Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Andrew
Last Name: Tucker
Mailing Address: 4763 Shorecrest Drive
City: Orlando
Country: United States
State or Province: FL
ZIP/Postal Code: 32817
Email Address: tuckeran@gmail.com
Organization Name: self
Comment: Do NOT do this, Half of FCC/Congress don't even understand half of these terms. Keep our devices free! We've paid for them! Let us use them the way we want!

Do NOT do this, Half of FCC/Congress don't even understand half of these terms. Keep our devices free! We've paid for them! Let us use them the way we want!

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: Thomas
Last Name: Totty
Mailing Address: 1120 Sharon Drive
City: Chesapeake
Country: United States
State or Province: VA
ZIP/Postal Code: 23320
Email Address:
Organization Name:
Comment: Please do not pass this. I want to be able to fix security holes in my wireless devices. If this passes then companies would be able to charge for security software updates that I could otherwise implement myself.

Please do not pass this. I want to be able to fix security holes in my wireless devices. If this passes then companies would be able to charge for security software updates that I could otherwise implement myself.

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: Ripon Hossain
Last Name: Jewel
Mailing Address: riponhossain876@gmail.com
City: Dhaka
Country: Bangladesh
State or Province: Asia
ZIP/Postal Code: 1340
Email Address: riponhossain876@gmail.com
Organization Name: Bsc in computer science & engineering
Comment: I object this because security and privacy is important to me.Please don't do this

I object this because security and privacy is important to me.Please don't do this

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Andrew
Last Name: Brannon
Mailing Address: 696 Alberta Ave.
City: Sunnyvale
Country: United States
State or Province: CA
ZIP/Postal Code: 94087
Email Address: andrewebrannon@gmail.com
Organization Name:
Comment: It would be a bad idea to implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. Please do not implement rules that would be detrimental both to users and to commerce, as well as to computer security and stability.

It would be a bad idea to implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. Please do not implement rules that would be detrimental both to users and to commerce, as well as to computer security and stability.

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: Sears
Mailing Address: 2711 King St.
City: Bellingham
Country: United States
State or Province: WA
ZIP/Postal Code: 98225
Email Address:
Organization Name:
Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

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

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

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

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

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

Please Do Not Reply To This Email.

Public Comments on Equipment 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: Trevor
Last Name: Fenlon
Mailing Address: 245 Area Drive
City: mill valley
Country: United States
State or Province: CA
ZIP/Postal Code: 94941
Email Address: mista.t007@gmail.com
Organization Name:
Comment: Fcc, stop screwing us with our devices that we own. If i have bought a router or a computer, it should be my right to install my own OS on my devices instead of sticking with a propritary peice of garbage operating system like Windows 10 and OS X. Also, some people have the need to install a custom firmware on their routers to enable them to do things that a normal router can't do.

Fcc, stop screwing us with our devices that we own. If i have bought a router or a computer, it should be my right to install my own OS on my devices instead of sticking with a propritary peice of garbage operating system like Windows 10 and OS X. Also, some people have the need to install a custom firmware on their routers to enable them to do things that a normal router can't do.

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: Steven
Last Name: Hogan
Mailing Address: 1913 Magdalena Cir Apt 107
City: Santa Clara
Country: United States
State or Province: CA
ZIP/Postal Code: 95051
Email Address: stevehogan@stevehogan.com
Organization Name: None
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. My reasons include: 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; and, 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.

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. My reasons include: 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; and, 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: Anon
Last Name: Mous
Mailing Address: 1234 56th St.
City: West Des Moines
Country: United States
State or Province: IA
ZIP/Postal Code: 50266
Email Address:
Organization Name:
Comment: Hello. First off, I'd like to thank you for letting us provide feedback. Second of all, I believe this would infringe on the personal rights of all computer owners. We should be able to fix security problems that we have with our device, as well as download customized OSes.

Hello. First off, I'd like to thank you for letting us provide feedback. Second of all, I believe this would infringe on the personal rights of all computer owners. We should be able to fix security problems that we have with our device, as well as download customized OSes.

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: Will
Last Name: Denham
Mailing Address: 603 Carrigan Drive
City: Danville
Country: United States
State or Province: KY
ZIP/Postal Code: 40422
Email Address: techie.will@gmail.com
Organization Name:
Comment: This proposal stands to greatly hinder both the professional and enthusiast groups that enjoy technology so much.

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 and other software, which would be banned under the NPRM. This is a huge step back in t he wrong direction.

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.

If this act is to proceed forward, it needs a huge make over to exclude the above and the other hindrances it would impose on every day users.

This proposal stands to greatly hinder both the professional and enthusiast groups that enjoy technology so much.

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 and other software, which would be banned under the NPRM. This is a huge step back in t he wrong direction.

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.

If this act is to proceed forward, it needs a huge make over to exclude the above and the other hindrances it would impose on every day 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: Robert
Last Name: Clark II
Mailing Address: 206 5th Ave NE
City: Reform
Country: United States
State or Province: AL
ZIP/Postal Code: 35481
Email Address: coriolisstorm@gmail.com
Organization Name:
Comment: I do not think these rules should be implemented. The open source community would be severely affected by these rules. I have owned Android phones in the past as well as other devices where open source projects have closed security holes long after the manufacturer stopped supporting the device. OpenWRT router software is far more secure than most manufacturers firmware and continually updated to closer security holes after manufacturers abandon said devices. This is a step in the wrong direction.

I do not think these rules should be implemented. The open source community would be severely affected by these rules. I have owned Android phones in the past as well as other devices where open source projects have closed security holes long after the manufacturer stopped supporting the device. OpenWRT router software is far more secure than most manufacturers firmware and continually updated to closer security holes after manufacturers abandon said devices. This is a step in the wrong direction.

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: Nick
Last Name: Turner
Mailing Address: 5474 Mersea
City: Burke
Country: United States
State or Province: VA
ZIP/Postal Code: 22015
Email Address: nickpturner98@yahoo.com
Organization Name: null
Comment: Hello. I am asking that you do not follow through with your proposal to ban modifying devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. I had to install custom firmware on my Android device because my carrier would not put out an update to stop the stage fright virus.

Hello. I am asking that you do not follow through with your proposal to ban modifying devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. I had to install custom firmware on my Android device because my carrier would not put out an update to stop the stage fright virus.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Anonymous
Last Name: Anonymous
Mailing Address: Anonymous
City: Anonymous
Country: United States
State or Province: VA
ZIP/Postal Code: Anonymous
Email Address: null
Organization Name: null
Comment: Enacting these new rules will in essence make the United States less secure. The companies that create Wi-Fi routers do not update the firmware with any regularity or with any meaning full security updates. It is in the best interest of every individual to ensure that their home machines do not get compromised by various nefarious individuals. Open source alternatives are the best thing to keep your machines safe. Machines that are compromised can be used as a weapon to do damage to the U.S economy and security. Weather they are used in BOT nets or the information on personal and small businesses get stolen for financial gain, it is detrimental to the United States and its interests. Removing the ability to protect yourself empowers the enemies of the United States wither they are individuals, organizations or governments. Please do not make my information and my country less secure by removing the ability to modify a thing that I own.

Enacting these new rules will in essence make the United States less secure. The companies that create Wi-Fi routers do not update the firmware with any regularity or with any meaning full security updates. It is in the best interest of every individual to ensure that their home machines do not get compromised by various nefarious individuals. Open source alternatives are the best thing to keep your machines safe. Machines that are compromised can be used as a weapon to do damage to the U.S economy and security. Weather they are used in BOT nets or the information on personal and small businesses get stolen for financial gain, it is detrimental to the United States and its interests. Removing the ability to protect yourself empowers the enemies of the United States wither they are individuals, organizations or governments. Please do not make my information and my country less secure by removing the ability to modify a thing that I own.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: john
Last Name: smith
Mailing Address: 2504 longview st.
City: austin
Country: United States
State or Province: TX
ZIP/Postal Code: 78705
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Cutler
Last Name: Fritz
Mailing Address: 1915 NW 38th Terrace
City: Gainesville
Country: United States
State or Province: FL
ZIP/Postal Code: 32605
Email Address: madseacowpro@gmail.com
Organization Name:
Comment: Good day,

I, Cutler Fritz, respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. There are many reasons why I believe this course of action would be deterimental. For instance, 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 also firmly believe in my right to do what I wish with the products I have purchased, if I wish to install an alternative firmware on my phone that lets me add features that the developers have deemed unnessacary for me to have access to, then I am in my right to do so because I have bought and paid for a product that is mine to modify as I see fit.

Respectfully ,
Cutler Fritz

Good day,

I, Cutler Fritz, respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. There are many reasons why I believe this course of action would be deterimental. For instance, 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 also firmly believe in my right to do what I wish with the products I have purchased, if I wish to install an alternative firmware on my phone that lets me add features that the developers have deemed unnessacary for me to have access to, then I am in my right to do so because I have bought and paid for a product that is mine to modify as I see fit.

Respectfully ,
Cutler Fritz

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Benjamin
Last Name: Meredith
Mailing Address: 6106 Alfred blvd
City: Punta Gorda
Country: United States
State or Province: FL
ZIP/Postal Code: 33982
Email Address: bmeredith331@gmail.com
Organization Name:
Comment: Hi, my name is Benjamin James Meredith, and to be honest I think this isn't an incredibly smart idea or bill to pass. by not allowing users to install their own software of their own choosing greatly impacts the users freedom to do as they please with the hardware they bought. Wireless networking research hinges on the ability of researchers to investigate and modify their own devices, and if this bill passes it kills jobs and doesn't allow for humanity as a whole to progress and research new and interesting RF ideas. And as an American citizen I've always valued being able to do something like fixing problems where manufacturers won't. It's what makes being American so amazing is that we have an ability to fix things ourselves without the help of others or big corporations if the opportunity arrives. Passing this will prevent future users from doing what others have done in the past, fixing serious bugs that would be banned under 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.

Hi, my name is Benjamin James Meredith, and to be honest I think this isn't an incredibly smart idea or bill to pass. by not allowing users to install their own software of their own choosing greatly impacts the users freedom to do as they please with the hardware they bought. Wireless networking research hinges on the ability of researchers to investigate and modify their own devices, and if this bill passes it kills jobs and doesn't allow for humanity as a whole to progress and research new and interesting RF ideas. And as an American citizen I've always valued being able to do something like fixing problems where manufacturers won't. It's what makes being American so amazing is that we have an ability to fix things ourselves without the help of others or big corporations if the opportunity arrives. Passing this will prevent future users from doing what others have done in the past, fixing serious bugs that would be banned under 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: Jonathan
Last Name: Traynor
Mailing Address: 1125 Grove Street N.E.
City: Palm Bay
Country: United States
State or Province: FL
ZIP/Postal Code: 32905
Email Address: Jonathan.Traynor@hotmail.com
Organization Name:
Comment: Consumers should be able to modify the software of their routers. More often than not current tech companies produce mediocre GUI interfaces, that don't work. Everytime I have bought a router I have had to change the operating software to get what I need out of it. These are simple things such as QoS routing, stronger encryption, and a more robust guest network.

While I understand that some people hack their router to overboost their Tx signal they are few and far between, I believe that there would be a better way to prevent that from happening via some hardware modification. Although those who want to do it will just modify the hardware then. Please allow me to continue to use my custom software for my routers.

Consumers should be able to modify the software of their routers. More often than not current tech companies produce mediocre GUI interfaces, that don't work. Everytime I have bought a router I have had to change the operating software to get what I need out of it. These are simple things such as QoS routing, stronger encryption, and a more robust guest network.

While I understand that some people hack their router to overboost their Tx signal they are few and far between, I believe that there would be a better way to prevent that from happening via some hardware modification. Although those who want to do it will just modify the hardware then. Please allow me to continue to use my custom software for my 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: Tyler
Last Name: Kropp
Mailing Address: 5 Nadelhoffer Ct.
City: Woodridge
Country: United States
State or Province: IL
ZIP/Postal Code: 60517
Email Address: tkdestroyer2@gmail.com
Organization Name:
Comment: The sort of changes this rule makes is an infringement of our rights as consumers in the area of technology. There is no possible way this can succeed.

The sort of changes this rule makes is an infringement of our rights as consumers in the area of technology. There is no possible way this can succeed.

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: Thomas
Last Name: Naugle
Mailing Address: 9 County Road 1090
City: Oxford
Country: United States
State or Province: MS
ZIP/Postal Code: 38655
Email Address: tnaugle@go.olemiss.edu
Organization Name:
Comment: To whom it may concern,

This proposed rule would completely stifle the innovation of future networking technologies. I know many computer hobbyists who are passionate about customized routers to control their home network security. Many companies rely on open source networking software/OSes (like OpenBSD) for their daily operations, and the maintenance of this software depends on the continuing tinkering by hobbyists. Additionally, building customized routers with open source operating systems is an invaluable educational tool for networking.

This proposed rule would stifle innovation by getting in the way of open source developers and networking students alike.

To whom it may concern,

This proposed rule would completely stifle the innovation of future networking technologies. I know many computer hobbyists who are passionate about customized routers to control their home network security. Many companies rely on open source networking software/OSes (like OpenBSD) for their daily operations, and the maintenance of this software depends on the continuing tinkering by hobbyists. Additionally, building customized routers with open source operating systems is an invaluable educational tool for networking.

This proposed rule would stifle innovation by getting in the way of open source developers and networking students alike.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Mark
Last Name: Perri
Mailing Address: 5 Plaza Loma
City: Novato
Country: United States
State or Province: CA
ZIP/Postal Code: 94947
Email Address:
Organization Name:
Comment: Please do not take away the ability for me to install the software of my choosing on my computing device. I rely on the ability to upgrade software myself when bugs are found to keep my house secure. The ability to install new firmware on devices, openWRT on my router, linux on my computer, and android ROM on my phone ensures that I can use my hardware as I intend, and in the most secure way possible.

Please do not take away the ability for me to install the software of my choosing on my computing device. I rely on the ability to upgrade software myself when bugs are found to keep my house secure. The ability to install new firmware on devices, openWRT on my router, linux on my computer, and android ROM on my phone ensures that I can use my hardware as I intend, and in the most secure way possible.

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: caldwell
Mailing Address: 14432 weller ln
City: queens
Country: United States
State or Province: NY
ZIP/Postal Code: 11422
Email Address:
Organization Name:
Comment: I am wholly against the implementation of 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 wholly against the implementation of 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: Alexander
Last Name: Taylor
Mailing Address: 6334 E Placita Neptuno
City: Tucson
Country: United States
State or Province: AZ
ZIP/Postal Code: 85710
Email Address: enneract@fingerbox.es
Organization Name:
Comment: This proposal is literally one of the worst ideas which the Commission has ever had under consideration.

I believe that outlawing all wireless communication other than carrier pigeon would have a lesser effect on our economy, and personal liberty.

This proposal is literally one of the worst ideas which the Commission has ever had under consideration.

I believe that outlawing all wireless communication other than carrier pigeon would have a lesser effect on our economy, and personal liberty.

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: Ash
Last Name: B
Mailing Address: #229 sfs 407 yelahabka new town
City: bangalore
Country: India
State or Province: Karnataka
ZIP/Postal Code: 560064
Email Address: ash32911@gmail.com
Organization Name:
Comment: To the FCC,

While we as the public understand and commend your efforts to keep us secure and safe. We would still like the ability to install software of our own choosing. We feel that this move may infringe on our personal and digital rights. We would be very disheartened and upset if we would lose the ability to install custom firmware. This move will only limit development and hinder further efforts to improve products beyond what the manufacturer might be able to. Please reconsider this policy.

Thanking you ,
Ash B

To the FCC,

While we as the public understand and commend your efforts to keep us secure and safe. We would still like the ability to install software of our own choosing. We feel that this move may infringe on our personal and digital rights. We would be very disheartened and upset if we would lose the ability to install custom firmware. This move will only limit development and hinder further efforts to improve products beyond what the manufacturer might be able to. Please reconsider this policy.

Thanking you ,
Ash B

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: Joah
Last Name: Fitzgerald
Mailing Address: 150 N Yamhill St
City: Carlton
Country: United States
State or Province: OR
ZIP/Postal Code: 97111
Email Address: joahfitzgerald@gmail.com
Organization Name: null
Comment: The FCC Should not be able to regulate human beings in the manner. If an object is purchased, the owner has full rights to the object, and there should be no law prohibiting humans personal lives from being protected by open source software. Purchasing electronics is the same as purchasing anything. Modifying a human's own personal belongings should never be regulated, especially by a governing body. There are no laws prohibiting one from modifying clothing purchased to custom fit one's body, and the same should be so about personal owned electronics.

This rule will easily pave the way for terrible changes in other policies and allow more abuse of the system then by deregulating custom personal uses of ones' own purchased objects, and allow for a situation similar to patents and copyrights that are being used in an abusive manner.

This terrible ruling removes privacy, and in many cases the safety of peoples lives. Open source software has been used by many to provide anonymity and security that cannot be otherwise obtained without the use of custom firmware and software.

I urge anyone viewing this comment to comment about your feelings regarding this issue. It is imperative to the future law and security of mankind during the information age, that this proposed rule not pass.

Thank you for this opportunity to comment.

The FCC Should not be able to regulate human beings in the manner. If an object is purchased, the owner has full rights to the object, and there should be no law prohibiting humans personal lives from being protected by open source software. Purchasing electronics is the same as purchasing anything. Modifying a human's own personal belongings should never be regulated, especially by a governing body. There are no laws prohibiting one from modifying clothing purchased to custom fit one's body, and the same should be so about personal owned electronics.

This rule will easily pave the way for terrible changes in other policies and allow more abuse of the system then by deregulating custom personal uses of ones' own purchased objects, and allow for a situation similar to patents and copyrights that are being used in an abusive manner.

This terrible ruling removes privacy, and in many cases the safety of peoples lives. Open source software has been used by many to provide anonymity and security that cannot be otherwise obtained without the use of custom firmware and software.

I urge anyone viewing this comment to comment about your feelings regarding this issue. It is imperative to the future

law and security of mankind during the information age, that this proposed rule not pass.

Thank you for this opportunity to comment.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: T
Last Name: G
Mailing Address: 1048 Wagonwheel Drive
City: Fort Collins
Country: United States
State or Province: CO
ZIP/Postal Code: 80526
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 such as routers and PCs.
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.
Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
Users should be able to manipulate and control all aspects of their devices.
The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and systems.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices such as routers and PCs.
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.
Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
Users should be able to manipulate and control all aspects of their devices.
The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
These new rules will make it extremely difficult if not illegal, to make an open source baseband for cellphones to prevent rogue towers like Stingrays. It will also harm any attempts to build open source cell towers and 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: Patrick
Last Name: Spinler
Mailing Address: 403 Sixth St Sw
City: Kasson
Country: United States
State or Province: MN
ZIP/Postal Code: 55944
Email Address:
Organization Name:
Comment: To Whom it May Concern:

I request that this proposed rule not block consumers from installing alternate, third party, open source, or home created software on consumer wireless devices.

I currently install open source or alternate software on all of my smart phones, and tablet devices, and several of my laptops with embedded wifi. Such a proposed rule would prevent me from legally doing so.

Sincerely,
Patrick Spinler

To Whom it May Concern:

I request that this proposed rule not block consumers from installing alternate, third party, open source, or home created software on consumer wireless devices.

I currently install open source or alternate software on all of my smart phones, and tablet devices, and several of my laptops with embedded wifi. Such a proposed rule would prevent me from legally doing so.

Sincerely,
Patrick Spinler

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: Austin
Last Name: DeLauney
Mailing Address: 5425 Broadwater lane
City: Clarksville
Country: United States
State or Province: MD
ZIP/Postal Code: 21029
Email Address: adelauney96@outlook.com
Organization Name: null
Comment: Please do not implement this! It is our right to put what we want out our products. You should not do this because timely updates may not be put out regularly and gaping security holes may be left wide open. Another reason why we should not have this is because after you purchase something it should be your right to do whatever you want with it.

Please do not implement this! It is our right to put what we want out our products. You should not do this because timely updates may not be put out regularly and gaping security holes may be left wide open. Another reason why we should not have this is because after you purchase something it should be your right to do whatever you want with it.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Jim
Last Name: Ekleberry
Mailing Address: 1000 Worthington Ln #30-311
City: Spring Hill
Country: United States
State or Province: TN
ZIP/Postal Code: 37174
Email Address:
Organization Name:
Comment: The FCC should rescind the proposal contained in Document number 2015-18402 regarding wireless devices. The reason for my suggestion is due to the proposal being too broad, it will limit functionality available to consumers for the equipment they have purchased, and open consumers up to potential security breaches.

The FCC should rescind the proposal contained in Document number 2015-18402 regarding wireless devices. The reason for my suggestion is due to the proposal being too broad, it will limit functionality available to consumers for the equipment they have purchased, and open consumers up to potential security breaches.

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: Oliver
Last Name: Faso
Mailing Address: 21 Hancock Avenue
City: Newton
Country: United States
State or Province: MA
ZIP/Postal Code: 02459
Email Address: oli1243@live.com
Organization Name:
Comment: Dear FCC reader,
Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. With this right being restricted, the development of technology for the greater good will also be restricted. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This is a problem that is unfortunately common, and to prevent consumers from fixing security problems themselves will cause more theft of information and problems with devices. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Banning this would, again, cause problems with information theft. 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. Without freedom to employ fitting software, many companies' and people's devices will not be able to function as they are and they will have to employ possibly unfitting software for a purpose the software was not meant for or badly functions doing.

Dear FCC reader,
Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. With this right being restricted, the development of technology for the greater good will also be restricted. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This is a problem that is unfortunately common, and to prevent consumers from fixing security problems themselves will cause more theft of information and problems with devices. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Banning this would, again, cause problems with information theft. 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. Without freedom to employ fitting software, many companies' and people's devices will not be able to function as they are and they will have to employ possibly unfitting software for a purpose the software was not meant for or badly functions doing.

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: Hunter
Last Name: kauffman
Mailing Address: 140 lazy laurel chase
City: roswell
Country: United States
State or Province: GA
ZIP/Postal Code: 30076
Email Address: hkauffman@gmail.com
Organization Name: georgia institute of technology
Comment: As someone involved in network security and its research, this would be detrimental to the already poor state of cybersecurity

As someone involved in network security and its research, this would be detrimental to the already poor state of cybersecurity

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Eric
Last Name: Ayers
Mailing Address: 1106 Lakeside Village Dr SE
City: Atlanta
Country: United States
State or Province: GA
ZIP/Postal Code: 30317
Email Address: ericzundel@gmail.com
Organization Name:
Comment: I do not like the restricting of the ability to upload custom firmware on devices like mobile phones, tablets, and routers. Multiple times in the past I have been forced to load 3rdparty software on these devices in order to get continued use out of them due to:

- Security defects
- Incompatibility with a device (Connecting a new macbook to my wireless router)
- Incompatibility with a network (Connecting via VPN over a wireless router with broken software)
- Hardware that has aged and is no longer supported by the manufacturer and unable to use new features (Loading cyanogenmod on older Android phones)

Hardware manufacturers are incentivized to provide only stable functionality on old devices and to encourage their disuse and buying new hardware. That does not always align with consumer needs. Third party and open source software helps use extend the life of old devices and perform research into new protocols and extend compatibility to devices that were not invented at the time the device was manufactured.

I do not like the restricting of the ability to upload custom firmware on devices like mobile phones, tablets, and routers. Multiple times in the past I have been forced to load 3rdparty software on these devices in order to get continued use out of them due to:

- Security defects
- Incompatibility with a device (Connecting a new macbook to my wireless router)
- Incompatibility with a network (Connecting via VPN over a wireless router with broken software)
- Hardware that has aged and is no longer supported by the manufacturer and unable to use new features (Loading cyanogenmod on older Android phones)

Hardware manufacturers are incentivized to provide only stable functionality on old devices and to encourage their disuse and buying new hardware. That does not always align with consumer needs. Third party and open source software helps use extend the life of old devices and perform research into new protocols and extend compatibility to devices that were not invented at the time the device was manufactured.

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: Simon
Last Name: Alveteg
Mailing Address: Skarpskyttevgen 28A
City: Lund
Country: Sweden
State or Province: Skne
ZIP/Postal Code: 22642
Email Address:
Organization Name:
Comment:
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.

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: Fan
Last Name: Zhang
Mailing Address: 2851 Thedford Rd
City: Bloomfield Hills
Country: United States
State or Province: MI
ZIP/Postal Code: 48304-2059
Email Address: masterfan@gmail.com
Organization Name:
Comment: It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems. The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology. On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures. Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM. The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent. I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems. The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology. On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's

powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures. Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM. The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent. I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Richard
Last Name: M
Mailing Address: Not needed
City: Lagrange
Country: United States
State or Province: KY
ZIP/Postal Code: 40031
Email Address: Pacmanninja998@gmail.com
Organization Name: Mr.
Comment: Hi I'm an 18 year old Kentuckian. I've owned many wireless devices, that I has loaded aftermarket kernels on.
Although most people wohnt exploit the airways, and those that do will always find a way around the device locks. Why punish every developer, customization, or efficiency seeker? There must be a better answer, such as looking for new communication methods for communicating with and administrating transportation.

Hi I'm an 18 year old Kentuckian. I've owned many wireless devices, that I has loaded aftermarket kernels on.
Although most people wohnt exploit the airways, and those that do will always find a way around the device locks. Why punish every developer, customization, or efficiency seeker? There must be a better answer, such as looking for new communication methods for communicating with and administrating transportation.

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: Travis
Last Name: Bonnett
Mailing Address: 800 S Mattis Ave, Apt D-5
City: Champaign
Country: United States
State or Province: IL
ZIP/Postal Code: 61821
Email Address:
Organization Name:
Comment: I am not sure why FCC wants to ban consumers, or in the other words: the American people from making changes to devices that they brought with their own money and they own, not lease. Americans should be allowed to modify and tinker with their computers and devices as see fit. The vast majority of Americans who tinker with their devices are not terrorists or criminals; they just like to tinker with their devices. If this rule is passed, generations of tinkers and open source software developers will be harmed by the government who is supposedly commitment to innovation.

I am not sure why FCC wants to ban consumers, or in the other words: the American people from making changes to devices that they brought with their own money and they own, not lease. Americans should be allowed to modify and tinker with their computers and devices as see fit. The vast majority of Americans who tinker with their devices are not terrorists or criminals; they just like to tinker with their devices. If this rule is passed, generations of tinkers and open source software developers will be harmed by the government who is supposedly commitment to 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: Hyun Jun
Last Name: Jin
Mailing Address: 250 Overpeck Avenue
City: Ridgefield Park
Country: United States
State or Province: NJ
ZIP/Postal Code: 07660
Email Address:
Organization Name:
Comment: I am a computer science student at Tufts University. Although the intentions of this rule can be good and could lead to some benefits, the reality is that the majority of users being affected by this rule are just technology-loving consumers with absolutely no malicious intent. I urge you to consider the many users on sites like http://forum.xda-developers.com/ that love customizing and installing various things on their phones (me included), purely for our own enjoyment.

I am a computer science student at Tufts University. Although the intentions of this rule can be good and could lead to some benefits, the reality is that the majority of users being affected by this rule are just technology-loving consumers with absolutely no malicious intent. I urge you to consider the many users on sites like http://forum.xda-developers.com/ that love customizing and installing various things on their phones (me included), purely for our own enjoyment.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Anonymous
Last Name: Penguin
Mailing Address: 154 Calumet Street
City: Boston
Country: United States
State or Province: MA
ZIP/Postal Code: 02120
Email Address: null
Organization Name: null
Comment: Please do not implement any laws that will make it illegal for me to install software that I choose on my OWN devices. Where do you get off even thinking that it is acceptable for you to tell me what software I can and cannot install on a device that I own. How do you even think you're going to enforce this?

Users in the past have patched security vulnerabilities that manufacturers themselves have failed to fix. This would not be possible without free use of our own devices. Researches won't be allowed to mod their systems to find ways to make better software either. This law would halt expansion and open us up to more spying and security holes.

Manufacturers only care about their bottom line, and if patching a security hole doesn't align with that, they won't do it. Allow the users to take charge of their own lives.

Please do not implement any laws that will make it illegal for me to install software that I choose on my OWN devices. Where do you get off even thinking that it is acceptable for you to tell me what software I can and cannot install on a device that I own. How do you even think you're going to enforce this?

Users in the past have patched security vulnerabilities that manufacturers themselves have failed to fix. This would not be possible without free use of our own devices. Researches won't be allowed to mod their systems to find ways to make better software either. This law would halt expansion and open us up to more spying and security holes.

Manufacturers only care about their bottom line, and if patching a security hole doesn't align with that, they won't do it. Allow the users to take charge of their own lives.

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: Rigney
Mailing Address: 2141 Route 38 APT 1401
City: Cherry Hill
Country: United States
State or Province: NJ
ZIP/Postal Code: 08002
Email Address:
Organization Name:
Comment: I would like to respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. This issue is of particular significance to me. I am an electrical engineer who routinely designs and field tests next-generation radios using SDR's as a platform. Limitations on the flexibility of SDR's would make it extremely difficult for researchers to develop new technologies which address the electromagnetic spectrum challenges which currently exist (and will only get worse in the future).

In addition:

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

Wireless networking research depends on the ability of researchers to investigate and modify their devices. This issue is of particular significance to me. I am an electrical engineer who routinely designs and field tests next-generation radios using SDR's as a platform. Limitations on the flexibility of SDR's would make it extremely difficult for researchers to develop new technologies which address the electromagnetic spectrum challenges which currently exist (and will only get worse in the future).

In addition:

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: Charles
Last Name: Tam
Mailing Address: 2593 Douglas Ln
City: Thompsons Station
Country: United States
State or Province: TN
ZIP/Postal Code: 37179
Email Address: Charles_Tam@outlook.com
Organization Name:
Comment: To whom it may concern;

I would like for you to consider withdrawing this proposal.There are many things that concern me about this proposal.
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.

Restricting the ability work on and experiment on technologies is much like restricting one's ability to work on their own car. Americans enjoy and use this freedom, and rarely is it done with malicious intent.

To whom it may concern;

I would like for you to consider withdrawing this proposal.There are many things that concern me about this proposal.
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.

Restricting the ability work on and experiment on technologies is much like restricting one's ability to work on their own car. Americans enjoy and use this freedom, and rarely is it done with malicious intent.

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: Illya
Last Name: Yefimenko
Mailing Address: 301 Heights ln apt 33c
City: Feasterville
Country: United States
State or Province: PA
ZIP/Postal Code: 19053
Email Address:
Organization Name:
Comment:

Public servants of the Federal Communications Commission,

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

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

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

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

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

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the

implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Edgar
Last Name: Costa
Mailing Address: 935 Saint Nicholas Avenue #4E
City: New York
Country: United States
State or Province: NY
ZIP/Postal Code: 10032
Email Address: edgarcosta@nyu.edu
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Ian
Last Name: Scott
Mailing Address: 1770 Kings Point Blvd.
City: Kissimmee
Country: United States
State or Province: FL
ZIP/Postal Code: 34744
Email Address: ian243@live.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.

Please allow personal use.

Thank you,

-Ian Scott

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.

Please allow personal use.

Thank you,

-Ian 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: David
Last Name: Sikes
Mailing Address: 2001 Dartmouth Ave
City: Winter Park
Country: United States
State or Province: FL
ZIP/Postal Code: 32789
Email Address: pockybum522@gmail.com
Organization Name:
Comment: Please do not do this. This policy would be extremely overreaching and ban many of the things I take for granted at the moment:

DD-WRT on my router
Custom ROMs on my Android phone
Wireless security research

Please do not do this. This policy would be extremely overreaching and ban many of the things I take for granted at the moment:

DD-WRT on my router
Custom ROMs on my Android phone
Wireless security 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: M
Last Name: D
Mailing Address: 123 Main Streete
City: Glendale
Country: United States
State or Province: CA
ZIP/Postal Code: 91205
Email Address:
Organization Name:
Comment: This is a solution in search of a problem. Limiting the firmware available on routers will limit innovation and usability. It will allow manufacturers to "race to the bottom" of firmware. Whereas the availability and widespread use of alternative router firmware has pushed manufacturers to improve their software.

This is an ill-conceived proposal that the FCC should roundly reject. It is anti-competitive and serves only to protect router manfacturers.

This is a solution in search of a problem. Limiting the firmware available on routers will limit innovation and usability. It will allow manufacturers to "race to the bottom" of firmware. Whereas the availability and widespread use of alternative router firmware has pushed manufacturers to improve their software.

This is an ill-conceived proposal that the FCC should roundly reject. It is anti-competitive and serves only to protect router manfacturers.

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: Jeremy
Last Name: Barrentine
Mailing Address: 509 E Hampton St
City: Darlington
Country: United States
State or Province: SC
ZIP/Postal Code: 29532
Email Address:
Organization Name:
Comment: The movement by the FCC to effectively lock down devices like PCs, cell phones, and routers should be seed as short sighted and the proposal modified or dismissed.

Much of the public wishes to install open source Operating Systems like Linux on their computers, which this proposal will affect. They also install open source firmware on their routers and even flash their own phones in various ways.

Making these efforts illegal not only creates criminals out of a pool of law abiding citizens but discourages curiosity in the young and destroys the ability to discover and learn about the technology of today by those who will create it tomorrow. The world turns on the deeds of the ordinary citizen. Without the knowledge the home tinkerer gains from his own endeavors we as a country will be left wanting at a time when all curiosity should be cultivated that we might better excel in the world market.

What is currently being considered is overreach and should be carefully modified to exempt such tinkering by the average individual in good faith or scrapped altogether.

Please make the correct, logical choice on behalf of the people and not on behalf of corporations.

The movement by the FCC to effectively lock down devices like PCs, cell phones, and routers should be seed as short sighted and the proposal modified or dismissed.

Much of the public wishes to install open source Operating Systems like Linux on their computers, which this proposal will affect. They also install open source firmware on their routers and even flash their own phones in various ways.

Making these efforts illegal not only creates criminals out of a pool of law abiding citizens but discourages curiosity in the young and destroys the ability to discover and learn about the technology of today by those who will create it tomorrow. The world turns on the deeds of the ordinary citizen. Without the knowledge the home tinkerer gains from his own endeavors we as a country will be left wanting at a time when all curiosity should be cultivated that we might better excel in the world market.

What is currently being considered is overreach and should be carefully modified to exempt such tinkering by the average individual in good faith or scrapped altogether.

Please make the correct, logical choice on behalf of the people and not on behalf of corporations.