

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: Pratt

Mailing Address: 145 E 1100 N

City: Bountiful

Country: United States

State or Province: UT

ZIP/Postal Code: 84010

Email Address: null

Organization Name: null

Comment: I have read that this particular rule contains language that would effectively remove the ability of individuals and businesses to modify the firmware of, among other things, wifi-providing routers and hotspots.

I personally use OpenWRT to manage my home wifi, the router in its default settings doesn't allow several features which are available with the custom firmware, including:

-the ability to change the router from a 'master' to 'slave' configuration, or 'primary wifi' to 'repeater' if you prefer, from the laptop, with no reset required. I use this often as we set up the router in multiple homes and need to change it from one to the other.

-the ability to choose my own passwords without the restrictions built-in to the router's default programming

-using the router's hardware in ways the manufacturer didn't include in their firmware, such as reports on signal strength, real-time connected users' bandwidth usage, limitations of space and times the wifi is available (essentially personalized parental controls) all automated once set up.

I think that despite the number of products on the market, there are always features that creative people will find ways to implement, and the option to customize electronics provides a great platform for researching new tech, and teaching the principles to others.

On the other side of the supply chain, manufacturers don't always get the intended features working properly either. By allowing users to install firmware that works great over top of bug-ridden or poorly-secured firmware, businesses and individuals can customize their own security, and use great hardware in models that fall short in programming.

In short, I believe the proposed rules would lead to a lower quality product being available, reduce fair competition and stifle motivation to innovate and produce quality parts, and open up serious security holes in wifi-management generally.

Please consider these potential consequences, and choose to promote, rather than prohibit, the contributions of capable programmers who have done so much to provide an awesome alternative!

Sincerely,

Andrew "home user" Pratt

I have read that this particular rule contains language that would effectively remove the ability of individuals and businesses to modify the firmware of, among other things, wifi-providing routers and hotspots.

I personally use OpenWRT to manage my home wifi, the router in its default settings doesn't allow several features which are available with the custom firmware, including:

-the ability to change the router from a 'master' to 'slave' configuration, or 'primary wifi' to 'repeater' if you prefer, from the laptop, with no reset required. I use this often as we set up the router in multiple homes and need to change it from one to the other.

-the ability to choose my own passwords without the restrictions built-in to the router's default programming

-using the router's hardware in ways the manufacturer didn't include in their firmware, such as reports on signal strength, real-time connected users' bandwidth usage, limitations of space and times the wifi is available (essentially personalized parental controls) all automated once set up.

I think that despite the number of products on the market, there are always features that creative people will find ways to implement, and the option to customize electronics provides a great platform for researching new tech, and teaching the principles to others.

On the other side of the supply chain, manufacturers don't always get the intended features working properly either. By allowing users to install firmware that works great over top of bug-ridden or poorly-secured firmware, businesses and individuals can customize their own security, and use great hardware in models that fall short in programming.

In short, I believe the proposed rules would lead to a lower quality product being available, reduce fair competition and stifle motivation to innovate and produce quality parts, and open up serious security holes in wifi-management generally.

Please consider these potential consequences, and choose to promote, rather than prohibit, the contributions of capable programmers who have done so much to provide an awesome alternative!

Sincerely,

Andrew "home user" Pratt