

commercial systems doesn't help.

3. Software bugs are normal and as studies found the number of bugs in open source software and commercial software is not that different. So a bug in approved firmware or customized firmware are equally likely to affect the compliance.

4. Many people rely on the customization for new features, custom applications or security fixes. This new rule would make it more expensive for effected people. They would have to buy expensive certified niche products or replace devices more often because manufacturers are not fixing bugs anymore. This is going to cause damage to the economy and the environment (due to additional electronic waste products).

5. A more simple solution could be a warning sticker or even a mandatory warning during a software update to take care that the new software is reliable and doesn't violate any FCC regulations. This way the device owner can take responsibility and carefully consider the modification.

I hope you will consider modifying before finalizing the regulation.

Sincerely,

Wolfram Grziwa

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: Dawn

Last Name: Daniels

Mailing Address: 30119 N park drive APT 302

City: Chesterfield

Country: United States

State or Province: MI

ZIP/Postal Code: 48047

Email Address:

Organization Name:

Comment: Enacting this law would not only violate the rights of the consumer to have full control/ownership over their own property, but it will also introduce security holes in systems currently relying on linux-kernel routers (such as DD-WRT). Proprietary software is notoriously buggy, and there is a precedent set (Cisco circa 2012) for backdoors in proprietary firmware being used as a method of surveillance.

Furthermore, this will impact the ability of consumers to choose how their electronic devices, including smartphones, tablets, and computers, run. Open source operating systems often rely on modified drivers; restricting the modification of drivers will restrict accessibility to alternative operating systems.

Restricting the ability of consumers to legally modify firmware on their own devices will both violate the rights of ownership and prevent consumers from protecting their data online.

Enacting this law would not only violate the rights of the consumer to have full control/ownership over their own property, but it will also introduce security holes in systems currently relying on linux-kernel routers (such as DD-WRT). Proprietary software is notoriously buggy, and there is a precedent set (Cisco circa 2012) for backdoors in proprietary firmware being used as a method of surveillance.

Furthermore, this will impact the ability of consumers to choose how their electronic devices, including smartphones, tablets, and computers, run. Open source operating systems often rely on modified drivers; restricting the modification of drivers will restrict accessibility to alternative operating systems.

Restricting the ability of consumers to legally modify firmware on their own devices will both violate the rights of ownership and prevent consumers from protecting their data online.

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: Easton

Last Name: Pierce

Mailing Address: 24009 19th ave S

City: Des Moines

Country: United States

State or Province: WA

ZIP/Postal Code: 98198

Email Address: heaven.walker@hotmail.com

Organization Name:

Comment: Please don't.

Please don't.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Young

Mailing Address: 3479 Filoli Circle

City: Carlsbad

Country: United States

State or Province: CA

ZIP/Postal Code: 92009

Email Address:

Organization Name:

Comment: To Whom it may concern.

Please reconsider this proposed rule for the following reasons:

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

Please preserve user freedom.

To Whom it may concern.

Please reconsider this proposed rule for the following reasons:

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

Please preserve user freedom.

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: Carlos

Last Name: Young

Mailing Address: 7733 park falls dr

City: Houston

Country: United States

State or Province: TX

ZIP/Postal Code: 77095

Email Address: spiffman10@gmail.com

Organization Name:

Comment: In Humble regards Please accept my statement,

First to propose a regulation that limits the power of "WIFI" as it is referred is like shooting ones own foot and wondering why one cant walk or progress,also hindering improvement in wireless communication is not a wise move for the FCC. Second This action is a SLAP to the face to the American public and the IT community alike. There are multiple reasons why this regulation should not pass most are explained below. Here are some listed: It 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 Device. 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. In closing I would like to express that in as American citizen that this bill is a infringement on ones open source rights and free source rights.---> Carlos Young GOD BLESS AMERICA

In Humble regards Please accept my statement,

First to propose a regulation that limits the power of "WIFI" as it is referred is like shooting ones own foot and wondering why one cant walk or progress,also hindering improvement in wireless communication is not a wise move for the FCC. Second This action is a SLAP to the face to the American public and the IT community alike. There are multiple reasons why this regulation should not pass most are explained below. Here are some listed: It 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 Device. 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. In closing I would like to express that in as American citizen that this bill is a infringement on ones open source rights and free source rights.---> Carlos Young GOD BLESS AMERICA

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: Scott

Last Name: Yacko

Mailing Address: 2409 Hastings Dr

City: Belmont

Country: United States

State or Province: CA

ZIP/Postal Code: 94002

Email Address:

Organization Name:

Comment: Hello,

Please leave technology open to modification, so that people can experiment and develop better solutions.

Thank you,

Scott

Hello,

Please leave technology open to modification, so that people can experiment and develop better solutions.

Thank you,

Scott

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: Jeffery

Last Name: Farrell

Mailing Address: 19545 Morrie Drive

City: Oregon City

Country: United States

State or Province: OR

ZIP/Postal Code: 97045

Email Address: jefffarrell@hotmail.com

Organization Name: Private Citizen of the United States

Comment: I respectfully request that you do not implement the proposed rule 'Equipment Authorization and Electronic Labeling for Wireless Devices'; this regulation would stifle innovation, make us less secure, and set back innovation in the United States decades.

This rule would discourage the development of alternative free and open source WiFi firmware, like OpenWrt. It would also infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

OpenWrt was used to create 'LibraryBox' (<http://www.librarybox.us>), a small WiFi enabled file server that delivers information to devices (cellular phones, tablets, etc.) within a range of up to 100 feet. It is necessary for the original manufacturers router (in LibraryBox's case, the TP-Link MR3020) to have its firmware flashed with OpenWrt, in order to further install the LibraryBox software. I am 'forking' the original LibraryBox software to create a device that can assist the general public during a disaster event.

Without the ability to flash the firmware of this WiFi enabled router, I will be unable to deliver my product; thus being unable to deliver vital information during a disaster event, which could cost lives!

Thank You for your consideration.

I respectfully request that you do not implement the proposed rule 'Equipment Authorization and Electronic Labeling for Wireless Devices'; this regulation would stifle innovation, make us less secure, and set back innovation in the United States decades.

This rule would discourage the development of alternative free and open source WiFi firmware, like OpenWrt. It would also infringe upon the ability of amateur radio operators to create high powered mesh networks to assist emergency personnel in a disaster.

OpenWrt was used to create 'LibraryBox' (<http://www.librarybox.us>), a small WiFi enabled file server that delivers information to devices (cellular phones, tablets, etc.) within a range of up to 100 feet. It is necessary for the original manufacturers router (in LibraryBox's case, the TP-Link MR3020) to have its firmware flashed with OpenWrt, in order to further install the LibraryBox software. I am 'forking' the original LibraryBox software to create a device that can assist the general public during a disaster event.

Without the ability to flash the firmware of this WiFi enabled router, I will be unable to deliver my product; thus being unable to deliver vital information during a disaster event, which could cost lives!

Thank You for your consideration.

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: Vicki

Last Name: Fletcher

Mailing Address: 20990 SW Blaine Terrace

City: Beaverton

Country: United States

State or Province: OR

ZIP/Postal Code: 97003

Email Address: vfletcher@arrowmakers.net

Organization Name:

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

* I want to run the OS of my choosing on my devices! I am a linux user and plan to remain one.

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

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

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

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

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

* I want to run the OS of my choosing on my devices! I am a linux user and plan to remain one.

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

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

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

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Joseph

Last Name: Abelseth

Mailing Address: 227 Taylor Street

City: Bristol

Country: United States

State or Province: TN

ZIP/Postal Code: 37620

Email Address:

Organization Name:

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

- 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.

Please do 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.) 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: Timothy

Last Name: Knox

Mailing Address: 309 NE 155th Street

City: Shoreline

Country: United States

State or Province: WA

ZIP/Postal Code: 98155

Email Address: tdk-fcc@thelbane.com

Organization Name:

Comment: To the FCC Commissioners,

I would urge you to be extremely careful in formulating rules limiting software changes to devices that can utilize the 5GHz band. I realise that you are trying to protect the American consumer from bad actors who would abuse that frequency band, making it unusable as currently designated. I applaud your desire to do so.

However, I am concerned that if your regulations are overbroad, you will limit some useful, perhaps even vital, freedoms of the consumer. For example, I run a WiFi base station at home that can use the 5GHz band (as well as the 2.4GHz band). I overwrote the "as shipped" firmware with DD-WRT. Not only is this firmware far more actively maintained than the manufacturer's version, it provides greater security, and greater functionality than that provided by the manufacturer.

Without the freedom to replace the built-in firmware, I would either have had to 1) use a far less capable and secure base station, 2) shop for another brand that was more capable and secure, or 3) do without 5GHz capability. These are all far from satisfactory options.

NB I am asking you to completely abrogate your regulatory responsibility in this arena. I respect that you have a role to play in this regard. However, I'd urge you to strike a balance that prohibits the truly bad acts, while retaining the freedoms that have been so useful to date.

I thank you for your time and your consideration.

To the FCC Commissioners,

I would urge you to be extremely careful in formulating rules limiting software changes to devices that can utilize the 5GHz band. I realise that you are trying to protect the American consumer from bad actors who would abuse that frequency band, making it unusable as currently designated. I applaud your desire to do so.

However, I am concerned that if your regulations are overbroad, you will limit some useful, perhaps even vital, freedoms of the consumer. For example, I run a WiFi base station at home that can use the 5GHz band (as well as the 2.4GHz band). I overwrote the "as shipped" firmware with DD-WRT. Not only is this firmware far more actively maintained than the manufacturer's version, it provides greater security, and greater functionality than that provided by the manufacturer.

Without the freedom to replace the built-in firmware, I would either have had to 1) use a far less capable and secure base station, 2) shop for another brand that was more capable and secure, or 3) do without 5GHz capability. These are all far from satisfactory options.

NB I am asking you to completely abrogate your regulatory responsibility in this arena. I respect that you have a role to play in this regard. However, I'd urge you to strike a balance that prohibits the truly bad acts, while retaining the freedoms that have been so useful to date.

I thank you for your time and your consideration.

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: Sergey

Last Name: Zaikin

Mailing Address: grau87@yandex.ru

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: 303630

Email Address:

Organization Name:

Comment: It's silly to block another system or updates

It's silly to block another system or updates

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: William

Last Name: Drago

Mailing Address: williamdrago@libero.it

City: Cosenza

Country: Italy

State or Province: Cosenza

ZIP/Postal Code: 87100

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: Justin

Last Name: King-Lacroix

Mailing Address: Department of Computer Science, University of Oxford, Wolfson Building, Parks Road

City: Oxford

Country: United Kingdom

State or Province: Oxfordshire

ZIP/Postal Code: OX1 3QD

Email Address: justin.king-lacroix@cs.ox.ac.uk

Organization Name: Department of Computer Science, University of Oxford

Comment: The rules, as proposed, combined with the economics of manufacturing WiFi routers and router-like devices, would eliminate the ability of consumers to install custom firmwares on their routers.

This is not simply a 'consumer choice' problem, it has real security implications. The useful lifetime of a WiFi router is often *far* greater than the period for which the router's manufacturer provides security updates, if such updates are indeed ever provided. Custom firmwares fill this niche: they are kept up to date, and very rarely drop support for old platforms. Installing one is therefore a viable way to maintain an up-to-date software configuration past the manufacturer's update period -- which, it must be stressed, is *far* shorter than even the device's support period, to say nothing of the useful life of the device.

Any rules on 5GHz WiFi must take this problem into account, lest the current problems of IT security on embedded platforms worsen. That effect will furthermore be hugely magnified by the ever-increasing popularity of Internet of Things solutions. The concomitant proliferation of embedded systems,

The rules, as proposed, combined with the economics of manufacturing WiFi routers and router-like devices, would eliminate the ability of consumers to install custom firmwares on their routers.

This is not simply a 'consumer choice' problem, it has real security implications. The useful lifetime of a WiFi router is often *far* greater than the period for which the router's manufacturer provides security updates, if such updates are indeed ever provided. Custom firmwares fill this niche: they are kept up to date, and very rarely drop support for old platforms. Installing one is therefore a viable way to maintain an up-to-date software configuration past the manufacturer's update period -- which, it must be stressed, is *far* shorter than even the device's support period, to say nothing of the useful life of the device.

Any rules on 5GHz WiFi must take this problem into account, lest the current problems of IT security on embedded platforms worsen. That effect will furthermore be hugely magnified by the ever-increasing popularity of Internet of Things solutions. The concomitant proliferation of embedded systems,

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: Dino

Last Name: Ciuffetti

Mailing Address: Via Luciano Conti 66

City: Rome

Country: Italy

State or Province: RM

ZIP/Postal Code: 00132

Email Address: dino@tuxweb.it

Organization Name: TuxWeb S.r.l.

Comment: As an internet citizen, linux system administrator and open source expert, I'm very disappointed about the creation of such measures that restrict the modification of U-NII devices.

This certainly will create big security holes not promptly fixed by device manufacturers, and it will also stop innovation.

What you are trying to do will create big problems in USA, but it will also create problems here in EU and in the rest of the world for sure.

Please STOP before is too late!!

Thank you.

As an internet citizen, linux system administrator and open source expert, I'm very disappointed about the creation of such measures that restrict the modification of U-NII devices.

This certainly will create big security holes not promptly fixed by device manufacturers, and it will also stop innovation.

What you are trying to do will create big problems in USA, but it will also create problems here in EU and in the rest of the world for sure.

Please STOP before is too late!!

Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Herbert

Last Name: Beadle IV

Mailing Address: 947 Klem Rd

City: Webster

Country: United States

State or Province: NY

ZIP/Postal Code: 14580

Email Address: null

Organization Name: null

Comment: This would be extremely harmful in a number of ways. Taking away the ability of individuals to improve the software on their wireless devices will stifle beneficial things including academic researchers, security patches, improved 3rd party drivers, and a great many things that are too numerous to list. I'm certain that it would have negative consequences far beyond what most of us can discern, since stifling innovation causes fast-propagating problems throughout our economy. As a researcher, programmer, and free software enthusiast, I have to strongly recommend against this proposed rule.

This would be extremely harmful in a number of ways. Taking away the ability of individuals to improve the software on their wireless devices will stifle beneficial things including academic researchers, security patches, improved 3rd party drivers, and a great many things that are too numerous to list. I'm certain that it would have negative consequences far beyond what most of us can discern, since stifling innovation causes fast-propagating problems throughout our economy. As a researcher, programmer, and free software enthusiast, I have to strongly recommend against this proposed 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: Norbert

Last Name: Kiesel

Mailing Address: 904 Kara Way

City: Campbell

Country: United States

State or Province: CA

ZIP/Postal Code: 95008

Email Address: nk@iname.com

Organization Name:

Comment: This regulations would

- increase costs for consumers because of limited competition
- decrease security for consumers because they cannot fix their wireless routers anymore
- prevent advances in research

This regulations would

- increase costs for consumers because of limited competition
- decrease security for consumers because they cannot fix their wireless routers anymore
- prevent advances in research

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: Tabor

Last Name: Kelly

Mailing Address: 4909 Willamette Dr

City: Vancouver

Country: United States

State or Province: WA

ZIP/Postal Code: 98661

Email Address: taborkelly@gmail.com

Organization Name:

Comment: I oppose any change to regulations that would require Wireless networking manufacturers to prevent end users and independent researchers from modifying device firmware. Specifically:

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

Sincerely,
Tabor Kelly

I oppose any change to regulations that would require Wireless networking manufacturers to prevent end users and independent researchers from modifying device firmware. Specifically:

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

Sincerely,
Tabor Kelly

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: Lilly

Mailing Address: Camden-Elk Rd.

City: Elk

Country: United States

State or Province: WA

ZIP/Postal Code: 99009

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.

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

I 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.

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Colby

Last Name: Rome

Mailing Address: 253 Billings Mill Rd

City: Tunkhannock

Country: United States

State or Province: PA

ZIP/Postal Code: 18657

Email Address: colbyrome@gmail.com

Organization Name:

Comment: I think this proposed regulation is not only ridiculous but also highly damaging to Computer Science in general. Please, do NOT pass this incredibly draconian regulation.

I think this proposed regulation is not only ridiculous but also highly damaging to Computer Science in general. Please, do NOT pass this incredibly draconian regulation.

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: Kevin

Last Name: Meagher

Mailing Address: 2702 Archangel Court

City: Bowie

Country: United States

State or Province: MD

ZIP/Postal Code: 20716

Email Address: kmeaghermd@verizon.net

Organization Name: --

Comment: Using Authentication to ensure compliance would prevent low cost development key devices, reduce device security and contribute to e-waste.

REf: Paragraph 17:

<https://www.federalregister.gov/articles/2015/08/06/2015-18402/equipment-authorization-and-electronic-labeling-for-wireless-devices#p-35>

Key to the low cost "Internet of Things" industry are integrated RF modules such as the ESP8266EX (FCC identifier is: 2AC7Z-ESP8266EX). These modules can be added to many different types of form factors to provide RF access. Integrated into these types of modules is a micro-controller that can be programmed by the form factor maker or the consumer of of the form factor maker. Re-use of this processor lowers the form factor cost since the form factor manufacturer does not need to add a separate processor. The program-ability of the module processor is key to form factor manufactures developing low cost rf items such as low cost low power portable medical monitors, safety/warning devices, energy monitoring/saving devices, location beacons, consumer items, etc. Limiting program-ability to the module manufacturer would shutdown an industry that is raising the quality of life at prices that even 3rd world populations can afford. An "authentication" requirement could easily prevent this program-ability.

Accessing the internet form many small businesses and consumers requires a Small Office/Home Office (SOHO) router with wireless access point. These SOHO routers are low cost commodity items. Since the routers are connected to the internet, they are often the target of hackers trying to gain entry into a network or to use in bot armies employed to cause denial of service attacks. Many security vulnerabilities have been found in such devices and new exploits are discovered every day. The only way to guard against attacks is for the manufacturers to patch the security holes and for customers to apply these security updates. Unfortunately, these SOHO devices are low cost and support is abandoned by the manufacture quickly after the product is released ending any further efforts to patch security problems. Fortunately, for customers several open source software alternatives are available for these manufacturers' SOHO routers. SW from DD-WRT, Tomato, OpenWRT and others can be installed on SOHO routers replacing the original manufacturers SW. These OpenSource projects continually update there software providing secure updates for SOHO routers. An authentication requirement would prevent these open source projects forcing consumers to buy new routers every few years and discard their previous routers.

Using Authentication to ensure compliance would prevent low cost development key devices, reduce device security and contribute to e-waste.

REf: Paragraph 17:

<https://www.federalregister.gov/articles/2015/08/06/2015-18402/equipment-authorization-and-electronic-labeling-for-wireless-devices#p-35>

Key to the low cost "Internet of Things" industry are integrated RF modules such as the ESP8266EX (FCC identifier is: 2AC7Z-ESP8266EX). These modules can be added to many different types of form factors to provide RF access. Integrated into these types of modules is a micro-controller that can be programmed by the form factor maker or the consumer of the form factor maker. Re-use of this processor lowers the form factor cost since the form factor manufacturer does not need to add a separate processor. The program-ability of the module processor is key to form factor manufactures developing low cost rf items such as low cost low power portable medical monitors, safety/warning devices, energy monitoring/saving devices, location beacons, consumer items, etc. Limiting program-ability to the module manufacturer would shutdown an industry that is raising the quality of life at prices that even 3rd world populations can afford. An "authentication" requirement could easily prevent this program-ability.

Accessing the internet from many small businesses and consumers requires a Small Office/Home Office (SOHO) router with wireless access point. These SOHO routers are low cost commodity items. Since the routers are connected to the internet, they are often the target of hackers trying to gain entry into a network or to use in bot armies employed to cause denial of service attacks. Many security vulnerabilities have been found in such devices and new exploits are discovered every day. The only way to guard against attacks is for the manufacturers to patch the security holes and for customers to apply these security updates. Unfortunately, these SOHO devices are low cost and support is abandoned by the manufacture quickly after the product is released ending any further efforts to patch security problems. Fortunately, for customers several open source software alternatives are available for these manufacturers' SOHO routers. SW from DD-WRT, Tomato, OpenWRT and others can be installed on SOHO routers replacing the original manufacturers SW. These OpenSource projects continually update there software providing secure updates for SOHO routers. An authentication requirement would prevent these open source projects forcing consumers to buy new routers every few years and discard their previous routers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Doby

Mailing Address: 2360 Vandenberg Drive #1437

City: United States Air Force Academy

Country: United States

State or Province: CO

ZIP/Postal Code: 80841

Email Address: dobes17@outlook.com

Organization Name:

Comment: To the FCC:

The right to property and ownership is fundamental to the history and function of the United States. Indeed, Jefferson's famous "life, liberty, and pursuit of happiness" is a paraphrase of Locke's "life, liberty, and property" which saw use in the 1st Continental Constitution. Every facet of American culture, from its economy to our values of government, hinge upon the fact that our citizens both have the right to ownership of goods and the right to /use/ those goods as allowed by the law.

This value for independent ownership and freedom of use has been a driving force in the history of American innovation. Nowhere can this better be seen than the technological revolution of the Information Age. The spirit of tinkering and customization that drove the development of the first personal computers in dirty garages by college dropouts is the same spirit that drives the development of clever apps and software that we nowadays take for granted - need a patch for Windows that supports extra monitors? Someone's made modifications for that. Need a patch for your phone so that it'll work as a key to your car? Someone's made that!

The proposed regulation regarding the lockdown of wireless router firmware flies in the face not only of historical approaches to technology, but also is in contradiction to common sense.

Wifi routers, despite being on the relative background of technological modification, are no different than any other technology when it comes to accessibility and utility. From home wireless to corporate networks, ability to customize and adapt functional hardware to meet the needs of your situation. The security and use requirements for a college dorm are far removed from the security and use requirements for a wireless military network! Factory-built settings cannot, by nature, be made to match all scenarios - hence the need for personal customization.

Firmware lockdown is a security risk. Due to fund allocation, legal liability, and scale, corporations are rather slow in finding and reacting to security holes, especially in hardware. Time and time again, in all technological hardware, the patches and solutions created by users have proven invaluable not only in maintaining network security in commercial and military fields but also in finding solutions that corporations are unwilling to touch. What happens in 10 years when Cisco stops supporting my wireless router and a security hole is found? Rather than being allowed to fix my property, this regulation would tie my hands and /force/ me to throw away a perfectly functional piece of equipment.

Additionally, wireless routers are used in many roles beyond cut-and-paste network creation; many research and development teams rely on firmware modifications to use routers in new and innovative ways. From testing new software for the purpose of commercial applications - such as wireless hotspot companies, secure wifi services, and the

like - to using routers as unconventional network nodes, with the restriction of who can change the function of a wireless router comes the outright destruction of several fields of technologies and entire swathes of the technology industry!

The motives behind this regulation are not necessarily stated, but one can infer (from good faith) that the intention is in the interest of security. There does exist malicious code that takes advantage of wireless node firmware updates to propagate or exploit networks. However, the solution to this problem is not an outright ban on all router modification. To do so would be akin to banning, say, dairy products because of the risk of salmonella infection; the better solution, as is seen with the food industry, is to crack down on the malicious elements so that people may still enjoy the benefits of the good product.

Restricting firmware modification, and in effect banning firmware tinkering, is an action that will do far more harm than it will do good. For the sake of economic interests, of future innovation, and of respect for fundamental American values, please deny of this proposal regulation.

To the FCC:

The right to property and ownership is fundamental to the history and function of the United States. Indeed, Jefferson's famous "life, liberty, and pursuit of happiness" is a paraphrase of Locke's "life, liberty, and property" which saw use in the 1st Continental Constitution. Every facet of American culture, from its economy to our values of government, hinge upon the fact that our citizens both have the right to ownership of goods and the right to /use/ those goods as allowed by the law.

This value for independent ownership and freedom of use has been a driving force in the history of American innovation. Nowhere can this better be seen than the technological revolution of the Information Age. The spirit of tinkering and customization that drove the development of the first personal computers in dirty garages by college dropouts is the same spirit that drives the development of clever apps and software that we nowadays take for granted - need a patch for Windows that supports extra monitors? Someone's made modifications for that. Need a patch for your phone so that it'll work as a key to your car? Someone's made that!

The proposed regulation regarding the lockdown of wireless router firmware flies in the face not only of historical approaches to technology, but also is in contradiction to common sense.

Wifi routers, despite being on the relative background of technological modification, are no different than any other technology when it comes to accessibility and utility. From home wireless to corporate networks, ability to customize and adapt functional hardware to meet the needs of your situation. The security and use requirements for a college dorm are far removed from the security and use requirements for a wireless military network! Factory-built settings cannot, by nature, be made to match all scenarios - hence the need for personal customization.

Firmware lockdown is a security risk. Due to fund allocation, legal liability, and scale, corporations are rather slow in finding and reacting to security holes, especially in hardware. Time and time again, in all technological hardware, the patches and solutions created by users have proven invaluable not only in maintaining network security in commercial and military fields but also in finding solutions that corporations are unwilling to touch. What happens in 10 years when Cisco stops supporting my wireless router and a security hole is found? Rather than being allowed to fix my property, this regulation would tie my hands and /force/ me to throw away a perfectly functional piece of equipment.

Additionally, wireless routers are used in many roles beyond cut-and-paste network creation; many research and development teams rely on firmware modifications to use routers in new and innovative ways. From testing new software for the purpose of commercial applications - such as wireless hotspot companies, secure wifi services, and the like - to using routers as unconventional network nodes, with the restriction of who can change the function of a wireless router comes the outright destruction of several fields of technologies and entire swathes of the technology industry!

The motives behind this regulation are not necessarily stated, but one can infer (from good faith) that the intention is in the interest of security. There does exist malicious code that takes advantage of wireless node firmware updates to propagate or exploit networks. However, the solution to this problem is not an outright ban on all router modification. To do so would be akin to banning, say, dairy products because of the risk of salmonella infection; the better solution, as is seen with the food industry, is to crack down on the malicious elements so that people may still enjoy the benefits of the good product.

Restricting firmware modification, and in effect banning firmware tinkering, is an action that will do far more harm than it will do good. For the sake of economic interests, of future innovation, and of respect for fundamental American values, please deny of this proposal regulation.

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: Ragnar

Last Name: Edholm

Mailing Address: 1185 Kelsey Dr

City: Sunnyvale

Country: United States

State or Province: CA

ZIP/Postal Code: 94087

Email Address:

Organization Name:

Comment: I do not understand the logic of preventing action 1 (updating software firmware) because you want to prevent result 2 (illegal radio transmissions). If you want radio transmission to behave in a certain way, then make it illegal to break the radio transmission rules. Why focus on a software update that is not necessary related to radio transmissions? It is illegal to speed not to increase the engine power of a car.

I own a handful of WiFi enabled routers from several reputable vendors. Every single one has software security vulnerabilities that is either not fixed at all or fixed so slowly that I do not feel comfortable to run the device on my network. There are constant vulnerabilities reported for devices.

Security bugs are not the only bugs that do not get fixed. Devices get shipped with beta quality software/firmware get almost usable and then get replaced by a new model. My friends complain that they need to reboot their wifi access point/routers weekly and ask me for advice of what to buy. My only proper answer is professional devices for a lot more money or devices that support 3rd party software/firmware.

Look at the excellent work done by the bufferbloat project (<http://www.bufferbloat.net/>) Researchers needed a cheap consumer device to modify so they could get people to test in different real environments. Research like this helps commercial vendors and end users but would not be doable with the proposed rules.

Your rules will affect a wide variety of devices routers, accespoints, tablets, phones, laptops, etc. How many incidents have happened because of 3rd party firmware? How many issues compared to the number of 3rd party software installations? I have not seen any reported in the press but I see security issues with devices reported all the time.

Software bugs are not planned they will not only be in the none RF-controlling software they are everywhere.

Please modify the proposed changes to target bad radio transmission do not the tools hardware and software/firmware that were involved. The tools can be used for many other beneficial things.

I do not understand the logic of preventing action 1 (updating software firmware) because you want to prevent result 2 (illegal radio transmissions). If you want radio transmission to behave in a certain way, then make it illegal to break the radio transmission rules. Why focus on a software update that is not necessary related to radio transmissions? It is illegal to speed not to increase the engine power of a car.

I own a handful of WiFi enabled routers from several reputable vendors. Every single one has software security

vulnerabilities that is either not fixed at all or fixed so slowly that I do not feel comfortable to run the device on my network. There are constant vulnerabilities reported for devices.

Security bugs are not the only bugs that do not get fixed. Devices get shipped with beta quality software/firmware get almost usable and then get replaced by a new model. My friends complain that they need to reboot their wifi access point/routers weekly and ask me for advice of what to buy. My only proper answer is professional devices for a lot more money or devices that support 3rd party software/firmware.

Look at the excellent work done by the bufferbloat project (<http://www.bufferbloat.net/>) Researchers needed a cheap consumer device to modify so they could get people to test in different real environments. Research like this helps commercial vendors and end users but would not be doable with the proposed rules.

Your rules will affect a wide variety of devices routers, accespoints, tablets, phones, laptops, etc. How many incidents have happened because of 3rd party firmware? How many issues compared to the number of 3rd party software installations? I have not seen any reported in the press but I see security issues with devices reported all the time.

Software bugs are not planned they will not only be in the none RF-controlling software they are everywhere.

Please modify the proposed changes to target bad radio transmission do not the tools hardware and software/firmware that were involved. The tools can be used for many other beneficial things.

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: Clinton

Last Name: Shepard

Mailing Address: 5730 176th St SW

City: Lynnwood

Country: United States

State or Province: WA

ZIP/Postal Code: 98037

Email Address: clintonshpard@gmail.com

Organization Name:

Comment: Locking down device hardware should not be permitted in any shape or form. Relying on companies to have a long term policies to fix security issues within devices has been a failure in the past. Devices have seen a growth in how they gather data, allowing industries to profit from individuals that do not know that this is happening. Allowing devices to be locked down allows for an avenue for this to continue without an individuals knowledge. There should now be a lockdown on devices that have limited range of their communications.

Locking down device hardware should not be permitted in any shape or form. Relying on companies to have a long term policies to fix security issues within devices has been a failure in the past. Devices have seen a growth in how they gather data, allowing industries to profit from individuals that do not know that this is happening. Allowing devices to be locked down allows for an avenue for this to continue without an individuals knowledge. There should now be a lockdown on devices that have limited range of their communications.

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: Elad

Last Name: Yarom

Mailing Address: 404-110 Bishop Dr

City: Fredericton

Country: Canada

State or Province: New Brunswick

ZIP/Postal Code: e3c 1b2

Email Address:

Organization Name:

Comment: Dear FCC Commissioners,

I urge you to stop this proposal. Firmware in devices should be modifiable by the consumer as a matter of principle - to both guarantee liberty of the ones of the consumer's property and enhance security and usability of commercial wireless devices. I would like to direct your attention to vulnerabilities like misfortune cookie (<http://mis.fortunecook.ie/>, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9222>) that rely on outdated, exploitable firmware. Community solutions to known vulnerabilities and issues have led to alternate firmware such as asuswrt-merlin (<http://asuswrt.lostrealm.ca/about>) which enhances the asuswrt firmware both in features and security - patches that were later incorporated into the official firmware. Another thing to note is that many current firmwares rely on the FOSS community for their products, that are Open WRT or Tomato based (like asuswrt).

In the interest of more secure internet and the rights of consumers and small businesses, please do not pass this proposed rule.

Thanks you for your time.

Elad Yarom,
System Engineer, B.Sc.C.S. (Networking)

Dear FCC Commissioners,

I urge you to stop this proposal. Firmware in devices should be modifiable by the consumer as a matter of principle - to both guarantee liberty of the ones of the consumer's property and enhance security and usability of commercial wireless devices. I would like to direct your attention to vulnerabilities like misfortune cookie (<http://mis.fortunecook.ie/>, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9222>) that rely on outdated, exploitable firmware. Community solutions to known vulnerabilities and issues have led to alternate firmware such as asuswrt-merlin (<http://asuswrt.lostrealm.ca/about>) which enhances the asuswrt firmware both in features and security - patches that were later incorporated into the official firmware. Another thing to note is that many current firmwares rely on the FOSS community for their products, that are Open WRT or Tomato based (like asuswrt).

In the interest of more secure internet and the rights of consumers and small businesses, please do not pass this proposed rule.

Thanks you for your time.

Elad Yarom,
System Engineer, B.Sc.C.S. (Networking)

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Anthony

Last Name: Lozano

Mailing Address: 2892 E Harrison St

City: Gilbert

Country: United States

State or Province: AZ

ZIP/Postal Code: 85295

Email Address: lockes5shadow@gmail.com

Organization Name:

Comment: Being able to modify the software of a wireless device is an important freedom. With this regulation in place, consumers will have no ability to stop WiFi devices from spying on them. Companies that manufacturer these devices will be able to purposefully cripple them with software, forcing them to do things like only work with the manufacturers own devices. It could easily become Ma Bell all over again.

We already have legal restrictions that are sufficient governing the use of WiFi devices. Please do not restrict the freedom of users with this regulation.

Being able to modify the software of a wireless device is an important freedom. With this regulation in place, consumers will have no ability to stop WiFi devices from spying on them. Companies that manufacturer these devices will be able to purposefully cripple them with software, forcing them to do things like only work with the manufacturers own devices. It could easily become Ma Bell all over again.

We already have legal restrictions that are sufficient governing the use of WiFi devices. Please do not restrict the freedom of users with this regulation.

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: Lees

Mailing Address: 24 Norfolk Road

City: Congleton

Country: United Kingdom

State or Province: Cheshire

ZIP/Postal Code: CW12 1PA

Email Address:

Organization Name:

Comment: Throughout this document I will use the term System Software to refer to software that controls the radio or other parameters subject to the Commission's rules.

The Commission proposes new rules that will require an applicant for certification to describe the RF device's capabilities for software configuration and upgradeability in the application for certification (Paragraph 46). Such a description would include how the System Software may control the frequency bands, power levels, modulation types, or other modes of operation for which the device is designed to operate, including modes not enabled in the device as initially marketed. However, depending on the configuration of the computer hardware in question, the System Software used to control the RF device, may also have the ability to control and access other parts of the computer unrelated to the RF-device, including the CPU or other processors on the computer as well as system memory (RAM, cache, drives, et al).

Does the Commission acknowledge that the System Software software may have the ability to access the user's private information stored on the computer?

Does the Commission acknowledge that such System Software may also be designed to transmit the private information of the user via the RF device, such as over Wifi or Bluetooth, with or without the end-user's knowledge?

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

Does the Commission acknowledge that the end-user and owner of a device may not, by default, be considered an authorized party that will be able to install new System Software onto the computing device?

Does the Commission acknowledge that since the device is designed to to only run software that is authorized by a party that is not the owner or end-user, that the end-user may, in some cases, be unable to ever replace or change the software on the device?

Does the Commission acknowledge that, while only authorized parties would be allowed to provide new software to be updated, that the Commission has not put in place any requirements that it **must** be at the choice of the end-user or purchaser of a product to decide **if** new software will be installed on the device?

Does the Commission acknowledge that it may, in some cases, be the case that the only authorized parties listed and

able to install new System Software are companies not located in the United States and that are otherwise not required to abide by the laws of the United States?

Does the Commission acknowledge that because the System Software may have the ability to control the wireless capabilities of the device that the System Software may be designed to connect and share information, or even allow for the authorized party to be able to effectively remotely control the device without the user's knowledge or consent, when that device has connected to the Internet or a local area network for which the RF device is designed to interact with?

Does the Commission acknowledge that the authorized parties may be corporations that may be controlled or may eventually be acquired by other companies, governments, or foreign entities?

Does the Commission acknowledge that authorized parties may cease to exist and therefore it may be the case that an individual may never be able to update the computer again?

Does the Commission acknowledge that authorized parties based outside of the United States may be compelled by their local governments or other entities to share the means or methods for providing software updates for authorized equipment?

Does the Commission acknowledge that the computing devices maybe purchased by officials within all branches of state and local Governments which may or may not be using the computing devices for viewing or producing confidential information including, but not limited to, secret information and private medical information?

Does the Commission acknowledge that these regulations would only apply to those who follow the laws and those who have no qualms violating the law would not even care?

Does the Commission acknowledge that these regulations does not prevent people from buying from a foreign company and modify the software to be illegal?

Would the Commission consider strengthening the penalties for operating outside of the laws but not restrict, limit, cause the users to be insecure or otherwise take away freedom from the users?

Throughout this document I will use the term System Software to refer to software that controls the radio or other parameters subject to the Commission's rules.

The Commission proposes new rules that will require an applicant for certification to describe the RF device's capabilities for software configuration and upgradeability in the application for certification (Paragraph 46). Such a description would include how the System Software may control the frequency bands, power levels, modulation types, or other modes of operation for which the device is designed to operate, including modes not enabled in the device as initially marketed. However, depending on the configuration of the computer hardware in question, the System Software used to control the RF device, may also have the ability to control and access other parts of the computer unrelated to the RF-device, including the CPU or other processors on the computer as well as system memory (RAM, cache, drives, et al).

Does the Commission acknowledge that the System Software software may have the ability to access the user's private information stored on the computer?

Does the Commission acknowledge that such System Software may also be designed to transmit the private information of the user via the RF device, such as over Wifi or Bluetooth, with or without the end-user's knowledge?

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

Does the Commission acknowledge that the end-user and owner of a device may not, by default, be considered an authorized party that will be able to install new System Software onto the computing device?

Does the Commission acknowledge that since the device is designed to only run software that is authorized by a party that is not the owner or end-user, that the end-user may, in some cases, be unable to ever replace or change the software on the device?

Does the Commission acknowledge that, while only authorized parties would be allowed to provide new software to be updated, that the Commission has not put in place any requirements that it **must** be at the choice of the end-user or purchaser of a product to decide **if** new software will be installed on the device?

Does the Commission acknowledge that it may, in some cases, be the case that the only authorized parties listed and able to install new System Software are companies not located in the United States and that are otherwise not required to abide by the laws of the United States?

Does the Commission acknowledge that because the System Software may have the ability to control the wireless capabilities of the device that the System Software may be designed to connect and share information, or even allow for the authorized party to be able to effectively remotely control the device without the user's knowledge or consent, when that device has connected to the Internet or a local area network for which the RF device is designed to interact with?

Does the Commission acknowledge that the authorized parties may be corporations that may be controlled or may eventually be acquired by other companies, governments, or foreign entities?

Does the Commission acknowledge that authorized parties may cease to exist and therefore it may be the case that an individual may never be able to update the computer again?

Does the Commission acknowledge that authorized parties based outside of the United States may be compelled by their local governments or other entities to share the means or methods for providing software updates for authorized equipment?

Does the Commission acknowledge that the computing devices maybe purchased by officials within all branches of state and local Governments which may or may not be using the computing devices for viewing or producing confidential information including, but not limited to, secret information and private medical information?

Does the Commission acknowledge that these regulations would only apply to those who follow the laws and those who have no qualms violating the law would not even care?

Does the Commission acknowledge that these regulations does not prevent people from buying from a foreign company and modify the software to be illegal?

Would the Commission consider strengthening the penalties for operating outside of the laws but not restrict, limit, cause the users to be insecure or otherwise take away freedom from the users?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: matthew

Last Name: conner

Mailing Address: 13404 ROSSELLO DR

City: AUSTIN

Country: United States

State or Province: TX

ZIP/Postal Code: 78729

Email Address: michael.conner@gmail.com

Organization Name: 900237351

Comment: To whom it may concern,

The problem with constraining a consumer's ability to modify firmware or install custom firmware on devices such as wifi routers, cellular phones, tablets, and computers is not simply about protecting the spectrum.

However, the law of unintended consequences applies here. Preventing consumers, enthusiasts, and tinkerers -- many of whom may eventually contribute to the tech industry -- from modifying the devices that they own threatens to stifle innovation.

There have been no published complaints made about third-party custom firmware installed on wifi routers. Private home users of DD-WRT firmware are not endangering the spectrum.

The proposed rules are overly broad and should be revised.

To whom it may concern,

The problem with constraining a consumer's ability to modify firmware or install custom firmware on devices such as wifi routers, cellular phones, tablets, and computers is not simply about protecting the spectrum.

However, the law of unintended consequences applies here. Preventing consumers, enthusiasts, and tinkerers -- many of whom may eventually contribute to the tech industry -- from modifying the devices that they own threatens to stifle innovation.

There have been no published complaints made about third-party custom firmware installed on wifi routers. Private home users of DD-WRT firmware are not endangering the spectrum.

The proposed rules are overly broad and should be revised.

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: Prentiss

Last Name: Riddle

Mailing Address: The University of Texas at Austin

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78712

Email Address: prentiss.riddle@gmail.com

Organization Name:

Comment: I urge the FCC not to restrict the rights of consumers or users of computing devices, including smartphones and networking equipment, to install software of their choosing on those devices.

An essential characteristic of the economy in which we now live is the fact that software has so few constraints on innovation in comparison with hardware. Software allows tinkerers to become inventors, inventors to become entrepreneurs, and early adopters to constitute a viable market with markedly fewer delays or barriers to entry than in hardware-based industries. Many of the core enabling technologies on which the entire contemporary IT field is based began as open-source software developed by thousands of volunteer programmers who were free to write, install, and test experimental code without prior vetting by hardware manufacturers or government agencies.

To adopt a regulatory system under which only pre-approved software can be installed on computing devices would be a mistake with grave consequences for innovation and U.S. technological competitiveness.

I urge the FCC not to restrict the rights of consumers or users of computing devices, including smartphones and networking equipment, to install software of their choosing on those devices.

An essential characteristic of the economy in which we now live is the fact that software has so few constraints on innovation in comparison with hardware. Software allows tinkerers to become inventors, inventors to become entrepreneurs, and early adopters to constitute a viable market with markedly fewer delays or barriers to entry than in hardware-based industries. Many of the core enabling technologies on which the entire contemporary IT field is based began as open-source software developed by thousands of volunteer programmers who were free to write, install, and test experimental code without prior vetting by hardware manufacturers or government agencies.

To adopt a regulatory system under which only pre-approved software can be installed on computing devices would be a mistake with grave consequences for innovation and U.S. technological competitiveness.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Michael

Last Name: Bosch

Mailing Address: Flandernstrae 53/2

City: Esslingen

Country: Germany

State or Province: Baden-Wrttemberg

ZIP/Postal Code: 73732

Email Address:

Organization Name:

Comment: This regulation of the free ISM-Band cuts some essential needs of private developers and small start-ups. With the restriction of almost every wireless communication device to predefined modes and settings of usage, the new economic carriers of the future can't develop. This regulation distorts the economic development within a free market and gives bigger enterprises huge advantages over their smaller competitors. In order to maintain a fair level of competition between freelancers and multinational enterprises the FCC should discard this proposal.

On the other hand this proposal cuts the free development of private projects of students, etc. The education of the following generation would be very restricted leading to a lower innovation capability and thus gives economic competitors in other countries advantages in recruiting competent staff.

This regulation of the free ISM-Band cuts some essential needs of private developers and small start-ups. With the restriction of almost every wireless communication device to predefined modes and settings of usage, the new economic carriers of the future can't develop. This regulation distorts the economic development within a free market and gives bigger enterprises huge advantages over their smaller competitors. In order to maintain a fair level of competition between freelancers and multinational enterprises the FCC should discard this proposal.

On the other hand this proposal cuts the free development of private projects of students, etc. The education of the following generation would be very restricted leading to a lower innovation capability and thus gives economic competitors in other countries advantages in recruiting competent staff.

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: Stepan

Last Name: Semenukha

Mailing Address: 850 N Randolph St

City: Arlington

Country: United States

State or Province: VA

ZIP/Postal Code: 22203

Email Address: semenukha@gmail.com

Organization Name:

Comment: Hello,

I believe the proposed regulation violates basic human rights for freedom and encourages unfair competition. It creates grounds for certain corporations seizing control over the wireless device market and outlaws usage of free (libre) software. As such, this proposal is counterproductive and contradicts the spirit of U.S. Law.

Please withdraw this proposal. Thank you.

Hello,

I believe the proposed regulation violates basic human rights for freedom and encourages unfair competition. It creates grounds for certain corporations seizing control over the wireless device market and outlaws usage of free (libre) software. As such, this proposal is counterproductive and contradicts the spirit of U.S. Law.

Please withdraw this proposal. Thank you.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Francesco

Last Name: Cristaldi

Mailing Address: F.cristaldi@tin.it

City: Cosenza

Country: Italy

State or Province: Calabria

ZIP/Postal Code: 87100

Email Address: F.cristaldi@tin.it

Organization Name: Kristaldi.com

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: Lloyd

Last Name: Kvam

Mailing Address: 5 Foliage View

City: Lebanon

Country: United States

State or Province: NH

ZIP/Postal Code: 03766

Email Address: kvamlnk@gmail.com

Organization Name: null

Comment: The freedom to use low-cost wifi routers as special purpose network devices is invaluable. Open source firmware such as OpenWRT provide support for capabilities that were not envisioned by the manufacturer. I have used OpenWRT to implement filtering bridges that segment a network and block hostile network traffic. I currently use CeroWRT, an experimental firmware that implements experimental bandwidth algorithms that provide better latency than the manufacturer provided firmware. While these algorithms WILL become standard, they are not yet included in the default firmware.

CeroWRT could not have been developed without the ability to reflash router firmware. Researchers operating with tight budget constraints find these low cost devices to be ideal for testing new protocols and developing innovative products.

I expect you will be hearing from many organizations that have adapted routers to provide customized services to fit their needs. This will range from restaurants and other businesses providing hot spots to volunteer fire departments using customized routers to enhance communications.

Finally, the manufacturers have a poor record of providing security updates. Even when vulnerabilities are discovered, patches are not provided for older routers. OpenWRT provides innovative package management and sophisticated update procedures.

I hope you realize that whatever benefits you think will be gained from this rule come at a substantial cost to the general public in lost productivity and innovation.

The freedom to use low-cost wifi routers as special purpose network devices is invaluable. Open source firmware such as OpenWRT provide support for capabilities that were not envisioned by the manufacturer. I have used OpenWRT to implement filtering bridges that segment a network and block hostile network traffic. I currently use CeroWRT, an experimental firmware that implements experimental bandwidth algorithms that provide better latency than the manufacturer provided firmware. While these algorithms WILL become standard, they are not yet included in the default firmware.

CeroWRT could not have been developed without the ability to reflash router firmware. Researchers operating with tight budget constraints find these low cost devices to be ideal for testing new protocols and developing innovative products.

I expect you will be hearing from many organizations that have adapted routers to provide customized services to fit their needs. This will range from restaurants and other businesses providing hot spots to volunteer fire departments using customized routers to enhance communications.

Finally, the manufacturers have a poor record of providing security updates. Even when vulnerabilities are discovered, patches are not provided for older routers. OpenWRT provides innovative package management and sophisticated update procedures.

I hope you realize that whatever benefits you think will be gained from this rule come at a substantial cost to the general public in lost productivity and innovation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jake

Last Name: Lagant

Mailing Address: 8 Regent Road

City: Prague

Country: Czech Republic

State or Province: Prague

ZIP/Postal Code: 65926

Email Address: null

Organization Name: null

Comment: Please do not restrict the flashing of firmware on routers. What if I need to do something such as run a VPN to my corporate network, but I cannot due to not being able to flash firmware that is able to achieve that?

What do I do if there is a severe security bug in the stock firmware and I can't patch it myself? You're creating a hackers dream. Hackers already have enough power, don't give them more power by standardising firmware. One popular firmware gets a bug and millions of routers will be hijacked. Is this what you want?

What do you gain from this? Why take away the freedom from the users that buy the hardware for themselves, not for you?

Thank you for your time.

Please do not restrict the flashing of firmware on routers. What if I need to do something such as run a VPN to my corporate network, but I cannot due to not being able to flash firmware that is able to achieve that?

What do I do if there is a severe security bug in the stock firmware and I can't patch it myself? You're creating a hackers dream. Hackers already have enough power, don't give them more power by standardising firmware. One popular firmware gets a bug and millions of routers will be hijacked. Is this what you want?

What do you gain from this? Why take away the freedom from the users that buy the hardware for themselves, not for you?

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: Jeff

Last Name: Nemic

Mailing Address: 1411 William St

City: Baltimore

Country: United States

State or Province: MD

ZIP/Postal Code: 21230

Email Address:

Organization Name:

Comment: Please don't prevent us from using custom firmware on the routers we own.

Custom firmware has proved essential to me in several instances:

-To fix a bug preventing me from connecting more than one device to my router at a time. The manufacturer never fixed the issue.

-To provide useful features that the manufacturer did not. For example, my current router has a number of blue LEDs that light up my living room like a disco ball. The custom router allows me to turn those lights off when I don't need them, cutting out an annoyance and perhaps saving me money and extending the life of the device at the same time.

-Custom firmware also extends the functional life of electronic devices. Thanks to custom firmware on my router, I have been able to keep using my router long after the manufacturer had abandoned supporting it, saving me money and reducing waste. This is also the case with other electronics I own as well, including Android phones and MP3 players.

-Custom firmware can also increase the efficiency of electronics. Battery life improved 40% on my MP3 player when I installed custom firmware.

On top of this, allowing people to create custom firmware both speeds technological improvement and increases the number skilled tech workers.

Please don't prevent us from using custom firmware on the routers we own.

Custom firmware has proved essential to me in several instances:

-To fix a bug preventing me from connecting more than one device to my router at a time. The manufacturer never fixed the issue.

-To provide useful features that the manufacturer did not. For example, my current router has a number of blue LEDs that light up my living room like a disco ball. The custom router allows me to turn those lights off when I don't need them, cutting out an annoyance and perhaps saving me money and extending the life of the device at the same time.

-Custom firmware also extends the functional life of electronic devices. Thanks to custom firmware on my router, I have been able to keep using my router long after the manufacturer had abandoned supporting it, saving me money and reducing waste. This is also the case with other electronics I own as well, including Android phones and MP3 players.

-Custom firmware can also increase the efficiency of electronics. Battery life improved 40% on my MP3 player when I installed custom firmware.

On top of this, allowing people to create custom firmware both speeds technological improvement and increases the number skilled tech workers.

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: Gibbs

Mailing Address: 3501 Abingdon Rd.

City: Columbia

Country: United States

State or Province: SC

ZIP/Postal Code: 29203

Email Address: sbbig.je@gmail.com

Organization Name: James Gibbs

Comment: To whom this may concern,

This is wrong, and will stifle innovation.

James Gibbs

To whom this may concern,

This is wrong, and will stifle innovation.

James 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: sam

Last Name: micheal

Mailing Address: 123 abc

City: florida

Country: United States

State or Province: FL

ZIP/Postal Code: 6983049028

Email Address:

Organization Name:

Comment: Please stop ruining the tech world.

I believe this proposal will limit our ability to innovate and secure our own networks and devices. Any proposal which limits the owners ability to modify their own property has negative implications all across the board.

Researchers need to be able to test and modify devices to help build a more secure and better updated version of the technology. Owners need the ability to fix what the businesses wont. It has been done before in spite of the incompetence of the manufacturers.

Many businesses depend on the ability to install their software and modify the code of the device to better suite their applications.

sam, florida

Please stop ruining the tech world.

I believe this proposal will limit our ability to innovate and secure our own networks and devices. Any proposal which limits the owners ability to modify their own property has negative implications all across the board.

Researchers need to be able to test and modify devices to help build a more secure and better updated version of the technology. Owners need the ability to fix what the businesses wont. It has been done before in spite of the incompetence of the manufacturers.

Many businesses depend on the ability to install their software and modify the code of the device to better suite their applications.

sam, florida

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: P

Last Name: Hodson

Mailing Address: 20 Private Lane

City: Private

Country: United States

State or Province: PA

ZIP/Postal Code: 18032

Email Address: private@private.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