Please Do Not Reply To This Email.

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

Title: Equipment Authorization and Electronic Labeling for Wireless Devices

FR Document Number: 2015-18402

RIN:

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

Submitter Info:

First Name: Daniel

Last Name: Osborne

Mailing Address: 2200 Juliesse Ave

City: Sacramento

Country: United States

State or Province: CA

ZIP/Postal Code: 95821

Email Address: fcc@danielosborne.net

Organization Name:

Comment: I would like to ask that the FCC not implement rules that will take away (remove) the ability for users to install the software of our choosing on our computing devices.

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

As is more frequently the case as devices age, Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Just because the manufacturer no longer releases updates, doesn't mean the device is no longer functional. If that were the case, we would need to buy a new vehicle every two years, and throw away the old one.

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.

If the ability to enforce FCC requirements for wireless devices has been problematic in the past, a proper solution is instead to force those parameters to be permanently burned into the actual wireless device, not restricting all software. For example, the allowed frequencies, or max transmission power, can be burned into a non-programmable region. This would prevent future software updates from ever changing those parameters again.

I would like to ask that the FCC not implement rules that will take away (remove) the ability for users to install the software of our choosing on our computing devices.

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

As is more frequently the case as devices age, Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Just because the manufacturer no longer releases updates, doesn't mean the device is no longer functional. If that were the case, we would need to buy a new vehicle every two years, and throw away the old one.

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.

If the ability to enforce FCC requirements for wireless devices has been problematic in the past, a proper solution is instead to force those parameters to be permanently burned into the actual wireless device, not restricting all software. For example, the allowed frequencies, or max transmission power, can be burned into a non-programmable region. This would prevent future software updates from ever changing those parameters agai