

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: Connor

Last Name: Johnson

Mailing Address: 910 Granger Drive

City: Allen

Country: United States

State or Province: TX

ZIP/Postal Code: 75013-1112

Email Address:

Organization Name:

Comment: I believe that although it may not be the intention of this document to do so, this regulation could prohibit users from installing, developing, or customizing their own software on their own devices. It is concerning to me as a person who uses open-source software, that it is possible for the government to regulate how I use the device that I purchased and what I can install on my computer. By requiring firmware, the government could hurt businesses and home users of open source software and operating systems.

I believe that although it may not be the intention of this document to do so, this regulation could prohibit users from installing, developing, or customizing their own software on their own devices. It is concerning to me as a person who uses open-source software, that it is possible for the government to regulate how I use the device that I purchased and what I can install on my computer. By requiring firmware, the government could hurt businesses and home users of open source software and operating 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: Nicolas

Last Name: Schurando

Mailing Address: 2 Rue de Verdun

City: Eaubonne

Country: France

State or Province: Ile-de-France

ZIP/Postal Code: 95600

Email Address:

Organization Name:

Comment: Hello,

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

As an embedded systems engineer, I consider that it is with a good understanding of the ins and the outs that I can make this request. In particular,

- Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
  - Consider also that although FCC rules apply in the United States of America, they do impact the rest of the world as handling exceptions in product development is often avoided to minimize costs.
  - The security of any system relies on its openness and the ability for experienced and even less experienced users to experiment, contribute and publish their findings with the rest of the world.
- Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- Wireless networking research depends on the ability of researchers to investigate and modify their devices.
  - 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 considering this request.

Hello,

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

As an embedded systems engineer, I consider that it is with a good understanding of the ins and the outs that I can make this request. In particular,

- Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
  - Consider also that although FCC rules apply in the United States of America, they do impact the rest of the world as handling exceptions in product development is often avoided to minimize costs.
  - The security of any system relies on its openness and the ability for experienced and even less experienced users to experiment, contribute and publish their findings with the rest of the world.
- Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

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

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: Dan

Last Name: Forbes

Mailing Address: 6405 Haney Drive

City: Austin

Country: United States

State or Province: TX

ZIP/Postal Code: 78723

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.

My reasons for making this request include:

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

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.

My reasons for making this request include:

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

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: K.G.H.

Last Name: Nicholes

Mailing Address: 10 Jawbone Rd

City: Martinsdale

Country: United States

State or Province: MT

ZIP/Postal Code: 59053

Email Address: kg hn@ttc-cmc.net

Organization Name: null

Comment: Do not restrict device owners'/users' flashing of firmware.

Do not restrict device owners'/users' flashing of 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: H.

Last Name: van Megen

Mailing Address: Corterhoven 40

City: Druten

Country: Netherlands

State or Province: Gelderland

ZIP/Postal Code: 6552GV

Email Address: hvanmegen+wifi.federalregister.gov@gmail.com

Organization Name:

Comment: As an European citizen with a lot of American friends I must stress that this proposed rule is going to have a serious negative impact on your economy and national security:

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

Please find the wisdom to reconsider.

As an European citizen with a lot of American friends I must stress that this proposed rule is going to have a serious negative impact on your economy and national security:

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

Please find the wisdom to reconsider.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Derek

Last Name: LaHousse

Mailing Address: 12306 Malvern Way

City: Bristow

Country: United States

State or Province: VA

ZIP/Postal Code: 20136

Email Address: dlahouss@mtu.edu

Organization Name: null

Comment: I request that the FCC not implement the rule as it is written, as it will have minimal effect toward the stated goal of enforcing band compliance and many negative effects on consumers and users of equipment.

Every day, bugs are discovered in software running on consumer devices. Some of these bugs enable an attacker to take control of the device and use it to the detriment of the device owner or other internet users. The best way to protect devices is to keep software up-to-date with bug fixes. A requirement to load only signed firmware would mean that any updates to the software would need to be delivered by the device manufacturer. Historically, device manufacturers' commitment to updates ends when the next model year is delivered. For a concrete example, the venerable WRT54G still receives updates, but only through third-party firmware such as OpenWRT. If it were under the proposed FCC rule, consumers would be left vulnerable.

On the other side of the proposal, the requirement for signed firmware is not iron-clad proof against the loading of third-party software. Many cell phone vendors have had their firmware usurped by enterprising individuals, allowing such third-party operating systems as Replicant and CyanogenMod. While these firmwares are used for positive ends, it demonstrates that a criminal who seeks to step outside the wifi regulations would be no more limited by a requirement to run signed firmware. Only those consumers who are following the rules would be limited by the proposal.

In summation, the proposed rule causes a burden on device manufacturers, limits consumers who want to follow the rules, and does not prevent criminals from breaking the rules. Please do not enact this rule.

I request that the FCC not implement the rule as it is written, as it will have minimal effect toward the stated goal of enforcing band compliance and many negative effects on consumers and users of equipment.

Every day, bugs are discovered in software running on consumer devices. Some of these bugs enable an attacker to take control of the device and use it to the detriment of the device owner or other internet users. The best way to protect devices is to keep software up-to-date with bug fixes. A requirement to load only signed firmware would mean that any updates to the software would need to be delivered by the device manufacturer. Historically, device manufacturers' commitment to updates ends when the next model year is delivered. For a concrete example, the venerable WRT54G still receives updates, but only through third-party firmware such as OpenWRT. If it were under the proposed FCC rule, consumers would be left vulnerable.

On the other side of the proposal, the requirement for signed firmware is not iron-clad proof against the loading of third-party software. Many cell phone vendors have had their firmware usurped by enterprising individuals, allowing such third-party operating systems as Replicant and CyanogenMod. While these firmwares are used for positive ends, it demonstrates that a criminal who seeks to step outside the wifi regulations would be no more limited by a requirement to run signed firmware. Only those consumers who are following the rules would be limited by the proposal.

In summation, the proposed rule causes a burden on device manufacturers, limits consumers who want to follow the rules, and does not prevent criminals from breaking the rules. Please do not enact this rule.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Christopher

Last Name: Silver

Mailing Address: 7816 Southside Blvd S

City: Jacksonville

Country: United States

State or Province: FL

ZIP/Postal Code: 32256-0710

Email Address:

Organization Name:

Comment: Preventing flashing of firmware on wifi devices will prevent people like me from using open source routing software such as DD-WRT and OpenWRT on devices which have integrated wifi chipsets. In the modern era, many new SoC systems will have this stack integrated into them and will thus prevent them from receiving any firmware updates. This will include embedded devices as well as cellphones. A ruling to disallow reflashing of firmware only supports additional vendor lock in, and I do not support that as an engineer or a consumer.

Preventing flashing of firmware on wifi devices will prevent people like me from using open source routing software such as DD-WRT and OpenWRT on devices which have integrated wifi chipsets. In the modern era, many new SoC systems will have this stack integrated into them and will thus prevent them from receiving any firmware updates. This will include embedded devices as well as cellphones. A ruling to disallow reflashing of firmware only supports additional vendor lock in, and I do not support that as an engineer or a consumer.

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: June

Last Name: Taylor

Mailing Address: 639 Humbolt Ave

City: St Paul

Country: United States

State or Province: MN

ZIP/Postal Code: 55107

Email Address: june@simplykiwi.com

Organization Name:

Comment: Respectfully, I 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.

It is vital that users remain in control of all levels of the technology we use.

Respectfully, I 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.

It is vital that users remain in control of all levels of the technology we use.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Robert

Last Name: Berg

Mailing Address: 1707 w 140th st

City: Burnsville

Country: United States

State or Province: MN

ZIP/Postal Code: 55337

Email Address:

Organization Name:

Comment: The environment simply cannot handle more regulations that prevent recycling of consumer products. The ability to change firmware of a device that has been purchased by individuals, allows re-purposing, and reusing hardware that would normally be thrown into the garbage.

This only benefits big business, and imprisons innovative, creative, and intelligent individuals who want to get the most out of their property.

And they will do it anyway. We don't need to add more, to the ever growing list of incarcerated individuals in the current American population of inmates.

Which by the way, is the largest on the planet, in every way, compared to other nations.

Land of the free, really?

Throwing people in prison is not moving into the bright technological future that we all want.

PrisonPlanet?

or

PrivilegedPlanet?

You decide.

P.S. If you want to make more rules and regulations, why not force foreign companies to comply with U.S. rules of human rights, employee rights, in their factories if they want to sell products to United States markets.

How does this comment relate to the current topic? Well, simply refusing a products FCC approval from manufacturers who fail to meet U.S. labor standards for their workers(no matter where that product is made) if they want the product to be sold in American markets.

The environment simply cannot handle more regulations that prevent recycling of consumer products. The ability to change firmware of a device that has been purchased by individuals, allows re-purposing, and reusing hardware that would normally be thrown into the garbage.

This only benefits big business, and imprisons innovative, creative, and intelligent individuals who want to get the most out of their property.

And they will do it anyway. We don't need to add more, to the ever growing list of incarcerated individuals in the current American population of inmates.

Which by the way, is the largest on the planet, in every way, compared to other nations.

Land of the free, really?

Throwing people in prison is not moving into the bright technological future that we all want.

PrisonPlanet?

or

PrivilegedPlanet?

You decide.

P.S. If you want to make more rules and regulations, why not force foreign companies to comply with U.S. rules of human rights, employee rights, in their factories if they want to sell products to United States markets.

How does this comment relate to the current topic? Well, simply refusing a products FCC approval from manufacturers who fail to meet U.S. labor standards for their workers(no matter where that product is made) if they want the product to be sold in American markets.

# Labor Rights in China

China wants to change its labor law in favor of workers and, according to Tim Costello, Brendan Smith, and Jeremy Brecher, foreign corporations are squawking.

By [Brendan Smith](#), [Tim Costello](#) and [Jeremy Brecher](#). Edited by [John Feffer](#), December 19, 2006.

Share



A major debate is underway in China on a proposed law that would grant new rights to Chinese workers. The debate has not been widely reported outside of China; until recently it has been almost entirely ignored by media in the United States. But when the Chinese government opened a 30-day public comment period this spring, it received nearly 200,000 comments, the majority from ordinary workers. But some comments also came from big U.S.- and European-based global corporations and their lobbying groups. These powerful forces squarely opposed the new law.

Wal-Mart's recent agreement to recognize unions in China has made headlines worldwide. But Wal-Mart and other corporations, including Google, UPS, Microsoft, Nike, AT&T, and Intel, have acted through the American Chamber of Commerce in Shanghai (AmCham) and other industry associations to try to block Chinese legislation that would significantly increase the power and protection of workers.

This corporate campaign contradicts the justifications that have been given for public policies that encourage corporations to invest in China. U.S.-based corporations have repeatedly claimed to be raising human and labor rights standards abroad. For example, the American Chamber of Commerce in Hong Kong asserts among its "[universal principles](#)" that "American business plays an important role as a catalyst for positive social change by promoting human welfare and guaranteeing to uphold the dignity of the workers and set positive examples for their remuneration, treatment, health, and safety." But U.S.-based corporations are trying to block legislation designed specifically to improve the remuneration, treatment, health and safety, and other standards for Chinese workers.

At a time when China exerts a growing impact on the global economy, efforts to improve the conditions of Chinese workers are profoundly important for workers everywhere. As U.S. wages stagnate, many Americans worry that low wages and labor standards in China are driving down those in America. Improving labor conditions in China can thus help workers in the rest of the world resist a race to the bottom that threatens to bring global wages and conditions down to the level of the least protected.

China's proposed legislation will not eliminate its labor problems. The law will not provide Chinese workers with the right to independent trade unions with leaders of their own choosing and the right to strike. But foreign corporations are attacking the legislation not because it

provides workers too little protection but because it provides them too much. Indeed, the proposed law may well encourage workers to organize to demand the enforcement of the rights it offers. And the prospect of independent, organized labor in China has pushed corporations to do some organizing of their own.

## **Corporate Campaign**

The Chinese government released its Draft Labor Contract Law, whose proclaimed purpose is to protect workers' rights and interests, in April. The corporate campaign against the law began soon after, spearheaded by three major organizations representing foreign corporations operating in China: the American Chamber of Commerce in Shanghai (representing over 1,300 corporations, including 150 Fortune 500 companies), the U.S.-China Business Council (representing 250 U.S. companies doing business across all sectors in China), and the European Union Chamber of Commerce in China (representing more than 860 members). All three have sent the Chinese government extensive attacks on the proposed law. The [statement](#) of AmCham in Shanghai runs to 42 pages.

These organizations have also issued barely veiled threats that foreign companies will leave China if the new legislation is passed. According to AmCham [comments](#) on the draft legislation, the law may “reduce employment opportunities for PRC workers” and “negatively impact the PRC’s competitiveness and appeal as a destination for foreign investment.”

“Business is attracted to China not only because of its labor costs but also because of its efficiency,” [states](#) Dr. Keyong Wu, an expert for the British Chambers of Commerce. “If regulation starts to affect that and flexibility, then companies could turn to India, Pakistan, and South-East Asia.”

American corporations have so much affection for the status quo in China that they have gone out of their way to preserve current Chinese labor law. As the AmCham document proclaims, that labor law has “significantly promoted standardized operation of enterprises and establishment of modern enterprise system.” AmCham criticizes the proposed changes in the law for making it harder to fire workers and for “rigid” restrictions on “business administration of enterprises,” and concludes that “we doubt whether it is necessary to carry out such significant changes.”

## **Why the Opposition?**

The extraordinarily rapid growth of the Chinese economy has depended a great deal on foreign corporations. According to Morgan Stanley’s chief economist Stephen Roach, 65% of the tripling of Chinese exports—from \$121 billion in 1994 to \$365 billion in mid-2003—is “traceable to outsourcing by Chinese subsidiaries of multinational corporations and joint ventures.”<sup>1</sup> The export surge blamed on China is primarily an export surge of global corporations using low-wage Chinese workers. Foreign corporations thus fear that the law protecting Chinese workers may eliminate their cheap labor costs.

Foreign corporations have another, less obvious, motive for opposing protections for Chinese workers. The ability to hire cheap labor in China has put downward pressure on wages and workers' conditions around the globe. China plays a key role in setting global wage norms. It is the linchpin of what Morgan Stanley chief economist Stephen Roach has called "[global labor arbitrage](#)" in which corporations move from one labor market to another to take advantage of cheaper labor. The result is a global "race to the bottom" in which workers and their communities are put into competition with each other to see who can provide the lowest-cost labor and the most corporate-friendly conditions. According to Roach, this global labor arbitrage is also now acting as "a powerful structural depressant on traditional sources of job creation in high-wage countries such as the United States."[2](#)

China's downward pressure on the world's wages is enormous. Harvard economist Richard Freeman estimates that the entry of India, Russia, and China into the world economy in the past few decades has doubled the workforce employed in the global economy. China alone accounts for 50% of this increase. And because these countries did not add significant capital to the global economy, more workers are competing to be employed by essentially the same amount of capital. This unbalanced equation has [increased](#) the bargaining power of capital, decreased that of labor, and substantially contributed to wage stagnation or decline in countries around the world. Chairman Ben Bernanke of the Federal Reserve Bank recently stated that the rapid integration of China, India, and the former Communist bloc into the world's economy in the space of a just a couple of decades has "no historical antecedents."[3](#)

Andrew Ross of New York University, who recently spent a year in China studying how workers are coping with the rapid changes of the last decade, notes that foreign corporations can use the wages and working conditions in their Chinese operations to drive down labor conditions for workers at all levels worldwide:

No industrializing country has been able to compete for the top-end slot at the same time as it absorbs jobs lower down the production chain ... To command this spread—from the lowest assembly platform work to the upper reaches of industry and services—is to be in a position to set the global norm for employee standards as never before. Given the chronic disregard for job security and workplace rights in China's foreign-invested private sector, such a norm is a clear threat to the stability of livelihoods everywhere.[4](#)

## **U.S. Responses**

The exposure of the role of U.S.-based businesses in trying to block new rights for Chinese workers—in a [report](#) by Global Labor Strategies—has struck a responsive chord. A front-page article in *The New York Times*, drawing largely on the report, triggered a widespread discussion in the media, on blogs, and throughout the labor movement.

Members of the U.S. Congress quickly stepped forward to address the concerns raised by the report. U.S. Representatives Lynn Woolsey (D-CA), Barbara Lee (D-CA), George Miller (D-CA), Barney Frank (D-MA), and 23 other House members sent a letter to President Bush "protesting the efforts of U.S. corporations to undermine the most basic human rights of Chinese

workers and block proposed new worker rights and labor standards protections in the proposed new Chinese labor law.”

According to Lynn Woolsey, “We are appalled that the American Chamber of Commerce in China and some of America’s most-prestigious, brand-name corporations are leading efforts inside China to weaken, if not block altogether, significant worker rights and protection provisions in the proposed Chinese labor law. This shameful lobbying campaign is totally inconsistent with our country’s long-standing commitment to promote respect for fundamental worker rights in law and practice everywhere. It is challenging enough for hard-working Americans to compete in the new global economy without having U.S. corporate leaders seeking to play them off against the least-protected and lowest-wage workers in the world.”

Specifically, the congressional letter calls upon President Bush to instruct the U.S. ambassador in China and the U.S. Trade Representative to deliver letters to Chinese government officials in support of worker rights and protection provisions in the Draft Labor Contract Law; repudiate the efforts of any U.S.-based corporations and their representatives doing business in China to weaken such provisions; and urge pertinent U.S.-based corporations and their representatives doing business in China to reverse their opposition and make clear their commitment to the universal rights of all Chinese workers and to improve their working conditions and living standards.

Both major U.S. trade union federations, the AFL-CIO and Change to Win, are planning to make the opposition of U.S. corporations to expanded rights for Chinese workers a significant focus of attention in upcoming political battles over the response to globalization.

## **Linking Workers**

The spread of globalization brought U.S. companies to China. The media has often focused on how the Chinese government was suppressing workers’ struggles and not enforcing existing labor law. But in a globalized world, the Chinese government is no longer the only or even the major actor in this regard. Global corporations or their subsidiaries and suppliers are exploiting millions of Chinese workers. Indeed, nearly two-thirds of the increase in “Chinese” exports actually represents non-Chinese corporations and their subsidiaries and suppliers.

Public policy in the United States and other countries has allowed these corporations to realize immense benefits from the low pay and poor conditions under which their Chinese workers work. These policies have been justified largely on the grounds that foreign corporations operating in China would elevate labor and human rights standards.

But these corporations have not raised the standards. And it is, ironically, the Chinese government that now wants to improve the situation, albeit in incremental ways. By opposing a labor contract reform law that would elevate labor and human rights standards, American and other foreign corporations are aggravating the very conditions they claimed they would ameliorate. Their campaign against the law blocks protections for Chinese workers and continues protections for corporations that would exploit them.

China's new labor bill faces a third reading this fall. If passed, it will come into [full effect](#) in March 2007. U.S., European, and other global corporations have already weighed in on the bill. They want it gutted.

Corporations and business organizations in China, and their political allies, should hold to their original promises to improve the conditions for Chinese workers. They should immediately reverse their opposition to the draft labor code and publicly support further legislation to ensure the basic human right of Chinese workers to organize, choose their own leaders, bargain collectively, and strike.

Here is an issue that links the interests of workers not only in the United States and China but everywhere. Higher wages, better working conditions, and the right to organize independent unions help workers everywhere to draw a line against the race to the bottom.

There is no need to travel to Beijing to fight for the rights of Chinese workers. The headquarters of the corporations opposing reforms for Chinese workers are in New York and Brussels, Los Angeles and London, and other cities and towns around the world. Washington, too, must make a choice. Will it support the rights of workers in China or the profits of U.S. corporations?

## End Notes

1. Stephen Roach, "How Global Labor Arbitrage Will Shape the World Economy," *Global Agenda*, 2005 Edition.
2. Stephen Roach, "False Recovery," *Global Economic Forum*, Morgan Stanley, January 1, 2004.
3. Krishna Guha, "Bernanke Calls for Fairer Globalization," *Financial Times*, August 25, 2006.
4. Andrew Ross, "A Fast Boat to China," delivered at the Cornell Global Labor Conference on February 10, 2006. Ross is author of the book *A Fast Boat to China: Corporate Flight and the Consequences of Free Trade; Lessons from Shanghai*, (Pantheon, 2006).

Tim Costello, Brendan Smith, and Jeremy Brecher wrote the report Behind the Great Wall of China for *Global Labor Strategies* (<http://www.laborstrategies.org/index.php?>).

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: Brad

Last Name: Sawatzky

Mailing Address: 704 Prescott Circle

City: Newport News

Country: United States

State or Province: VA

ZIP/Postal Code: 23602

Email Address:

Organization Name:

Comment: I have seen recent articles saying that the FCC is looking at a rule that would require manufacturers to cryptographically lock down computing devices if they contain a wireless radio.

Such a proposal is insane, and deeply out of touch with the reality of modern hardware.

Hardware manufacturers have an appalling track record of maintaining and updating such devices. Fortunately, Open Source software is used in the majority of consumer wireless devices produced today, and allow users the option of having these issues corrected outside the (generally non-existent) 'official' process.

Hardware manufacturers really suck at writing their firmware in the first place. A very large fraction of severe bugs / security holes identified in consumer devices are identified by external researchers that need the ability to investigate and modify their devices. This includes software wireless drivers on desktop hardware, laptops, cell phones, wifi-basestations, electronic voting machines, etc... The list is endless.

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. Do not shut this down for under some illusion that locking down the firmware to prevent external attacks is somehow less damaging than the crap baked into the firmware by the companies themselves.

-- Dr. Brad Sawatzky

I have seen recent articles saying that the FCC is looking at a rule that would require manufacturers to cryptographically lock down computing devices if they contain a wireless radio.

Such a proposal is insane, and deeply out of touch with the reality of modern hardware.

Hardware manufacturers have an appalling track record of maintaining and updating such devices. Fortunately, Open Source software is used in the majority of consumer wireless devices produced today, and allow users the option of having these issues corrected outside the (generally non-existent) 'official' process.

Hardware manufacturers really suck at writing their firmware in the first place. A very large fraction of severe bugs / security holes identified in consumer devices are identified by external researchers that need the ability to investigate and modify their devices. This includes software wireless drivers on desktop hardware, laptops, cell phones, wifi-

basestations, electronic voting machines, etc... The list is endless.

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. Do not shut this down for under some illusion that locking down the firmware to prevent external attacks is somehow less damaging than the crap baked into the firmware by the companies themselves.

-- Dr. Brad Sawatzky

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: David

Last Name: Noonan

Mailing Address: 2360 Saxony Trce

City: Alpharetta

Country: United States

State or Province: GA

ZIP/Postal Code: 30005

Email Address:

Organization Name:

Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This has the effect of creating an artificial monopoly and taking choice away from the consumer.

The result of these rules would a dramatic decrease in the security of wireless network equipment as as wireless research depends on the ability of researchers to investigate and modify their devices.

Further, manufacturers often have little incentive to fix security holes and these rules would prevent Americans from fixing the holes themselves. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

These rules are badly misguided, will not benefit anyone, and will do measurable harm. Please DO NOT limit the ability of Americans to run software of their own choice on the hardware that they purchase.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This has the effect of creating an artificial monopoly and taking choice away from the consumer.

The result of these rules would a dramatic decrease in the security of wireless network equipment as as wireless research depends on the ability of researchers to investigate and modify their devices.

Further, manufacturers often have little incentive to fix security holes and these rules would prevent Americans from fixing the holes themselves. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Not fixing security holes either feeds cyberthreats or increases electronic waste.

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

These rules are badly misguided, will not benefit anyone, and will do measurable harm. Please DO NOT limit the ability of Americans to run software of their own choice on the hardware that they purchase.

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: Carlyn

Last Name: Maw

Mailing Address: 10526 Venice Blvd

City: Culver City

Country: United States

State or Province: CA

ZIP/Postal Code: 90232

Email Address:

Organization Name:

Comment: As a product designer and teacher, the ability to modify, dissect, explore and change off the shelf devices is vital to my work.

I understand the concerns about security and protecting the vulnerable, but the proposed rules will encourage ignorance and laziness. I refuse to believe that this is the real American way.

Ignorance because being able to "open the hood" on the items we have in our homes is a vital learning tool. Is cyber security a real problem? Yes. Is security through obscurity a real solution? No. Is preventing people who are better at security than the original designers from contributing solutions? Absolutely not.

Laziness, because that which can't be examined, gets sloppy. Humans are lazy, it is part of our charm. We come up with the cunning devices to save ourselves work. When under the gun, we perform to metrics. Sadly the majority of "The Market" doesn't understand what they are purchasing. If the devices become completely sealed, there will be nobody looking. When executives who have financial metrics as their highest calling are making decision about selling to people who don't really understand technology, sloppy decisions will be made. They have to be. Shipping a "good enough" product has to happen sometimes for a company to survive. I understand the desire to not be embarrassed, but that doesn't unhack the baby-monitor.

The proposed rules would make the burgeoning internet of things not safer, but a security nightmare that could never be fully trusted. The nefarious and malignant will continue to be nefarious and malignant. With a nice law-abiding ignorant user-base to toy with handily secured, these regulations will give them plenty to be happy about.

As a product designer and teacher, the ability to modify, dissect, explore and change off the shelf devices is vital to my work.

I understand the concerns about security and protecting the vulnerable, but the proposed rules will encourage ignorance and laziness. I refuse to believe that this is the real American way.

Ignorance because being able to "open the hood" on the items we have in our homes is a vital learning tool. Is cyber security a real problem? Yes. Is security through obscurity a real solution? No. Is preventing people who are better at

security than the original designers from contributing solutions? Absolutely not.

Laziness, because that which can't be examined, gets sloppy. Humans are lazy, it is part of our charm. We come up with the cunning devices to save ourselves work. When under the gun, we perform to metrics. Sadly the majority of "The Market" doesn't understand what they are purchasing. If the devices become completely sealed, there will be nobody looking. When executives who have financial metrics as their highest calling are making decision about selling to people who don't really understand technology, sloppy decisions will be made. They have to be. Shipping a "good enough" product has to happen sometimes for a company to survive. I understand the desire to not be embarrassed, but that doesn't unhack the baby-monitor.

The proposed rules would make the burgeoning internet of things not safer, but a security nightmare that could never be fully trusted. The nefarious and malignant will continue to be nefarious and malignant. With a nice law-abiding ignorant user-base to toy with handily secured, these regulations will give them plenty to be happy about.

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: Stephen

Last Name: Sewall

Mailing Address: 4302 Hackney Coach Lane

City: Fairfax

Country: United States

State or Province: VA

ZIP/Postal Code: 22030

Email Address: drevilkep@hotmail.com

Organization Name:

Comment: I respectfully ask that the FCC does not implement rules that take away the freedom of Americans to modify or fix their computing devices. Doing so would have unintended consequences such as:

- Preventing the ability to fix, patch, or secure devices that the manufacturer no longer supports. This could have lasting security implications as many of these devices are used far longer than their support windows. There is a rich history of individual users finding and fixing serious security holes in their electronic devices.
- Wireless research needs unrestricted access to software radios. If the ability to create or modify firmware requires complicated regulatory paperwork, this will shut out hobbyists and small businesses. This will setback innovation in America and allow entrenched companies that already have access to develop firmware to stifle innovation.
- There is a multi-billion dollar industry that depends on the ability to modify firmware for electronic devices. Restricting this ability could affect this industry and cost Americans their jobs.

I respectfully ask that the FCC does not implement rules that take away the freedom of Americans to modify or fix their computing devices. Doing so would have unintended consequences such as:

- Preventing the ability to fix, patch, or secure devices that the manufacturer no longer supports. This could have lasting security implications as many of these devices are used far longer than their support windows. There is a rich history of individual users finding and fixing serious security holes in their electronic devices.
- Wireless research needs unrestricted access to software radios. If the ability to create or modify firmware requires complicated regulatory paperwork, this will shut out hobbyists and small businesses. This will setback innovation in America and allow entrenched companies that already have access to develop firmware to stifle innovation.
- There is a multi-billion dollar industry that depends on the ability to modify firmware for electronic devices. Restricting this ability could affect this industry and cost Americans their jobs.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Richard

Last Name: Sanders

Mailing Address: 305 Brookhaven Ave Ne, Apt 429

City: Atlanta

Country: United States

State or Province: GA

ZIP/Postal Code: 30319

Email Address: richard.sandes@usdoj.gov

Organization Name:

Comment: As a security researcher, being able to use open source or other firmware/software on WiFi devices is of great importance. This is why I am asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Additional points of emphasis you should consider adding:

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

As a security researcher, being able to use open source or other firmware/software on WiFi devices is of great importance. This is why I am asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Additional points of emphasis you should consider adding:

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

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: Shane

Last Name: Caldwell

Mailing Address: 5673 Yaupon Holly Dr

City: Cocoa

Country: United States

State or Province: FL

ZIP/Postal Code: 32927

Email Address:

Organization Name: New College of Florida

Comment: These restrictions could easily harm innovation by making it harder for researcher's to experiment with modified firmware, as well as quelling the curiosity of interested citizens.

While in theory keeping people safe is a worthy goal, it might not be worth the cost.

These restrictions could easily harm innovation by making it harder for researcher's to experiment with modified firmware, as well as quelling the curiosity of interested citizens.

While in theory keeping people safe is a worthy goal, it might not be worth the cost.

Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Aaron

Last Name: Gray

Mailing Address: 7415 Suburbia Drive

City: Pine Bluff

Country: United States

State or Province: AR

ZIP/Postal Code: 71603

Email Address:

Organization Name:

Comment: Respectfully,

Our company, Tech Friends, Inc., provides services to correctional institutions around the nation. Obviously, security in these institutions is of paramount concern. For that reason, we utilize a custom firmware for routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

Aaron Gray  
Accounting Technician  
Tech Friends, Inc.  
870.933.6386

Respectfully,

Our company, Tech Friends, Inc., provides services to correctional institutions around the nation. Obviously, security in these institutions is of paramount concern. For that reason, we utilize a custom firmware for routers based on OpenWRT. The proposed rule would prohibit our ability to install customized security firmware on commercial router hardware. This would be catastrophic for our business interests and for the security of correctional facilities around the

nation.

It is essential that businesses and individuals have the freedom to install custom firmware on routers.

We urgently ask you to reconsider this portion of the rule to ensure that innovation, security, and flexibility remain an integral part of the network ecosystem.

Aaron Gray  
Accounting Technician  
Tech Friends, Inc.  
870.933.6386

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: Chris

Last Name: Turner

Mailing Address: 2324 Stratford Dr

City: Mesquite

Country: United States

State or Province: TX

ZIP/Postal Code: 75150

Email Address: cyberstick@gmail.com

Organization Name:

Comment: This seems overreaching and is an anti-consumer move, people that own their hardware have a right to do whatever they want to it as long as they stay within the confines of existing law.

Honestly I'd be more concerned with the scores of people that can get/use part 90 equipment without being asked for a copy of a license.

This seems overreaching and is an anti-consumer move, people that own their hardware have a right to do whatever they want to it as long as they stay within the confines of existing law.

Honestly I'd be more concerned with the scores of people that can get/use part 90 equipment without being asked for a copy of a license.