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: Nicholas
Last Name: Ver Hoeve
Mailing Address: 17525 NE 40th St
City: Redmond
Country: United States
State or Province: WA
ZIP/Postal Code: 98052
Email Address: ALLULTIMA1@GMAIL.COM
Organization Name:
Comment: I find the requirement for manufacturers to "secure" the labels to be troubling. While the proposal describes security against a "third party", casting such a net will clearly catch the end user as well. I understand the labels are optional, but the incentive to manufacturers here is awful.

The bad incentive is asking for security (of any kind) against the end user. Keep in mind that manufacturers (especially in very small devices) ARE UNLIKELY TO SCOPE THEIR SECURITY TO ONLY PROTECT THE LABEL. Because it is cost effective, many manufacturers will choose to store this label in firmware, and then "lock down" the entire firmware and/or bootloader. This is extremely unfortunate, in my opinion.

Customer access to firmware and bootloaders is already hanging by but a thread in many devices, especially phones but also laptops. Some manufacturers seem to be doing everything possible to convince customers to accept a more submissive role where they accept a restricted device as is. When the customer does not have administrative authority over their own device, they are subject to things like forced telemetry and whatever fee extraction model they feel like pushing. That has nothing to do with labels, but the label security requirement will shift costs to encourage this even more. Ideally, manufacturers don't even develop technology intended to keep the end user out of any critical state for the device. Mobile phones are already heading down the path of the restricted end-user (unfortunately), but some hardware has no notion of "locking out the end user" (and this is a good thing!). In my opinion, the end user is the root authority and has unrestricted administrative privileges over their own device.

Please take a softer, alternative approach. Please require that component resellers know that removing/changing the label before resale is unacceptable. I would encourage separation of the label from other data which might be updated/refreshed/wiped. But forcing manufacturers to "secure" it is not the answer. The cure would be worse than the symptom, by far.

I find the requirement for manufacturers to "secure" the labels to be troubling. While the proposal describes security against a "third party", casting such a net will clearly catch the end user as well. I understand the labels are optional, but the incentive to manufacturers here is awful.

The bad incentive is asking for security (of any kind) against the end user. Keep in mind that manufacturers (especially in very small devices) ARE UNLIKELY TO SCOPE THEIR SECURITY TO ONLY PROTECT THE LABEL. Because it is cost effective, many manufacturers will choose to store this label in firmware, and then "lock down" the entire firmware and/or bootloader. This is extremely unfortunate, in my opinion.

Customer access to firmware and bootloaders is already hanging by but a thread in many devices, especially phones but

also laptops. Some manufacturers seem to be doing everything possible to convince customers to accept a more submissive role where they accept a restricted device as is. When the customer does not have administrative authority over their own device, they are subject to things like forced telemetry and whatever fee extraction model they feel like pushing. That has nothing to do with labels, but the label security requirement will shift costs to encourage this even more. Ideally, manufacturers don't even develop technology intended to keep the end user out of any critical state for the device. Mobile phones are already heading down the path of the restricted end-user (unfortunately), but some hardware has no notion of "locking out the end user" (and this is a good thing!). In my opinion, the end user is the root authority and has unrestricted administrative privileges over their own device.

Please take a softer, alternative approach. Please require that component resellers know that removing/changing the label before resale is unacceptable. I would encourage separation of the label from other data which might be updated/refreshed/wiped. But forcing manufacturers to "secure" it is not the answer. The cure would be worse than the symptom, by far.

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: Dana
Last Name: Clark
Mailing Address: 3200 Loch Ness Drive, #150
City: Lexington
Country: United States
State or Province: KY
ZIP/Postal Code: 40517
Email Address: skyblast83@gmail.com
Organization Name:
Comment: As a constant computer user, I must request that you not implement rules that take away the ability of users to install the software of their choosing on their computing devices. My reasons are as follows:

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.

As a constant computer user, I must request that you not implement rules that take away the ability of users to install the software of their choosing on their computing devices. My reasons are as follows:

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: Brian
Last Name: Davis
Mailing Address: UNCSA# 1278 1533 Broken Rock Dr.
City: Winston-Salem
Country: United States
State or Province: NC
ZIP/Postal Code: 27127
Email Address:
Organization Name:
Comment: Please do to not implement rules which take away the ability of users to install the software of their choosing on their computing devices.

Such a rule would be detrimental because:

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

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

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

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

Thank you for your time.

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

Such a rule would be detrimental because:

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

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

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

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

Thank you for your time.

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: Dylan
Last Name: Weber
Mailing Address: 296 Linden Park Place
City: Highland Park
Country: United States
State or Province: IL
ZIP/Postal Code: 60035
Email Address: weber1075@gmail.com
Organization Name:
Comment: The authorization of RF device firmware would prevent third-party firmware from being installed on typical networking devices that commonly use SoCs (system on a chip). This would be a big step backwards for the large community who try to extract the usefulness of the hardware that powers their networks. Taking away the public right for people to control the hardware they buy would be detrimental to network admins and typical computer users everywhere by setting the precedent for available management of any given hardware.

The authorization of RF device firmware would prevent third-party firmware from being installed on typical networking devices that commonly use SoCs (system on a chip). This would be a big step backwards for the large community who try to extract the usefulness of the hardware that powers their networks. Taking away the public right for people to control the hardware they buy would be detrimental to network admins and typical computer users everywhere by setting the precedent for available management of any given hardware.

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: Merton
Last Name: Duncan
Mailing Address: 11011 Woodmeadow parkway Apt 516
City: Dallas
Country: United States
State or Province: TX
ZIP/Postal Code: 75228-1490
Email Address: youwontliveforever@gmail.com
Organization Name:
Comment: I'd ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

You may of gotten many messages that seem identical to this one but personal freedom is at risk when considering implementing rules that in the end remove not only the choice to use certain software, but it would severely damage competition in the software market and history shows that when competition is removed everybody suffers.

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

You may of gotten many messages that seem identical to this one but personal freedom is at risk when considering implementing rules that in the end remove not only the choice to use certain software, but it would severely damage competition in the software market and history shows that when competition is removed everybody suffers.

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: Rand
Last Name: Hunt
Mailing Address: 1967 Courtland Avenue
City: Oakland
Country: United States
State or Province: CA
ZIP/Postal Code: 94601
Email Address: barukh@gmail.com
Organization Name: 1994
Comment: I want to tell you that being able to to install opensource software onto devices that you own is essential to freedom. These new regulations will inhibit innovation, limit freedom, and make a increase the profit margin of a few major manufacturers. Should we kill an innovative economy without receiving a benefit? OpenWRT and Linux have both played key roles in my own learning process leading me deeper and deeper into my understanding of how a computer works. Please protect this freedom. Anything else would be self sabotaging our development.

I want to tell you that being able to to install opensource software onto devices that you own is essential to freedom. These new regulations will inhibit innovation, limit freedom, and make a increase the profit margin of a few major manufacturers. Should we kill an innovative economy without receiving a benefit? OpenWRT and Linux have both played key roles in my own learning process leading me deeper and deeper into my understanding of how a computer works. Please protect this freedom. Anything else would be self sabotaging our development.

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: Mike
Last Name: Thiem
Mailing Address: 807-3102 Windsor Gate
City: Coquitlam
Country: Canada
State or Province: British Columbia
ZIP/Postal Code: V3B0J3
Email Address: mike.j.thiem@gmail.com
Organization Name:
Comment: I strongly believe that no action should be taken, nor ruling passed by the FCC or any other organization to limit the freedom of people using or creating custom firmware for their routers. There seems to be far too much room for interpretation in these rules, potentially providing the FCC with excessive and unjustifiable power to unreasonably limit the freedom of consumers and users of technology. I therefore cannot support these rules, and I would recommend that they not be enacted in their current form.

I strongly believe that no action should be taken, nor ruling passed by the FCC or any other organization to limit the freedom of people using or creating custom firmware for their routers. There seems to be far too much room for interpretation in these rules, potentially providing the FCC with excessive and unjustifiable power to unreasonably limit the freedom of consumers and users of technology. I therefore cannot support these rules, and I would recommend that they not be enacted in their current form.

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: Marc
Last Name: Wolpert
Mailing Address: 328 carl avenue
City: belleair
Country: United States
State or Province: FL
ZIP/Postal Code: 33756
Email Address: mewolpert@gmail.com
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Alex
Last Name: Haesche
Mailing Address: 1133 grape dr
City: moses lake
Country: United States
State or Province: WA
ZIP/Postal Code: 98837
Email Address:
Organization Name:
Comment: Please FCC, do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Here are a few reasons:

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

On top of that, I want to continue the following:

Install alternative operating systems on my PC, like GNU/Linux, OpenBSD, FreeBSD, etc.
Research into advanced wireless technologies, like mesh networking and bufferbloat fixes
Install custom firmware on my Android phone
Encourage the development of alternative free and open source WiFi firmware, like OpenWrt

Thank you for your time,
Alex Haesche

Please FCC, do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Here are a few reasons:

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

On top of that, I want to continue the following:

Install alternative operating systems on my PC, like GNU/Linux, OpenBSD, FreeBSD, etc.
Research into advanced wireless technologies, like mesh networking and bufferbloat fixes
Install custom firmware on my Android phone

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

Thank you for your time,
Alex Haesche

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Michael
Last Name: Lukowski
Mailing Address: 711 W. Grand River
City: East Lansing
Country: United States
State or Province: MI
ZIP/Postal Code: 48823
Email Address:
Organization Name:
Comment: The modifying of hardware is something that is helpful to the consumer, and , I would argue that it is also helpful for the company who produces the hardware. With routers for instance,the firmware that is pre-installed on them can be incredibly slow and buggy. Custom firmware on those exact same routers make for a better utilization of the hardware that is being used. As for PC's and not being able to install custom Operating systems that is even more crucial to today's technology. The alternative operating systems like linux are important for programming and scientific research. They allow us to use them in a more efficient, and more productive manner. These are important things that need to be kept in place. If there are restrictions on this, people will find a workaround with ease.

The modifying of hardware is something that is helpful to the consumer, and , I would argue that it is also helpful for the company who produces the hardware. With routers for instance,the firmware that is pre-installed on them can be incredibly slow and buggy. Custom firmware on those exact same routers make for a better utilization of the hardware that is being used. As for PC's and not being able to install custom Operating systems that is even more crucial to today's technology. The alternative operating systems like linux are important for programming and scientific research. They allow us to use them in a more efficient, and more productive manner. These are important things that need to be kept in place. If there are restrictions on this, people will find a workaround with ease.

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: Andrea
Last Name: Bontempi
Mailing Address: andreabont@yahoo.it
City: Milan
Country: Italy
State or Province: Milan
ZIP/Postal Code: 20060
Email Address: andreabont@yahoo.it
Organization Name:
Comment: I am a free software user, and i install this software on my devices. I do it because i like it and because i can incerase the security of my devices.

So, i ask you to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Thank you

I am a free software user, and i install this software on my devices. I do it because i like it and because i can incerase the security of my devices.

So, i ask you to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Thank you

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Max
Last Name: Niebergall
Mailing Address: 296 Indian Rd
City: Toronto
Country: Canada
State or Province: Ontario
ZIP/Postal Code: M6R 2X6
Email Address: Maxandsam55@gmail.com
Organization Name:
Comment: This potential regulation is harmful to the American people as well as the people of other countries who may enact similar regulations. This regulation is dangerous because it limits the end users ability to change and create, which will hamper innovation. Furthermore, the potential for abuse is low. Current regulations limit transmitting devices to safe levels of power. Exceeding these limits is already illegal, and more laws are not required to enforce safe use of personal transmitting devices.

This potential regulation is harmful to the American people as well as the people of other countries who may enact similar regulations. This regulation is dangerous because it limits the end users ability to change and create, which will hamper innovation. Furthermore, the potential for abuse is low. Current regulations limit transmitting devices to safe levels of power. Exceeding these limits is already illegal, and more laws are not required to enforce safe use of personal transmitting devices.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Bob
Last Name: Bob
Mailing Address: 12345 Street St.
City: San Diego
Country: United States
State or Province: CA
ZIP/Postal Code: 92129
Email Address:
Organization Name:
Comment: You can't do this. This is an insult to our rights, and an insult to America.

You can't do this. This is an insult to our rights, and an insult to America.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Stuart
Last Name: Westerman
Mailing Address: 1809 Overland Ave #1
City: Los Angeles
Country: United States
State or Province: CA
ZIP/Postal Code: 90025
Email Address:
Organization Name:
Comment: I respectfully request that the FCC not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

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

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

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

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

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.

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

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

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

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

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

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: Alfonso
Last Name: Sandoval
Mailing Address: 18a camino amansador
City: santa fe
Country: United States
State or Province: NM
ZIP/Postal Code: 87508
Email Address: alfanziox@yahoo.com
Organization Name:
Comment: Greetings Federal Communications Commission Representatives,

First off I wanted to thank you for helping with the fight for net neutrality. However that fight would be for nothing if rules for Wi-Fi Devices comes to being law.

It's too broad for one. Not only will it effect devices like Wi-Fi routers, extenders or other devices. It has the potential to effect any computer, phone, tablet that has Wi-Fi built in. When you buy a device It belongs to you and you should be able to modify it in anyway you choose that isn't malicious or designed to cause damage/signal jam to other devices, otherwise not owned by the person.

We live in an age where a lot of electronics manufacturers either build in weak security or don't perform updates or fixes to their own products for improvements. These rules will make it so that anyone who cares enough about their privacy or want to have better functionality, could face legal action for doing something that really wouldn't be harming others.

Another aspect is research. By locking down these devices you could probably kill a lot of open source projects that actually make the world a lot safer. A lot of companies have moved to using Linux for their webservers due to better security and functionality. This could drive these software's to stop growing and continue to be a major part in the marketplace.

Mesh networking will also be harmed by these rules. As you're probably aware. These types of networks can be used in many different beneficial ways. In disaster areas they can be used for better communication when things like cell towers, power grids are down.

I'm sure you're getting a lot of great comments and probably a lot of negative bashing ones too. Please don't allow the jerks of the internet control the conversation when there are plenty of us who will voice our opinions and desires in a respectful manner.

If any rules should be made it should be more to enhance the ability for consumers and researchers to install open source software, allowing for the ability to make these devices more their own. The ability to modify and install custom software/firmware is extremely important as a lot of these types of software are developed by people and help keep costs of other softwares low.

Greetings Federal Communications Commission Representatives,

First off I wanted to thank you for helping with the fight for net neutrality. However that fight would be for nothing if rules for Wi-Fi Devices comes to being law.

It's too broad for one. Not only will it effect devices like Wi-Fi routers, extenders or other devices. It has the potential to effect any computer, phone, tablet that has Wi-Fi built in. When you buy a device It belongs to you and you should be able to modify it in anyway you choose that isn't malicious or designed to cause damage/signal jam to other devices, otherwise not owned by the person.

We live in an age where a lot of electronics manufacturers either build in weak security or don't perform updates or fixes to their own products for improvements. These rules will make it so that anyone who cares enough about their privacy or want to have better functionality, could face legal action for doing something that really wouldn't be harming others.

Another aspect is research. By locking down these devices you could probably kill a lot of open source projects that actually make the world a lot safer. A lot of companies have moved to using Linux for their webservers due to better security and functionality. This could drive these software's to stop growing and continue to be a major part in the marketplace.

Mesh networking will also be harmed by these rules. As you're probably aware. These types of networks can be used in many different beneficial ways. In disaster areas they can be used for better communication when things like cell towers, power grids are down.

I'm sure you're getting a lot of great comments and probably a lot of negative bashing ones too. Please don't allow the jerks of the internet control the conversation when there are plenty of us who will voice our opinions and desires in a respectful manner.

If any rules should be made it should be more to enhance the ability for consumers and researchers to install open source software, allowing for the ability to make these devices more their own. The ability to modify and install custom software/firmware is extremely important as a lot of these types of software are developed by people and help keep costs of other softwares low.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Anthony
Last Name: Scheidel
Mailing Address: 14316 126th ave NE D304
City: Kirkland
Country: United States
State or Province: WA
ZIP/Postal Code: 98034
Email Address: ascheidel83@gmail.com
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Laine
Last Name: Wilde
Mailing Address: 3207 Jackson Farm Road
City: Hopewell
Country: United States
State or Province: VA
ZIP/Postal Code: 23860
Email Address: krylife@gmail.com
Organization Name:
Comment: I'm concerned about the rule "Equipment Authorization and Electronic Labeling for Wireless Devices". This rule unnecessarily damages the future of open source software. The rule gives manufacturers all the power to control wireless devices, including PCs and routers. Locking down these devices discourages innovation and security benefits that can result from consumers open-use. I strongly recommend re-working this rule to allow for open use distributions by consumers.

I'm concerned about the rule "Equipment Authorization and Electronic Labeling for Wireless Devices". This rule unnecessarily damages the future of open source software. The rule gives manufacturers all the power to control wireless devices, including PCs and routers. Locking down these devices discourages innovation and security benefits that can result from consumers open-use. I strongly recommend re-working this rule to allow for open use distributions by consumers.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Parker
Last Name: Mathews
Mailing Address: 5236 Nielsen Ave
City: Ferndale
Country: United States
State or Province: WA
ZIP/Postal Code: 98248
Email Address: dakine7t9@gmail.com
Organization Name:
Comment: Public servants of the Federal Communications Commission,

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

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

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

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

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

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

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

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

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

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

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

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

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

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Matt
Last Name: G
Mailing Address: 257 Mill Road
City: Toronto
Country: Canada
State or Province: Ontario
ZIP/Postal Code: M9C 1Y3
Email Address:
Organization Name:
Comment: I would to express my dislike of this Proposed Rule. This rule will have major negative effects on technology:
-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.
-Owners of PC have the right to use a different operating system.

I would to express my dislike of this Proposed Rule. This rule will have major negative effects on technology:
-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.
-Owners of PC have the right to use a different operating system.

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: Shatayu
Last Name: Kulkarni
Mailing Address: 7414 Stoneleaf Rd
City: San Ramon
Country: United States
State or Province: CA
ZIP/Postal Code: 94582
Email Address:
Organization Name:
Comment: Please do not proceed with this law. It hampers security research, innovation, and the ability of the consumer to do what they want with hardware they bought. This law would disallow Linux, which is used globally in the tech industry. It would greatly hamper the ability of America to compete with the rest of the world and stifle development of the world's most advanced technology.

Please do not proceed with this law. It hampers security research, innovation, and the ability of the consumer to do what they want with hardware they bought. This law would disallow Linux, which is used globally in the tech industry. It would greatly hamper the ability of America to compete with the rest of the world and stifle development of the world's most advanced technology.

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: Emil
Last Name: alicic
Mailing Address: 5879 west grove dr se
City: kentwood
Country: United States
State or Province: MI
ZIP/Postal Code: 49512
Email Address:
Organization Name:
Comment: Please, listen thoroughly,

The definition of the future is innovation,
Innovation can not happen without freedom,
Freedom, can not happen without innovation.

By entitling this act, you not only halt the innovation of new, alternate systems,
But you also block freedom, and therefore, slow down the future of technological advancement.

There were no issues prior to this act, and there are non now,
But you do cause an issue.

Personal Computers primarily run on the Operating System family of windows,
But windows has many limitations that some users felt gel back on, then came Linux and similar systems,
They unlocked much potential for these users, and allot of machinery these days run on Linux based systems, and from Linux, Chromebooks were born, an education tool for students everywhere, cheap an effective.

By placing this, you prevent companies and users from advancing technology in new and innovative ways, and also prevent students from learning.

Please, listen thoroughly,

The definition of the future is innovation,
Innovation can not happen without freedom,
Freedom, can not happen without innovation.

By entitling this act, you not only halt the innovation of new, alternate systems,
But you also block freedom, and therefore, slow down the future of technological advancement.

There were no issues prior to this act, and there are non now,
But you do cause an issue.

Personal Computers primarily run on the Operating System family of windows,
But windows has many limitations that some users felt gel back on, then came Linux and similar systems,

They unlocked much potential for these users, and allot of machinery these days run on Linux based systems, and from Linux, Chromebooks were born, an education tool for students everywhere, cheap an effective.

By placing this, you prevent companies and users from advancing technology in new and innovative ways, and also prevent students from learning.

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: Angela
Last Name: Steele
Mailing Address: 4829 S Mill Ave
City: Tempe
Country: United States
State or Province: AZ
ZIP/Postal Code: 85282
Email Address:
Organization Name:
Comment: I know copy/paste comments are often ignored, but I cannot put my thoughts together better than what has already been said. Please, if you haven't already, read this. I stand with it.

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.

I know copy/paste comments are often ignored, but I cannot put my thoughts together better than what has already been said. Please, if you haven't already, read this. I stand with it.

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: Ben
Last Name: Shepard
Mailing Address: 531 E Ramona Ave
City: Salt Lake City
Country: United States
State or Province: UT
ZIP/Postal Code: 84105
Email Address:
Organization Name:
Comment: A consumer should be allowed to modify a product they rightfully own, in any way they wish. This should include modifying or replacing software on hardware.

A consumer should be allowed to modify a product they rightfully own, in any way they wish. This should include modifying or replacing software on hardware.

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: Caleb
Last Name: Dasher
Mailing Address: 122 Old Edwards Rd.
City: Arnoldsville
Country: United States
State or Province: GA
ZIP/Postal Code: 30619
Email Address: calebdasher@outlook.com
Organization Name:
Comment: I would wish you to reconsider passing a law that would restrict what software I can install on my legally purchased hardware.

I would wish you to reconsider passing a law that would restrict what software I can install on my legally purchased hardware.

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: Williams
Mailing Address: 1615 Laurel Avenue, Apt 1017
City: Knoxville
Country: United States
State or Province: TN
ZIP/Postal Code: 37916
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.

Please do not pass this Proposed Rule. This is why:

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 don't pass this rule please. Thank you.

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.

Please do not pass this Proposed Rule. This is why:

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 don't pass this rule please. Thank you.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Michael
Last Name: Lee
Mailing Address: 620 Mariposa Ave #4
City: Mountain View
Country: United States
State or Province: CA
ZIP/Postal Code: 94041
Email Address: michael.hl.lee@gmail.com
Organization Name:
Comment: Altering the OS on mobile devices and computers has been essential to innovation in the past two decades. Please do not curtail this important practice.

Altering the OS on mobile devices and computers has been essential to innovation in the past two decades. Please do not curtail this important practice.

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: Collin
Last Name: Booth
Mailing Address: 9515 Upton Ave N
City: Brooklyn Park
Country: United States
State or Province: MN
ZIP/Postal Code: 55444
Email Address:
Organization Name:
Comment: While I can see that this regulation may have started with the intent to help protect some people from illegitimate/harmful alterations that could be made to radio/communication devices the proposed changes are too broad and potentially harmful to the computing world.

The potential to cut out community developed operating systems (unix systems, and things like hackintosh) can not be allowed to happen. These operating systems are basically the only thing preventing Microsoft and Apple from claiming 100% of the market on operating systems. If you know anything about how the two function as a whole, you will know that depending on your mindset for how your OS should function you won't have ANY other options. You will pay microsoft whatever they ask or you'll pay apple whatever they ask.

The internet and computers have been able to develop so quickly and so effectively because of our ability to manipulate it. For every concern the FCC may have regarding manipulated tech there are thousands of brilliant individuals who rely on this flexibility to push out new innovations that could change the world for the better. Please do not limit this, every step towards cutting out the ability of the public is a devastating blow.. Once that precedent is set we will never gain it back.

On a business side of things: It feels criminal to prevent a small business owner (such as myself) from being able to patch known security flaws in my hardware when the manufacturer delays or decides to ignore the issue. Do not take aware the American publics ability to take control of the hardware they rightfully own.

While I can see that this regulation may have started with the intent to help protect some people from illegitimate/harmful alterations that could be made to radio/communication devices the proposed changes are too broad and potentially harmful to the computing world.

The potential to cut out community developed operating systems (unix systems, and things like hackintosh) can not be allowed to happen. These operating systems are basically the only thing preventing Microsoft and Apple from claiming 100% of the market on operating systems. If you know anything about how the two function as a whole, you will know that depending on your mindset for how your OS should function you won't have ANY other options. You will pay microsoft whatever they ask or you'll pay apple whatever they ask.

The internet and computers have been able to develop so quickly and so effectively because of our ability to manipulate it. For every concern the FCC may have regarding manipulated tech there are thousands of brilliant individuals who rely on this flexibility to push out new innovations that could change the world for the better. Please do not limit this, every step towards cutting out the ability of the public is a devastating blow.. Once that precedent is set we will never gain it

back.

On a business side of things: It feels criminal to prevent a small business owner (such as myself) from being able to patch known security flaws in my hardware when the manufacturer delays or decides to ignore the issue. Do not take aware the American publics ability to take control of the hardware they rightfully 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: Jared
Last Name: Hohmeier
Mailing Address: 343 Angel St
City: Oceanside
Country: United States
State or Province: CA
ZIP/Postal Code: 92058
Email Address: null
Organization Name: null
Comment: The software used on devices with modular wireless radio should remain unrestricted. Open source and alternative firmware on routers give people more freedom, customization and security on their network. There is no current significant issue with people using alternative firmware to circumvent power restrictions on these wireless devices and if a problem arose it could be policed in other ways that do not restrict the freedoms of people who are not doing this.

The software used on devices with modular wireless radio should remain unrestricted. Open source and alternative firmware on routers give people more freedom, customization and security on their network. There is no current significant issue with people using alternative firmware to circumvent power restrictions on these wireless devices and if a problem arose it could be policed in other ways that do not restrict the freedoms of people who are not doing 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: Virat
Last Name: Gohil
Mailing Address: 1024 Valencia Ave
City: sunnyvale
Country: United States
State or Province: CA
ZIP/Postal Code: 94086
Email Address:
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: Nathaniel
Last Name: Pickett
Mailing Address: 1809 1/2 Massacusetts St
City: Lawrence
Country: United States
State or Province: KS
ZIP/Postal Code: 66046
Email Address:
Organization Name:
Comment: Dear FCC,

I am writing to urge you to not implement rules that take away the ability of users to install the software of their choosing on their computing device. Taking the ability away from users to make their own decisions about their own property and their online security is not only potentially dangerous, but it also circumscribes consumer rights. In this case, the NRPM rules would disproportionately affect one type of user/consumer more than others--the computer-literate, including IT professionals, hobbyist programmers, software developers, security engineers, technicians, researchers, and so on.

As our society continues to increasibly rely on technology, we have realized that many organizations and corporations do not have the best interests of their customers at heart--just their bottom line. ISPs and router manufacturers have consistently proven that they don't mind charging high rates for subpar services and technology in relation to their competitors in other countries. This leaves many unsuspecting and less-informed consumers vulnerable to security threats that are continuing to evolve at a rate that far outpaces any efforts from ISPs and router manufacturers.

Writing policy that specifically limits the ability of consumers/users/people to exercise their right to do what they want with their own property, especially when it concerns their own safety and security, is a special kind of irresponsible that reveals the policymakers' own disdain for those very consumers/users/people whom they purport to serve as functionaries in a government institution. Please scrap these new rules.

Dear FCC,

I am writing to urge you to not implement rules that take away the ability of users to install the software of their choosing on their computing device. Taking the ability away from users to make their own decisions about their own property and their online security is not only potentially dangerous, but it also circumscribes consumer rights. In this case, the NRPM rules would disproportionately affect one type of user/consumer more than others--the computer-literate, including IT professionals, hobbyist programmers, software developers, security engineers, technicians, researchers, and so on.

As our society continues to increasibly rely on technology, we have realized that many organizations and corporations do not have the best interests of their customers at heart--just their bottom line. ISPs and router manufacturers have consistently proven that they don't mind charging high rates for subpar services and technology in relation to their competitors in other countries. This leaves many unsuspecting and less-informed consumers vulnerable to security threats that are continuing to evolve at a rate that far outpaces any efforts from ISPs and router manufacturers.

Writing policy that specifically limits the ability of consumers/users/people to exercise their right to do what they want with their own property, especially when it concerns their own safety and security, is a special kind of irresponsible that reveals the policymakers' own disdain for those very consumers/users/people whom they purport to serve as functionaries in a government institution. Please scrap these new rules.

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: Mathew
Last Name: Foran
Mailing Address: 160 cooper road
City: Hummelstown
Country: United States
State or Province: PA
ZIP/Postal Code: 17036
Email Address: hex4d617474@gmail.com
Organization Name:
Comment: I'm not an expert by any means on this subject, and I won't pretend to have read the whole act. I have, however, heard a lot of people talking about what this act will do, and it sounds oppressive. There're a lot of good people who use these technologies every day, and limiting their use doesn't seem to be in the best interests of anybody. The way I see it, most people will continue to modify their wireless devices, and making this illegal will just cause undue conflict. Please think about the millions this act could affect negatively before making any decisions. Thank you.

I'm not an expert by any means on this subject, and I won't pretend to have read the whole act. I have, however, heard a lot of people talking about what this act will do, and it sounds oppressive. There're a lot of good people who use these technologies every day, and limiting their use doesn't seem to be in the best interests of anybody. The way I see it, most people will continue to modify their wireless devices, and making this illegal will just cause undue conflict. Please think about the millions this act could affect negatively before making any decisions. Thank you.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Matt
Last Name: Slunecka
Mailing Address: 19702 Woolworth Ave
City: Omaha
Country: United States
State or Province: NE
ZIP/Postal Code: 68130
Email Address: slunecka@gmail.com
Organization Name:
Comment: I am opposed to this proposal. Custom firmware for wireless routers is a security essential in 2015. There are hundreds of consumer wireless routers which no longer receive any manufacturer support. Without custom firmware there is no way to close security holes on these devices.

Furthermore, the wording on this proposal is overbroad and implies that even changing the OS on your laptop or PC would be illegal. Heard of linux? People use it.

I am opposed to this proposal. Custom firmware for wireless routers is a security essential in 2015. There are hundreds of consumer wireless routers which no longer receive any manufacturer support. Without custom firmware there is no way to close security holes on these devices.

Furthermore, the wording on this proposal is overbroad and implies that even changing the OS on your laptop or PC would be illegal. Heard of linux? People use 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: Matthew
Last Name: Reynolds
Mailing Address: 3115 SE 55th Ave
City: Portland
Country: United States
State or Province: OR
ZIP/Postal Code: 97206
Email Address: matt@hom3.us
Organization Name:
Comment: I appreciate the hard work that went into this proposal, but I would ask that I be able to install new/alternative firmware on networking devices. The general quality of the software on these devices is notoriously poor and often contains serious security flaws that would be unfixable without the ability to replace the firmware with 3rd party firmware.

The only way this would be acceptable is if there we some alternative proposal requiring manufacturers to test their software and patch security holes within a short period of time (30 days or less), since I would be unwilling to continue using the device (and thus the Internet) while the device was vulnerable to a security breach.

Please don't limit this ability without having alternative measures in place. Better, don't limit this ability in the first place. Thanks.

I appreciate the hard work that went into this proposal, but I would ask that I be able to install new/alternative firmware on networking devices. The general quality of the software on these devices is notoriously poor and often contains serious security flaws that would be unfixable without the ability to replace the firmware with 3rd party firmware.

The only way this would be acceptable is if there we some alternative proposal requiring manufacturers to test their software and patch security holes within a short period of time (30 days or less), since I would be unwilling to continue using the device (and thus the Internet) while the device was vulnerable to a security breach.

Please don't limit this ability without having alternative measures in place. Better, don't limit this ability in the first place. Thanks.

Please Do Not Reply To This Email.

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

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

Submitter Info:
First Name: Daniel
Last Name: Ribakoff
Mailing Address: 6524 Genstar Ln.
City: Dallas
Country: United States
State or Province: TX
ZIP/Postal Code: 75252-5406
Email Address:
Organization Name:
Comment: It is wrong to try to control devices people own if they are not using them for illegal activities. People have the right to modify their possessions, and this cannot be taken away from us.

We rely on security researchers who investigate devices to further secure our electronics.

If the manufacturer stops supporting their product, people should be able to modify the software themselves to maintain it, otherwise, security holes will never be patched.

In the past, users have fixed serious bugs on hardware that the manufacturer has deemed "outdated." An example of this is the Linksys WRT54G, which continues to recieve comminuty support through projects such as OpenWRT and Tomato. Linksys have since commended the efforts of the community and have released another "WRT" router specifically to be modified by the community.

If the government chooses to limit what the consumers of a product can do with what they have purchased, the people of that government will live in tyranny, and for a country that proclaims itself as "free," that is unacceptable.

Do not let this pass.

It is wrong to try to control devices people own if they are not using them for illegal activities. People have the right to modify their possessions, and this cannot be taken away from us.

We rely on security researchers who investigate devices to further secure our electronics.

If the manufacturer stops supporting their product, people should be able to modify the software themselves to maintain it, otherwise, security holes will never be patched.

In the past, users have fixed serious bugs on hardware that the manufacturer has deemed "outdated." An example of this is the Linksys WRT54G, which continues to recieve comminuty support through projects such as OpenWRT and Tomato. Linksys have since commended the efforts of the community and have released another "WRT" router specifically to be modified by the community.

If the government chooses to limit what the consumers of a product can do with what they have purchased, the people of that government will live in tyranny, and for a country that proclaims itself as "free," that is unacceptable.