or, most often, to fix security problems.

<p>

Many vendors have a VERY poor track record about fixing security issues, especially for non-leading edge equipment. Back generations of equipment that has significant useful life left is ignored by several vendors. There are more than one or two stories of the proper 'support' line response for people wanting a current security enhancement for a new WIFI router less than 6 months old being told 'it is too old to fix. Buy a new one.' This is un-acceptable to most of us on fixed or lower incomes.

<p>

Yes, I understand, there will be some people that modify software to allow the software controlled transmitters to provide higher power than the hardware is registered for.

<p>

One option is to require vendors to make equipment that cannot generate excess power rather than hamstringing users into not being able to keep the equipment more than a few months or live with security problems.

<p>

Please help the good user community to keep being able to use their consumer grade equipment without resorting to 'jail breaking' or 'hacking' it, making its use technically illegal.

<p>

Thank you for your understanding.

<p>Sorry for the poor formatting, I was not able to determine how to format this document in a more effective method.

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: Giff

Last Name: Hammar

Mailing Address: 1080 Crestview Dr

City: Annapolis

Country: United States

State or Province: MD

ZIP/Postal Code: 21409

Email Address: ghammar@sv-phoenix.com

Organization Name: null

Comment: In general, there is no recognition of legitimate changes to equipment for licensed services, particularly amateur radio. Since the frequencies between 5.65 and 5.85 GHz in section 2.1033(b)(10) fall within the 5.65 to 5.925 GHz amateur allocation, it is important to note the differences between these rules and allowed activities under Part 97. Many innovations in communications have been started in the amateur community as part of our activities to advance the art and science of wireless communications. The ability to add functionality via a software download allows end users to improve capabilities without replacing hardware. For wireless devices, this means, among other things, the ability to fix or improve security to ensure that others can't access the equipment, or to create new capabilities where none existed before. For amateur operators in particular, the inability to download new firmware to a device would prevent using existing hardware for experimentation or advancing the art and science of wireless communications. These are core tenets of the amateur radio community and would cause undue hardship in that portion of our allocated spectrum. Streamlining the rules is good as is responding to new technologies, but it should not be at the expense of creating future capabilities.

In general, there is no recognition of legitimate changes to equipment for licensed services, particularly amateur radio. Since the frequencies between 5.65 and 5.85 GHz in section 2.1033(b)(10) fall within the 5.65 to 5.925 GHz amateur allocation, it is important to note the differences between these rules and allowed activities under Part 97. Many innovations in communications have been started in the amateur community as part of our activities to advance the art and science of wireless communications. The ability to add functionality via a software download allows end users to improve capabilities without replacing hardware. For wireless devices, this means, among other things, the ability to fix or improve security to ensure that others can't access the equipment, or to create new capabilities where none existed before. For amateur operators in particular, the inability to download new firmware to a device would prevent using existing hardware for experimentation or advancing the art and science of wireless communications. These are core tenets of the amateur radio community and would cause undue hardship in that portion of our allocated spectrum. Streamlining the rules is good as is responding to new technologies, but it should not be at the expense of creating future capabilities.

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: Gadd

Mailing Address: 1566 Hudson Ct

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32808

Email Address: dgadd523@gmail.com

Organization Name: N/A

Comment: Dear Sirs

I am a retired software engineer turned hobbyist who spends most of my time experimenting with old equipment with new software. Often I've found this software works better than what came with the equipment. I'm especially disturbed that software would be linked to hardware by law, as this would make experimentation and improvements impossible. Some of the software I've worked with includes wireless equipment in PCs and routers. Not to mention the fact modifying this equipment often finds bugs and issues. Tying the equipment to software ties one into the manufacturer to fix or upgrade software on equipment already owned.

Thanks for taking the time to read this missive.

Sincerely

David A. Gadd

1566 Hudson Ct.

Orlando, FL 32808

Dear Sirs

I am a retired software engineer turned hobbyist who spends most of my time experimenting with old equipment with new software. Often I've found this software works better than what came with the equipment. I'm especially disturbed that software would be linked to hardware by law, as this would make experimentation and improvements impossible. Some of the software I've worked with includes wireless equipment in PCs and routers. Not to mention the fact modifying this equipment often finds bugs and issues. Tying the equipment to software ties one into the manufacturer to fix or upgrade software on equipment already owned.

Thanks for taking the time to read this missive.

Sincerely

David A. Gadd

1566 Hudson Ct.

Orlando, FL 32808



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: Rasche

Mailing Address: 702 E Amelia St

City: Orlando

Country: United States

State or Province: FL

ZIP/Postal Code: 32803

Email Address: brasche@gmail.com

Organization Name:

Comment: I am opposed to any proposed ruling which will:

-Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

-Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes

-Ban installation of custom firmware on an Android phone

-Discourage the development of alternative free and open source WiFi firmware, like OpenWrt

-Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

-Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.

-Prevent the ability of researchers to investigate and modify their devices.

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

-Prevent users from fixing serious bugs in their wifi drivers, which would be banned under the NPRM.

I am opposed to any proposed ruling which will:

-Restrict installation of alternative operating systems on your PC, like GNU/Linux, OpenBSD, FreeBSD, etc.

-Prevent research into advanced wireless technologies, like mesh networking and bufferbloat fixes

-Ban installation of custom firmware on an Android phone

- Discourage the development of alternative free and open source WiFi firmware, like OpenWrt
- Infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.
- Prevent resellers from installing firmware on routers, such as for retail WiFi hotspots or VPNs, without agreeing to any condition a manufacturer so chooses.
- Prevent the ability of researchers to investigate and modify their devices.
- Prevent the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- Prevent users from fixing serious bugs in their wifi drivers, which would be banned under the NPRM.

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: Tomanek

Mailing Address: 82 Knollwood Dr

City: Wallingford, CT

Country: United States

State or Province: CT

ZIP/Postal Code: 06492

Email Address:

Organization Name: R&D, research

Comment:

The document is a good try to rectify existing problems.

The whole document will cause harm to the US industry and public.

I believe, the document shall be rewritten page by page, chapters revised by multiple parties from the industry, and can't be used as is.

My experience is more than 40 years in the RF and Wireless industry.

Regards Dave

The document is a good try to rectify existing problems.

The whole document will cause harm to the US industry and public.

I believe, the document shall be rewritten page by page, chapters revised by multiple parties from the industry, and can't be used as is.

My experience is more than 40 years in the RF and Wireless industry.

Regards Dave

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: Gibbs

Mailing Address: 115 W 39th St

City: Minneapolis

Country: United States

State or Province: MN

ZIP/Postal Code: 55409

Email Address: dcquence@gmail.com

Organization Name:

Comment: Hello FCC,

I ask that you please do not impliment rules that will take away people's ability to install software to or even update the software on devices that they own due to these suggested 5Ghz regulations.

This will cause many many devices to fall out of safe use and allow manufacturers to force upgrades by means of simply not updating their existing devices among many other reasons why this is a terrible idea.

Thank you,

John Gibbs

Hello FCC,

I ask that you please do not impliment rules that will take away people's ability to install software to or even update the software on devices that they own due to these suggested 5Ghz regulations.

This will cause many many devices to fall out of safe use and allow manufacturers to force upgrades by means of simply not updating their existing devices among many other reasons why this is a terrible idea.

Thank you,

John Gibbs

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: Dawson

Last Name: Crisman

Mailing Address: 868 W Michaels Ct

City: Fountaintown

Country: United States

State or Province: IN

ZIP/Postal Code: 46130

Email Address: crismandawson@gmail.com

Organization Name:

Comment: I respectfully ask you to not limit a user's choice when it comes to the software of their computing devices. It is this type of choice that drives the innovation in the United States. Without the ability to change the software, researchers are unable to find vulnerabilities that would otherwise go unnoticed until a malicious individual exploits it.If we do not have the ability to change our software, we will be unable to fix security holes that the manufacturer has decided to leave open.

I respectfully ask you to not limit a user's choice when it comes to the software of their computing devices. It is this type of choice that drives the innovation in the United States. Without the ability to change the software, researchers are unable to find vulnerabilities that would otherwise go unnoticed until a malicious individual exploits it.If we do not have the ability to change our software, we will be unable to fix security holes that the manufacturer has decided to leave open.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Alan

Last Name: McIntyre

Mailing Address: 280 Jeremy Dr

City: Colbert

Country: United States

State or Province: GA

ZIP/Postal Code: 30628

Email Address:

Organization Name:

Comment: I am opposed to these rule changes, as they will result in restrictions on the freedom of owners of COTS RF equipment. If I purchase a piece of RF equipment, and later find that its firmware is insufficient for my purposes (or worse, defective and insecure), it seems unreasonable that I should be prevented from updating that firmware myself. I don't like being left at the mercy of a large company to provide a firmware update (assuming such a thing is even allowed under these new rules without lots of paperwork) out of an abundance of goodwill.

Moreover, it is not clear to me whether US citizens may find themselves in legal trouble if they should publish methods of bypassing the security measures on future RF hardware/firmware. These rule changes are a step in that direction, and I would prefer not to see such steps taken in any industry, much less one that is still undergoing rapid evolution.

Surely there are already mechanisms and policies in place for punishing those who abuse a device (modified or not) to violate existing FCC rules? I would prefer that the FCC spend its resources addressing such abuse directly, instead of coming up with new rules that will stifle innovation and limit the ability of property owners to modify their own property on the vague fear that they might misuse it.

I am opposed to these rule changes, as they will result in restrictions on the freedom of owners of COTS RF equipment. If I purchase a piece of RF equipment, and later find that its firmware is insufficient for my purposes (or worse, defective and insecure), it seems unreasonable that I should be prevented from updating that firmware myself. I don't like being left at the mercy of a large company to provide a firmware update (assuming such a thing is even allowed under these new rules without lots of paperwork) out of an abundance of goodwill.

Moreover, it is not clear to me whether US citizens may find themselves in legal trouble if they should publish methods of bypassing the security measures on future RF hardware/firmware. These rule changes are a step in that direction, and I would prefer not to see such steps taken in any industry, much less one that is still undergoing rapid evolution.

Surely there are already mechanisms and policies in place for punishing those who abuse a device (modified or not) to violate existing FCC rules? I would prefer that the FCC spend its resources addressing such abuse directly, instead of coming up with new rules that will stifle innovation and limit the ability of property owners to modify their own property on the vague fear that they might misuse it.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Cody

Last Name: Whitaker

Mailing Address: 3672 W. Pony Trail

City: Tucson

Country: United States

State or Province: AZ

ZIP/Postal Code: 85742

Email Address: ironclyde@netzero.net

Organization Name: Private Party

Comment: Ladies and Gentlemen of the FCC,

I would like to register my objection to the proposed regulations as set forth in the following:

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

Respectfully Submitted

Cody E. Whitaker

Ladies and Gentlemen of the FCC,

I would like to register my objection to the proposed regulations as set forth in the following:

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

Respectfully Submitted

Cody E. Whitaker

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: Raymond

Last Name: Black

Mailing Address: 20315 Louetta Reach Drive

City: Spring

Country: United States

State or Province: TX

ZIP/Postal Code: 77388

Email Address: rdb4133@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.