

features designed to be as easily accessible as possible, is not appropriate for any environment in which security is a concern. A central tenet of information security, and security in general, is that the attack surface should be as small as possible - services not needed for a particular installation should not be installed and enabled. The only software which definitely cannot be exploited is software which is not installed or not enabled. Therefore, the most secure firmware tends to be that with as many features _removed_ as possible, with only those items required for the current role installed.

Manufacturer firmware does the exact opposite, for ease-of-use by ordinary consumers. All services which might be of use to any customer are installed, enabled, and wide open for use (and abuse). Firmware which can be customized, trimmed down to provide only the required functionality (and therefore the smallest attack surface), such as OpenWRT, is a far in terms of security.

Lastly, these devices are frequently used as active security devices, such as firewalls and VPN endpoints. To require that these ubiquitous and therefore inexpensive devices be replaced with far more expensive niche versions branded as security devices necessarily reduces the number of security checkpoints which will be installed in networks. As an example, consider the twentyfold cost difference between a SOHO Cisco router and a Cisco firewall appliance which internally contains similar hardware. The small office can easily afford a firewall based on a third-party firmware for the ubiquitous router, and such a firewall can well meet the needs of a small office. They are unlikely to purchase a dedicated firewall from the same company costing several thousand dollars. Therefore, disallowing the third-party firewall firmware results in no firewall being used at all.

Based on 18 years of professional experience in network security, in both the private sector and government, the proposed rule causes significant concern for information security posture. There are three primary reasons. The legitimate goals of the FCC could be achieved in an alternate manner which does not cause the same widespread security vulnerabilities, by instead requiring that output power levels and any other critical parameters be limited to legal levels by a separate chip. This approach would be far superior to effectively banning proper security practice for the ENTIRE operating system and all utilities on the device, as the current proposal does.

The proposed rule which requires that manufacturers disallow firmware updates (other than signed manufacturer updates, typically provided for only a very short time), makes it much more difficult to prevent incidents such as the \$45 million loss at TJX and the Target breach. In both cases, the victim companies were initially targeted because insecure wifi devices were in use. To reduce future occurrences of such breaches, it is imperative to be able to update devices which use wireless networking. Especially when a vulnerability such as Shellshock is discovered, it is imperative that risks be mitigated immediately.

Updates provided by the manufacturer may at first seem to be a possible solution, but are not actually a viable solution for two reasons. Manufacturers generally do not provide long-term updates, updates for devices more than about one-two years old. In many cases, no updates are offered at all to handle issues after the date of sale. It is not reasonable to anticipate that organizations and families will replace their network gear every year or two - firmware updates are needed, including for devices which are a few years old. Perhaps ESPECIALLY for devices which are a few years old.

Secondly, updates from the manufacturer are not a viable solution for more sensitive government and private organizations due to the response time required. In the first 24 hours after the release of Shellshock, thousands of systems were compromised. For many networks, it is critically important to mitigate the threat during this initial time frame. Manufacturer full updates were not available for several days to several months, as we first discussed the best long term solution and that solution propagated downstream from the authors, to the subsystem maintainers, distribution maintainers, OEM repackagers, and finally out to customers after testing at each level. In the meantime, temporary MITIGATIONS were performed on-site by network engineers and security contractors. These vital mitigations which protected sensitive networks in the interim would be illegal and prevented by manufacturer locks under the proposed rule. In simple terms, the proposal makes it illegal to manufacturer equipment which can be _quickly_ protected against new threats to our cyber security.

Another reason that the proposed rule is problematic is that the manufacturer default firmware, with all available features designed to be as easily accessible as possible, is not appropriate for any environment in which security is a concern. A central tenet of information security, and security in general, is that the attack surface should be as small as possible - services not needed for a particular installation should not be installed and enabled. The only software which definitely cannot be exploited is software which is not installed or not enabled. Therefore, the most secure firmware tends to be that with as many features _removed_ as possible, with only those items required for the current role installed.

Manufacturer firmware does the exact opposite, for ease-of-use by ordinary consumers. All services which might be of use to any customer are installed, enabled, and wide open for use (and abuse). Firmware which can be customized, trimmed down to provide only the required functionality (and therefore the smallest attack surface), such as OpenWRT, is a far in terms of security.

Lastly, these devices are frequently used as active security devices, such as firewalls and VPN endpoints. To require that these ubiquitous and therefore inexpensive devices be replaced with far more expensive niche versions branded as security devices necessarily reduces the number of security checkpoints which will be installed in networks. As an example, consider the twentyfold cost difference between a SOHO Cisco router and a Cisco firewall appliance which internally contains similar hardware. The small office can easily afford a firewall based on a third-party firmware for the ubiquitous router, and such a firewall can well meet the needs of a small office. They are unlikely to purchase a dedicated firewall from the same company costing several thousand dollars. Therefore, disallowing the third-party firewall firmware results in no firewall being used at all.

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: Erik

Last Name: Ordway

Mailing Address: 1103 Brawne ave nw

City: Olympia

Country: United States

State or Province: WA

ZIP/Postal Code: 98502

Email Address: eriko@jumpsuit.org

Organization Name:

Comment: I have more of a question. Have this devices been abused to interfere with other regulated devices? If they have not then there might not be a need for this regulation. If they have been abused then the question is are there other easily accessible devices that are abused in the same manner. Give that we have easy access to China's markets where these other devices exist then this regulation will probably pointless.

I have more of a question. Have this devices been abused to interfere with other regulated devices? If they have not then there might not be a need for this regulation. If they have been abused then the question is are there other easily accessible devices that are abused in the same manner. Give that we have easy access to China's markets where these other devices exist then this regulation will probably pointless.

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: Leif

Last Name: Burrow

Mailing Address: 2139 Audubon Pl

City: Toledo

Country: United States

State or Province: OH

ZIP/Postal Code: 43606

Email Address: kc8rwr@unforgettability.net

Organization Name: unforgettability.net

Comment: Please do not take away the right for people to choose their own software to run on their WiFi enabled hardware, 5Ghz or otherwise.

These proposed rules could potentially make router hardware capable of running replacement firmware such as ddwrt, openwrt and others unavailable to consumers. These software options are often more secure, more stable and offer better, more inovative features than stock firmware. Similar projects exist for mobile phones for example Cyanogenmod for Android and could be affected due to most smartphones including WiFi support..

While arguably only a small part of the population tends to use custom software on their devices this loss would in the end affect everyone. Features that are developed by such users are often adopted by the industry. Preventing consumers from modifying their own software will eliminate a prime source of innovation that would otherwise result in better products that we all may enjoy.

Please do not take away the right for people to choose their own software to run on their WiFi enabled hardware, 5Ghz or otherwise.

These proposed rules could potentially make router hardware capable of running replacement firmware such as ddwrt, openwrt and others unavailable to consumers. These software options are often more secure, more stable and offer better, more inovative features than stock firmware. Similar projects exist for mobile phones for example Cyanogenmod for Android and could be affected due to most smartphones including WiFi support..

While arguably only a small part of the population tends to use custom software on their devices this loss would in the end affect everyone. Features that are developed by such users are often adopted by the industry. Preventing consumers from modifying their own software will eliminate a prime source of innovation that would otherwise result in better products that we all may enjoy.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Justin

Last Name: LaPre

Mailing Address: 415 Brunswick Drive Apt 3

City: Troy

Country: United States

State or Province: NY

ZIP/Postal Code: 12180

Email Address: justin@lapre.com

Organization Name:

Comment: Leaving the ability to alter the devices solely in the hands of the manufacturers does not sound particularly beneficial to the consumer in any measurable way. In fact the only alternative to waiting for a slow-to-patch vendor would be to purchase a new wireless transmitter. This is unfortunate as presumably the consumer's wireless device was previously adequate (outside of the newly found security issue).

Leaving the ability to alter the devices solely in the hands of the manufacturers does not sound particularly beneficial to the consumer in any measurable way. In fact the only alternative to waiting for a slow-to-patch vendor would be to purchase a new wireless transmitter. This is unfortunate as presumably the consumer's wireless device was previously adequate (outside of the newly found security issue).

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: Kirtan

Last Name: Shah

Mailing Address: 51 Clifton Ave

City: Newark

Country: United States

State or Province: NJ

ZIP/Postal Code: 07104

Email Address: kirtan.a.shah@gmail.com

Organization Name:

Comment: Dear FCC,

I request you 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.

Dear FCC,

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

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

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

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

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Don

Last Name: Hess

Mailing Address: 704 Rushmore Drive

City: Burnsville

Country: United States

State or Province: MN

ZIP/Postal Code: 55306

Email Address: null

Organization Name: null

Comment: To provide security for home users, they **MUST** be allowed to install open source firmware like OpenWRT on their home routers. As can be seen from the rash of exploits in home router firmware shipped from device makers, closed source routers cannot be trusted to prevent botnets from spreading. Any attempt to restrict radio firmware because of possible local RF misuse will produce the side effect of crushing user's ability to protect themselves as well as security researchers ability to find flaws before malicious attackers do. Thank you.

To provide security for home users, they **MUST** be allowed to install open source firmware like OpenWRT on their home routers. As can be seen from the rash of exploits in home router firmware shipped from device makers, closed source routers cannot be trusted to prevent botnets from spreading. Any attempt to restrict radio firmware because of possible local RF misuse will produce the side effect of crushing user's ability to protect themselves as well as security researchers ability to find flaws before malicious attackers do. 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: mitchell

Last Name: deoudes

Mailing Address: 60 Berry St.

City: brooklyn

Country: United States

State or Province: NY

ZIP/Postal Code: 11211

Email Address: mitch@houseofpain.org

Organization Name: mitch@houseofpain.org

Comment: I respectfully oppose the proposed rules that would prevent citizens from installing software (firmware) of their choosing on devices that they own. The rules would prevent far more legitimate uses than illegal ones, and would have far-ranging effects on innovation & the economy.

The fact is, third-party software is often better & more secure than that of the manufacturer - particularly in the case of devices such as cell phones and routers. Effectively crippling an entire class of tools on the off chance that someone might use them to break rules (specially when there is little indication that such rule-breaking is prevalent, and ample evidence that legitimate uses are widespread) not only makes no sense, but is contrary to the spirit of this country's Constitution.

I respectfully oppose the proposed rules that would prevent citizens from installing software (firmware) of their choosing on devices that they own. The rules would prevent far more legitimate uses than illegal ones, and would have far-ranging effects on innovation & the economy.

The fact is, third-party software is often better & more secure than that of the manufacturer - particularly in the case of devices such as cell phones and routers. Effectively crippling an entire class of tools on the off chance that someone might use them to break rules (specially when there is little indication that such rule-breaking is prevalent, and ample evidence that legitimate uses are widespread) not only makes no sense, but is contrary to the spirit of this country's Constitution.

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: Jon

Last Name: Larson

Mailing Address: 5801 Lombard Ave

City: Everett

Country: United States

State or Province: WA

ZIP/Postal Code: 98203

Email Address: jtlarson07@gmail.com

Organization Name:

Comment: As a long time user of routers with modified firmware (Tomato, OpenWRT, DDWRT, etc...) I am opposed to the broad nature of this proposal. It appears to enact restrictions that have no connection to the problem at hand--restrictions that rob millions of users of the opportunity to fix critical security issues and other valuable (and non-disruptive) functional improvements for their personal equipment.

I sincerely hope that the FCC will reconsider the tremendous negative impact of this rule and revise this proposal to address the necessary issues without infringing on the rights we have as users and hobbyists to secure and improve commercial devices.

As a long time user of routers with modified firmware (Tomato, OpenWRT, DDWRT, etc...) I am opposed to the broad nature of this proposal. It appears to enact restrictions that have no connection to the problem at hand--restrictions that rob millions of users of the opportunity to fix critical security issues and other valuable (and non-disruptive) functional improvements for their personal equipment.

I sincerely hope that the FCC will reconsider the tremendous negative impact of this rule and revise this proposal to address the necessary issues without infringing on the rights we have as users and hobbyists to secure and improve commercial 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: zachary

Last Name: mcurdy

Mailing Address: 226 college dr. NW #20

City: Salem

Country: United States

State or Province: OR

ZIP/Postal Code: 97304

Email Address:

Organization Name: modthethings

Comment: There exists NO good reason to prevent someone from installing software on a device they OWN. Not only will will this stop researchers from being able to find security holes, but it will prevent the average user from fixing them. Making it illegal to modify the software on a device you own doesn't solve the problem anyway.

There exists NO good reason to prevent someone from installing software on a device they OWN. Not only will will this stop researchers from being able to find security holes, but it will prevent the average user from fixing them. Making it illegal to modify the software on a device you own doesn't solve the problem anyway.

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: Jon

Last Name: Roberts

Mailing Address: 4412 Dove Dr

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78744

Email Address: jon@sxsw.com

Organization Name: SXSW

Comment: Please do not pass any regulation that prohibits open-source firmware usage or development.

There are other, better ways of ensuring that users do not exceed radio power or use non-permitted frequencies. Educating the users so that they know the limitations, or perhaps requiring a sane default configuration is much preferred to outlawing alternative firmware.

DD-WRT and related projects are enormously beneficial to businesses and individuals, and have many uses outside of controlling RF settings, such as routing, firewalls, VOIP, web servers, and VPNs.

Please do not pass any regulation that prohibits open-source firmware usage or development.

There are other, better ways of ensuring that users do not exceed radio power or use non-permitted frequencies. Educating the users so that they know the limitations, or perhaps requiring a sane default configuration is much preferred to outlawing alternative firmware.

DD-WRT and related projects are enormously beneficial to businesses and individuals, and have many uses outside of controlling RF settings, such as routing, firewalls, VOIP, web servers, and VPNs.

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: Otto

Last Name: Monnig

Mailing Address: 783 Foxdale

City: Winnetka

Country: United States

State or Province: IL

ZIP/Postal Code: 60093

Email Address:

Organization Name:

Comment: This act is an extremely bad idea for these reasons:

It limits the freedom of individuals to experiment with router equipment using open source software like OpenWRT and dd-wrt. Using packages like these allows future engineers to develop skills that are invaluable for inventing new technologies.

It forces router designers to disclose their intellectual property to the government, who will then be required to disclose it under FOIA. Not a prospect that I relish for my IP.

It forces citizens to rely on often buggy and insecure commercial equipment (several have been breached recently) provided from 'official' manufacturers.

I'm pretty sure that most of the routers that have been breached and are contributing to botnets are using the stock firmware, not the open source versions that you want to outlaw. Those who upgrade their firmware are more security conscious than normal folks. Leave them be.

The FCC would be better to spend their time encouraging internet providers to improve their shoddy customer service. Domestic US internet speeds are slow when compared with other developed nations. Why not pressure providers about that?

This act is an extremely bad idea for these reasons:

It limits the freedom of individuals to experiment with router equipment using open source software like OpenWRT and dd-wrt. Using packages like these allows future engineers to develop skills that are invaluable for inventing new technologies.

It forces router designers to disclose their intellectual property to the government, who will then be required to disclose it under FOIA. Not a prospect that I relish for my IP.

It forces citizens to rely on often buggy and insecure commercial equipment (several have been breached recently) provided from 'official' manufacturers.

I'm pretty sure that most of the routers that have been breached and are contributing to botnets are using the stock firmware, not the open source versions that you want to outlaw. Those who upgrade their firmware are more security conscious than normal folks. Leave them be.

The FCC would be better to spend their time encouraging internet providers to improve their shoddy customer service. Domestic US internet speeds are slow when compared with other developed nations. Why not pressure providers about that?

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Paul

Last Name: Rau

Mailing Address: 3607 N Athenian St

City: Wichita

Country: United States

State or Province: KS

ZIP/Postal Code: 67204

Email Address:

Organization Name:

Comment: The proposed rules requiring the lockdown of wireless equipment operating in the 5GHz would be detrimental and a step backward that would impede innovation and be detrimental to otherwise authorized users of equipment.

The growing capabilities and processing power of electronic equipment has allowed for greatly expanded uses at lower prices than ever before. Third party firmwares (such as the DD-WRT example called out) have brought features to consumer level gear that previously cost thousands of dollars or required much larger, power hungry equipped.

This consumer has used Third Party firmwares in networking equipment for over a decade to correct security issues that manufacturers are slow to correct, enable privacy and security features such as virtual private networks when travelling and away from home to avoid the security risks of open Wi-Fi networks, and other useful features.

Further, the development of third-party firmwares and the innovations there-in have fed back to the manufacturers of equipment, with products leveraging the innovation that has occurred, with manufacturers such as ASUS leveraging third party software (Tomato) in their high-end gear to give a better user experience.

I myself presently run a 5GHz wireless device, originally designed by the manufacturer to leverage a third party firmware, further updated by yet another third party to quickly close security risks and provide additional privacy features. This has allowed me to keep equipment current and modern without reliance on manufacturers who may not be interested in quickly responding to the needs of older hardware.

I have a large pile of e-waste that results from the use of encrypted firmwares and manufacturer lockdown. Units that may be otherwise re-purposed to secondary uses instead get thrown out. Requiring this to be the norm is not to the benefit of consumers and end users.

The proposed rules requiring the lockdown of wireless equipment operating in the 5GHz would be detrimental and a step backward that would impede innovation and be detrimental to otherwise authorized users of equipment.

The growing capabilities and processing power of electronic equipment has allowed for greatly expanded uses at lower prices than ever before. Third party firmwares (such as the DD-WRT example called out) have brought features to consumer level gear that previously cost thousands of dollars or required much larger, power hungry equipped.

This consumer has used Third Party firmwares in networking equipment for over a decade to correct security issues that manufacturers are slow to correct, enable privacy and security features such as virtual private networks when travelling

and away from home to avoid the security risks of open Wi-Fi networks, and other useful features.

Further, the development of third-party firmwares and the innovations there-in have fed back to the manufacturers of equipment, with products leveraging the innovation that has occurred, with manufacturers such as ASUS leveraging third party software (Tomato) in their high-end gear to give a better user experience.

I myself presently run a 5GHz wireless device, originally designed by the manufacturer to leverage a third party firmware, further updated by yet another third party to quickly close security risks and provide additional privacy features. This has allowed me to keep equipment current and modern without reliance on manufacturers who may not be interested in quickly responding to the needs of older hardware.

I have a large pile of e-waste that results from the use of encrypted firmwares and manufacturer lockdown. Units that may be otherwise re-purposed to secondary uses instead get thrown out. Requiring this to be the norm is not to the benefit of consumers and end users.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Obierek

Mailing Address: 209 Williams Rd.

City: Chester

Country: United States

State or Province: VT

ZIP/Postal Code: 05143

Email Address: aobierek@gmail.com

Organization Name:

Comment: Stop talking away our freedom. If I purchase a WiFi router, I should be bale to put open source software on it if I ant. What the hell has become of the USA!

Stop talking away our freedom. If I purchase a WiFi router, I should be bale to put open source software on it if I ant.
What the hell has become of the USA!

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: mitchell

Last Name: deoudes

Mailing Address: 109 N 9th st #3R

City: brooklyn

Country: United States

State or Province: NY

ZIP/Postal Code: 11249

Email Address: mitch@houseofpain.org

Organization Name:

Comment: I respectfully object to the proposed rules that would prevent citizens from installing software (firmware) of their choosing on the devices they own. The rules would prevent far more legitimate uses than illegal ones, and would have wide-ranging consequences to innovation, the economy, and security.

The fact of the matter is, third party software is often better & more secure than that of the manufacturer - particularly in the case of devices like cell phones and routers. Effectively crippling a whole range of devices because they *might* be used to break rules, especially when such rule-breaking is not known to be widespread and is dwarfed by the amount of legitimate use, makes no sense - and is contrary to the spirit of this country's Constitution.

I respectfully object to the proposed rules that would prevent citizens from installing software (firmware) of their choosing on the devices they own. The rules would prevent far more legitimate uses than illegal ones, and would have wide-ranging consequences to innovation, the economy, and security.

The fact of the matter is, third party software is often better & more secure than that of the manufacturer - particularly in the case of devices like cell phones and routers. Effectively crippling a whole range of devices because they *might* be used to break rules, especially when such rule-breaking is not known to be widespread and is dwarfed by the amount of legitimate use, makes no sense - and is contrary to the spirit of this country's Constitution.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Jason

Last Name: Wignot

Mailing Address: 14040 Brookstone Drive

City: Carmel

Country: United States

State or Province: IN

ZIP/Postal Code: 46032

Email Address: null

Organization Name: null

Comment: I would still like the ability to run open source firmware like OpenWRT and DD-WRT on wireless routers and disapprove of this draconian overarching regulation.

The FCC could instead put more money in the actual enforcement and tracking down violators (malicious/intentful or accidental), if this was an actual problem this issue would've been brought up long ago.

I would still like the ability to run open source firmware like OpenWRT and DD-WRT on wireless routers and disapprove of this draconian overarching regulation.

The FCC could instead put more money in the actual enforcement and tracking down violators (malicious/intentful or accidental), if this was an actual problem this issue would've been brought up long ago.

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: Bolger

Mailing Address: 1760 Taxville Road

City: York

Country: United States

State or Province: PA

ZIP/Postal Code: 17408

Email Address: mikebolger@gmail.com

Organization Name:

Comment: See attached file.

See attached file.

Although the signers believe that Commission has the best of intentions, the signers believe that the NPRM is a dangerous intrusion upon the rights of computing users and substantially interferes with innovation in the wireless space.

The signers are concerned about three changes in the NPRM:

- § 2.1033 Application for grant of certification. Paragraph 4(i),
- § 2.935 Electronic labeling of radiofrequency devices. Clause (d) and
- § 2.1042 Certified modular transmitters. Section 8(e)

The NPRM removes the ability of computing users to control and modify their devices in both Paragraph 4(i). In Paragraph 4(i), the manufacturer is required to describe how the software of the device is secured against modification. Additionally, Clause (d) implies that the device must be secured against modification due to the requirement to prevent label information from being modified. Finally, Section 8(e) requires manufacturers to only allow "approved" software to be installed on a device. These requirements combined prevent most modifications to the device even when the user wants to improve on the security of the device or even to correct problems with the wireless radio software itself.

Infringing upon computing users rights

Until now, users of computing devices have had the ability to install the software of their choice. In particular, users have had the ability to install free and open source operating systems and software which most appropriately fits their needs. Whether the user wants to install OpenWrt on a router or a distribution based upon the Linux kernel on their laptop computer or smartphone, users have been able to control the devices they own. Through this control, users can explore how their computing devices work, educate themselves on the design of hardware, protect themselves from invasive spying by competitors and foreign governments and enrich their own lives and the lives of others through improved software.

Interfering with innovation in the wireless space

Innovation in network and wireless technology depends on the ability of users and resellers to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, [developed a fix](#) for an important form of network congestion called Bufferbloat. This fix is [added](#) to the Linux kernel to be used by the billions of users of Linux.

Mesh networking technologies for developing stable distributed internet access are regularly implemented using various versions of Linux installed by an end-user and [much research and implementation on mesh networking](#) has occurred outside of manufacturers. [Nearly 7,200 scholarly articles](#) on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Mesh networking is [used for data](#)

[communication by amateur radio operators](#) responding to natural disasters. Without the ability to change the software on the device, these innovations would not have occurred.

User-access to source code is another innovation in and of itself. It has led to bug fixes, security enhancements, and features that were not part of the original code base. In one instance a user was able to fix a critical bug impacting all wifi adapters based on a particular set of Qualcomm Atheros wireless chipset(s). As users were frequently being disconnected under certain conditions one user took it upon themselves to track down and fix the bug [1]. This would not have been possible had the source code for the firmware been unavailable, or had these devices otherwise been locked.

Finally, numerous companies modify the software on off-the-shelf wireless devices for custom uses. Companies who sell hardware to retailers for WiFi hotspots often install software customized to that task. Additionally many commercial VPN providers sell wireless routers as part of their product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Recommendations

The signers respectfully recommend the following changes:

The regulations on software defined radios should not restrict the ability to replace software on computing devices

As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law abiding users to understand and improve the software on their devices.

The regulations on e-labels should not restrict the ability to replace software on computing devices

The signers appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

Conclusion

The signers share the commission's interest in protecting the wireless spectrum. As the Commission deliberates on the NPRM, we invite the Commission to meet with signers, the computing industry, users, free and open source software advocates and all interested parties. Through a collaboration we believe the wireless spectrum can be protected while enabling the innovation and freedom key to American competitiveness in the 21st century.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: John

Last Name: Carter

Mailing Address: 1055 Rugglestone Way

City: duluth

Country: United States

State or Province: GA

ZIP/Postal Code: 30097

Email Address: mattcarter64@gmail.com

Organization Name:

Comment: Hello,

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

Some additional points i would like to add are:

- 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.

Hello,

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

Some additional points i would like to add are:

- 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.

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: Driscoll

Mailing Address: 9 Sutton Place

City: Pleasantville

Country: United States

State or Province: NY

ZIP/Postal Code: 10570

Email Address: BrianDriscoll@yahoo.com

Organization Name:

Comment: Users should be able to install their own custom firmware on WiFi routers and other wireless routers that they own.

Users should be able to install their own custom firmware on WiFi routers and other wireless routers that they 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: Christopher

Last Name: de Vidal

Mailing Address: 11014 Starwood Dr

City: Jacksonville

Country: United States

State or Province: FL

ZIP/Postal Code: 32256

Email Address: CBdeVidal.jk1@Gmail.com

Organization Name:

Comment: Please do not implement these rules.

- * They will 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.
- * There will eventually be millions upon millions of vulnerable devices for which there's no way to upgrade the firmware.
- * There will be a chilling effect on the development of open source software and hinder the market.
- * 90% of all Internet-connected devices are running some form of Linux. Linux developers need the power to be able to modify and test all sorts of configurations in all sorts of hardware for countries all over the world.
- * By banning modification of hardware you'll effectively be banning a considerable portion of open source development in the USA.
- * Since other countries mostly just use the same hardware as what ships in the United States it will likely lead to fewer and fewer hardware options for open source developers.

Please do not implement these rules.

- * They will 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.
- * There will eventually be millions upon millions of vulnerable devices for which there's no way to upgrade the firmware.
- * There will be a chilling effect on the development of open source software and hinder the market.
- * 90% of all Internet-connected devices are running some form of Linux. Linux developers need the power to be able to modify and test all sorts of configurations in all sorts of hardware for countries all over the world.
- * By banning modification of hardware you'll effectively be banning a considerable portion of open source development in the USA.
- * Since other countries mostly just use the same hardware as what ships in the United States it will likely lead to fewer

and fewer hardware options for open source developers.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Andrew

Last Name: Rushmore

Mailing Address: 30 Sherman ST

City: Denver

Country: United States

State or Province: CO

ZIP/Postal Code: 80203

Email Address: ajrushmore@gmail.com

Organization Name:

Comment: Please allow firmware to remain open, just as the Internet with the recent FCC moves.

Don't take a step backwards.

Corporations timelines for researching security vulnerabilities should not set the timeline for security for wireless networking.

How often have companies waited until the last minute to fix an issue, instead of being preemptive? EVEN if that issue causes loss of lives of American Citizens. That's a great analogy for this situation. Imagine if my router has to wait for a security update to the point that my security is compromised. When anyone could have released a patch to protect us faster.

As a national security issue, imagine if a Secretary of State had her emails on a private server that was accessed through a router that didn't have the needed security due to this proposed legislation. Topical, timely, scary.

Please keep advancing America so we continue to remain the strongest nation in our world, and allow us to remain free from corporate oversight that is focused on the bottom line, regardless of the user experience.

We trust you, and thank you for your service.

Please allow firmware to remain open, just as the Internet with the recent FCC moves.

Don't take a step backwards.

Corporations timelines for researching security vulnerabilities should not set the timeline for security for wireless networking.

How often have companies waited until the last minute to fix an issue, instead of being preemptive? EVEN if that issue causes loss of lives of American Citizens. That's a great analogy for this situation. Imagine if my router has to wait for a security update to the point that my security is compromised. When anyone could have released a patch to protect us faster.

As a national security issue, imagine if a Secretary of State had her emails on a private server that was accessed through a router that didn't have the needed security due to this proposed legislation. Topical, timely, scary.

Please keep advancing America so we continue to remain the strongest nation in our world, and allow us to remain free from corporate oversight that is focused on the bottom line, regardless of the user experience.

We trust you, and thank you for your service.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kevin

Last Name: Kleinhomer

Mailing Address: 15 Forestal Circle

City: Newark

Country: United States

State or Province: DE

ZIP/Postal Code: 19711

Email Address: kevin@kleinhomer.com

Organization Name: n/a

Comment: This rule would kill many home wifi routers in the consumer space that have been abandoned by their manufacturers or have problematic firmware to begin with. There is a strong community around alternative and secure replacement firmware for these routers that enable them to continue to work and or become much more secure and usable than their factory firmware. Please consider either abandoning this or creating an exception for consumer wifi devices so that we can continue to support older and or unsecure devices with more robust and secure replacement firmware.

This rule would kill many home wifi routers in the consumer space that have been abandoned by their manufacturers or have problematic firmware to begin with. There is a strong community around alternative and secure replacement firmware for these routers that enable them to continue to work and or become much more secure and usable than their factory firmware. Please consider either abandoning this or creating an exception for consumer wifi devices so that we can continue to support older and or unsecure devices with more robust and secure replacement firmware.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: James

Last Name: Dempsey

Mailing Address: 21 Old Orchard Ln.

City: Boxborough

Country: United States

State or Province: MA

ZIP/Postal Code: 01719

Email Address: jjd+federalregister@jld.com

Organization Name:

Comment: This proposed regulation would be anti-freedom, reduce consumer choice and reduce security in the Internet.

Many commercially available routers that operate in the 5Ghz range allow for using 3rd party firmware on the routers. This 3rd party firmware is typically open source and offer features and security that are not available in the software supplied with the commercial router. (Those OEM softwares (often Chinese in origin) have often been the subject of security problems. Third party software such as OpenWRT and Tomato are in wide use, are significantly more secure and offer features that are not available in the commercial software. By restricting the firmware allowed on the devices, this firmware would likely be deemed illegal and consumers would have no choice but to use the insecure, less featureful OEM software.

It is understandable that the FCC might want to control the radio portions of this firmware in order to keep the public airways safe for everyone. However, such a regulation would have to carefully be written to allow the use of 3rd party router protocol firmware that doesn't affect the radio portion of the software.

Please do not approve this anti-freedom regulation as-is that reduces consumer freedom and security.

This proposed regulation would be anti-freedom, reduce consumer choice and reduce security in the Internet.

Many commercially available routers that operate in the 5Ghz range allow for using 3rd party firmware on the routers. This 3rd party firmware is typically open source and offer features and security that are not available in the software supplied with the commercial router. (Those OEM softwares (often Chinese in origin) have often been the subject of security problems. Third party software such as OpenWRT and Tomato are in wide use, are significantly more secure and offer features that are not available in the commercial software. By restricting the firmware allowed on the devices, this firmware would likely be deemed illegal and consumers would have no choice but to use the insecure, less featureful OEM software.

It is understandable that the FCC might want to control the radio portions of this firmware in order to keep the public airways safe for everyone. However, such a regulation would have to carefully be written to allow the use of 3rd party router protocol firmware that doesn't affect the radio portion of the software.

Please do not approve this anti-freedom regulation as-is that reduces consumer freedom and security.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ian

Last Name: Luster

Mailing Address: 5565 Redwood St

City: San Diego

Country: United States

State or Province: CA

ZIP/Postal Code: 92105

Email Address:

Organization Name:

Comment: I am a a firmware engineer working for a wireless company in San Diego. Banning changes to the firmware of a network device which I own is ludicrous. As long as the radio operates in the same range and at the same power it was originally certified at it remains the same radio. Updating the firmware of SoC processors while leaving the radio parameters and drivers in place is entirley safe. Please refrain from over simplifying regulations to the detriment of progress and innovation.

I am a a firmware engineer working for a wireless company in San Diego. Banning changes to the firmware of a network device which I own is ludicrous. As long as the radio operates in the same range and at the same power it was originally certified at it remains the same radio. Updating the firmware of SoC processors while leaving the radio parameters and drivers in place is entirley safe. Please refrain from over simplifying regulations to the detriment of progress and innovation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Kevin

Last Name: Ray

Mailing Address: 9 Brian Ct

City: Algonquin

Country: United States

State or Province: IL

ZIP/Postal Code: 60102

Email Address: kevin@kray.com

Organization Name: KRay

Comment: Limiting the ability to re-program [wifi] routers for end users is beyond dangerous.

I can't name one (1) manufacturer for [any] router that takes security seriously.

Making it illegal to modify various radio properties beyond certain limits is fine -- and already exist as laws on the books that the FCC can enforce. Adding addition restrictions is fruitless -- and given the choice I WILL break the law and install OpenWRT on any router I deem necessary [read: ALL of them].

Limiting the ability to re-program [wifi] routers for end users is beyond dangerous.

I can't name one (1) manufacturer for [any] router that takes security seriously.

Making it illegal to modify various radio properties beyond certain limits is fine -- and already exist as laws on the books that the FCC can enforce. Adding addition restrictions is fruitless -- and given the choice I WILL break the law and install OpenWRT on any router I deem necessary [read: ALL of them].

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: Tom

Last Name: Vickers

Mailing Address: 5785 Sugar Crossing Dr

City: Sugar Hill

Country: United States

State or Province: GA

ZIP/Postal Code: 30518

Email Address: thomas.e.vickers@gmail.com

Organization Name:

Comment: I would request that you not implement any rules that take away the ability of users to install software of my choice on my computing devices (including network equipment like routers and wifi devices). Implementing rules like this will inhibit innovation and improvements. It will limit the ability of the community to improve existing hardware when the manufacturer chooses not to. I am writing this comment using a modified wifi router that had a bug in the firmware that the manufacturer was unwilling to fix. The community of developers found a solution and released the improved code without charge. This type of innovation will be lost if you take away the ability to replace the factory firmware of network devices.

I would request that you not implement any rules that take away the ability of users to install software of my choice on my computing devices (including network equipment like routers and wifi devices). Implementing rules like this will inhibit innovation and improvements. It will limit the ability of the community to improve existing hardware when the manufacturer chooses not to. I am writing this comment using a modified wifi router that had a bug in the firmware that the manufacturer was unwilling to fix. The community of developers found a solution and released the improved code without charge. This type of innovation will be lost if you take away the ability to replace the factory firmware of network 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: Matthew

Last Name: Ellis

Mailing Address: 3526 Royal Ave

City: Simi Valley

Country: United States

State or Province: CA

ZIP/Postal Code: 93063

Email Address:

Organization Name:

Comment: User Freedom

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

User Freedom

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Thomas

Last Name: Doggette

Mailing Address: 136 Clingman Ave

City: Asheville

Country: United States

State or Province: NC

ZIP/Postal Code: 28801

Email Address: tdoggette@gmail.com

Organization Name:

Comment: I urge the FCC not to implement rules that limit the ability of American consumers to use whatever software they choose on the hardware they own. Further, these proposed rules would handcuff the US technology industry-- being able to develop and use new software (on hardware you own) is absolutely key to innovation.

I urge the FCC not to implement rules that limit the ability of American consumers to use whatever software they choose on the hardware they own. Further, these proposed rules would handcuff the US technology industry-- being able to develop and use new software (on hardware you own) is absolutely key to innovation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Erik

Last Name: Troan

Mailing Address: 1707 MCDONALD LN

City: RALEIGH

Country: United States

State or Province: NC

ZIP/Postal Code: 27608

Email Address: ewt@troan.org

Organization Name:

Comment: Please reconsider banning custom software on off the shelf devices.

If this rule were in place, projects like the Linux operating system would have been impossible. As the first engineer at Red Hat, I watched billions of dollars of value get created across the computing economy by letting technologists experiment with their hardware. This ruling would make such efforts either difficult or impossible, and cause irreparable harm.

Apart from the direct economic impact, this would remove educational opportunities. Today students can buy inexpensive devices and learn how they work, modify their software, and test the impact those changes have. They learn by doing with real hardware and that type of experience is irreplaceable. As our country struggles to fill high tech and STEM job offerings, removing an educational tool which excites our students would be a step backwards.

Finally, banning users from modifying items they have purchased is like banning drivers from changing their own brakes. Users who buy a set of electronics own those and should be allowed to modify, repair, and experiment with them just as if they had bought the individual parts. We have a long tradition of support consumer rights and open shops, and there is no compelling reason to go against that here.

Thank you for taking the time to read these comments.

Please reconsider banning custom software on off the shelf devices.

If this rule were in place, projects like the Linux operating system would have been impossible. As the first engineer at Red Hat, I watched billions of dollars of value get created across the computing economy by letting technologists experiment with their hardware. This ruling would make such efforts either difficult or impossible, and cause irreparable harm.

Apart from the direct economic impact, this would remove educational opportunities. Today students can buy inexpensive devices and learn how they work, modify their software, and test the impact those changes have. They learn by doing with real hardware and that type of experience is irreplaceable. As our country struggles to fill high tech and STEM job offerings, removing an educational tool which excites our students would be a step backwards.

Finally, banning users from modifying items they have purchased is like banning drivers from changing their own brakes. Users who buy a set of electronics own those and should be allowed to modify, repair, and experiment with them just as if they had bought the individual parts. We have a long tradition of support consumer rights and open

shops, and there is no compelling reason to go against that here.

Thank you for taking the time to read these comments.

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: Susan

Last Name: Tussing

Mailing Address: 66 W. Tallmadge Ave. #1

City: Akron

Country: United States

State or Province: OH

ZIP/Postal Code: 44310

Email Address: srtussing@gmail.com

Organization Name:

Comment: As a consumer, I own a number of devices that would fall under the proposed regulations, including a tablet and smartphone that run the Android operating system. Recently, Samsung pushed an update to my tablet which contained a bug that completely disabled many peripheral devices. This was in July. They did not release a fix for this until late August. I'm not economically in a position to replace my devices when things like this happen, nor am I in a position to wait for the manufacturer to take weeks or months to address the issue. After a few days of waiting, I installed an alternative Android firmware called Cyanogen, which never had the bug the Samsung firmware did, and I was suddenly able to use my device as intended. As an individual, I have no power to hold Samsung or any other manufacturer accountable if they release broken updates or, worse, stop releasing updates for my devices entirely. I do have the power to make alternate decisions about how to use my hardware.

The proposed regulation relies upon manufacturers to maintain working firmware. The manufacturers in question have already proven beyond any possible doubt that they cannot be trusted with this responsibility. Multiply my experience by every Android-using consumer in the United States, and the proposed regulation deprives all of us of the ability to maintain working and secure devices. Moreover, it puts an unfair burden on those with fewer resources, who are more likely to need third-party software to keep older devices working.

I would respectfully ask that the FCC not adopt the proposed regulation.

As a consumer, I own a number of devices that would fall under the proposed regulations, including a tablet and smartphone that run the Android operating system. Recently, Samsung pushed an update to my tablet which contained a bug that completely disabled many peripheral devices. This was in July. They did not release a fix for this until late August. I'm not economically in a position to replace my devices when things like this happen, nor am I in a position to wait for the manufacturer to take weeks or months to address the issue. After a few days of waiting, I installed an alternative Android firmware called Cyanogen, which never had the bug the Samsung firmware did, and I was suddenly able to use my device as intended. As an individual, I have no power to hold Samsung or any other manufacturer accountable if they release broken updates or, worse, stop releasing updates for my devices entirely. I do have the power to make alternate decisions about how to use my hardware.

The proposed regulation relies upon manufacturers to maintain working firmware. The manufacturers in question have already proven beyond any possible doubt that they cannot be trusted with this responsibility. Multiply my experience by every Android-using consumer in the United States, and the proposed regulation deprives all of us of the ability to maintain working and secure devices. Moreover, it puts an unfair burden on those with fewer resources, who are more likely to need third-party software to keep older devices working.

I would respectfully ask that the FCC not adopt the proposed regulation.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Diego

Last Name: Ercolani

Mailing Address: Serravalle

City: Serravalle

Country: San Marino

State or Province: San Marino

ZIP/Postal Code: 47891

Email Address:

Organization Name:

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

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

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

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

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

Thanks for listening.

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

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

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

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

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

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

Thanks for listening.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Ian

Last Name: Garris

Mailing Address: 2317 Dunbury Ct.

City: Winter Park

Country: United States

State or Province: FL

ZIP/Postal Code: 32792-6043

Email Address: ian.garris@gmail.com

Organization Name:

Comment: The scourge of botnets is well documented by now; what's less well known is that pwned routers have become a major component of this malady. Please do not do anything to further discourage the necessary security updates that we're already not receiving; with firmware etched into ROM - literally, or its functional equivalent WORM media - things will get worse. Viruses can persist, memory-resident, for years; most routers are never deliberately rebooted. Like an unpatched Windows XP machine, the time to compromise will be far shorter than the time to patch; once connected to the internet, vulnerable routers will be Owned in short order. And with no way to recover from a manufacturer's bleep-up, a catastrophic error at the time of manufacture (shipping known-vulnerable uP&P code, for example; use of demonstration code in production environments is endemic!) will lead to a direct-to-dumpster release for hardware except we both know that won't happen. It will be shipped to Wal-Mart on the cheap, who will distribute it to uninformed customers, who will operate it in perpetuity. It's only prompt and semiautomated firmware updates (automatic checking, manual installation) that successfully mitigates cyberattacks and brick-inducing bugs simultaneously.

Please don't double down on the egregious misconduct of SOHO router vendors, and don't stop the distribution of secure, well-vetted, and carefully engineered aftermarket firmware like Tomato and DD-WRT. We don't all have unlimited budgets, and I'd go so far as to say that most of us can't drop a couple hundred dollars on trustworthy IT equipment every time a new software exploit is found - I cringe every time lightning fries something, and if I had to buy new hardware six times a year, I'd simply give up on electronic banking & commerce.

And now we come to the crux of the argument - trustable networks underlie *vast* swaths of the American economy. Please, in the name of whatever you hold holy, don't bleep the economy *again*. We can't afford another recession because shortsighted regulation cut the American innovation engine off at the knees. This is important, and it's connected - and did I mention that it's *important?*

I understand there are risks associated with unlocked router hardware, and enforcement costs are well north of zero. But please realize that the costs of screwing up might involve the replacement of hundreds of millions of devices - mostly, per the law of averages - by poor and middle-income Americans with private funds, under the threat of identity theft and each one who doesn't act in time represents up to a million dollars each of fraud, associated expenses, and stress-related medical care. As heart disease still represents the leading cause of death in America per the CDC by a wide margin, (and stress is a factor in cancer per emerging medical research) small increases in stress nationwide can be expected to have a disproportionate impact on morbidity & mortality. Once again, per the law of averages, lots of those who suffer health impacts related to someone stealing their identity (and retirement savings, and rent money) will be too broke to pay for emergency hospital treatments (because they just got robbed).

Please pause to consider ramifications for twenty minutes before seriously considering implementing this proposal. It just gets worse the more steps removed you get.

The scourge of botnets is well documented by now; what's less well known is that pwned routers have become a major component of this malady. Please do not do anything to further discourage the necessary security updates that we're already not receiving; with firmware etched into ROM - literally, or its functional equivalent WORM media - things will get worse. Viruses can persist, memory-resident, for years; most routers are never deliberately rebooted. Like an unpatched Windows XP machine, the time to compromise will be far shorter than the time to patch; once connected to the internet, vulnerable routers will be Owned in short order. And with no way to recover from a manufacturer's bleep-up, a catastrophic error at the time of manufacture (shipping known-vulnerable uP&P code, for example; use of demonstration code in production environments is endemic!) will lead to a direct-to-dumpster release for hardware except we both know that won't happen. It will be shipped to Wal-Mart on the cheap, who will distribute it to uninformed customers, who will operate it in perpetuity. It's only prompt and semiautomated firmware updates (automatic checking, manual installation) that successfully mitigates cyberattacks and brick-inducing bugs simultaneously.

Please don't double down on the egregious misconduct of SOHO router vendors, and don't stop the distribution of secure, well-vetted, and carefully engineered aftermarket firmware like Tomato and DD-WRT. We don't all have unlimited budgets, and I'd go so far as to say that most of us can't drop a couple hundred dollars on trustworthy IT equipment every time a new software exploit is found - I cringe every time lightning fries something, and if I had to buy new hardware six times a year, I'd simply give up on electronic banking & commerce.

And now we come to the crux of the argument - trustable networks underlie **vast** swaths of the American economy. Please, in the name of whatever you hold holy, don't bleep the economy **again**. We can't afford another recession because shortsighted regulation cut the American innovation engine off at the knees. This is important, and it's connected - and did I mention that it's **important?**

I understand there are risks associated with unlocked router hardware, and enforcement costs are well north of zero. But please realize that the costs of screwing up might involve the replacement of hundreds of millions of devices - mostly, per the law of averages - by poor and middle-income Americans with private funds, under the threat of identity theft and each one who doesn't act in time represents up to a million dollars each of fraud, associated expenses, and stress-related medical care. As heart disease still represents the leading cause of death in America per the CDC by a wide margin, (and stress is a factor in cancer per emerging medical research) small increases in stress nationwide can be expected to have a disproportionate impact on morbidity & mortality. Once again, per the law of averages, lots of those who suffer health impacts related to someone stealing their identity (and retirement savings, and rent money) will be too broke to pay for emergency hospital treatments (because they just got robbed).

Please pause to consider ramifications for twenty minutes before seriously considering implementing this proposal. It just gets worse the more steps removed you get.

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: Samuel

Last Name: Herniman

Mailing Address: 5224 Beaumont Way

City: Santa Rosa

Country: United States

State or Province: CA

ZIP/Postal Code: 95409

Email Address:

Organization Name:

Comment: If there is one thing I have learnt over the last few years, it is that we have to work with the future and not against it. This is not the time to regulate the router industry.

If there is one thing I have learnt over the last few years, it is that we have to work with the future and not against it. This is not the time to regulate the router industry.

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: Margarita

Last Name: Zakirova

Mailing Address: Hersonskaya St.

City: Moscow

Country: Russia

State or Province: Moscow

ZIP/Postal Code: 117461

Email Address: margisha@ya.ru

Organization Name:

Comment: You cannot encroach on technical progress. This law contradicts the Constitution and the development of science in the future.

You cannot encroach on technical progress. This law contradicts the Constitution and the development of science in the future.

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: Konstantin

Last Name: Bazdyrev

Mailing Address: Krilova street 8-182

City: Moscow

Country: Russia

State or Province: Moscow state

ZIP/Postal Code: 143000

Email Address: warmonger2000@hotmail.ru

Organization Name:

Comment: SaveWifi

SaveWifi

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: Ricky

Last Name: Elrod

Mailing Address: 1474 Hampton Road

City: Akron

Country: United States

State or Province: OH

ZIP/Postal Code: 44305

Email Address:

Organization Name:

Comment: I hereby 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.

I hereby 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.