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: Ezra

Last Name: Teboul

Mailing Address: 6242 hallgarten hall

City: hanover

Country: United States

State or Province: NH

ZIP/Postal Code: 03755

Email Address: ezra.j.teboul.gr@dartmouth.edu

Organization Name:

Comment: To my understanding, the FCC is considering " proposed rules (ET Docket No. 15-170) that will require device makers with WiFi and other Radio Frequency (RF) devices to cryptographically lock down the RF-controlling software on those devices so as to prevent users from installing the software of their choice. This means not only routers, but also many phones, tablets, laptops, and any number of new devices that are wifi capable would now be required to implement a low level DRM system that prevents users from re-flashing or modifying the operating system and/or firmware on those devices." (source: https://libreplanet.org/wiki/Save_WiFi)

if this statement is accurate, I'd like to encourage you to do the exact opposite.

In my own field of research (history of music technology) more than two thirds of major technological breakthroughs can be traced back to amateurs and professionals in the field of RF electronics design and manufacture. Without post-WW2 kits, army radio operator dads and HAM radio sheds, electronic music

today would be a very different field. This is still true today with digital technology: most innovations in audio signal processing are directly related to communications an transmission research. My point is that allowing the general public to experiment within reason with consumer level technology isn't simply fun, it is incredibly productive, leading to invention in both the arts and the sciences. These innovations have overwhelmingly occurred to no negative consequence for anyone, except the occasional aesthetic divergence at thanksgiving dinner tables (yes, synthesizers are real instruments! I promise). The more people know about everyday technology, the better they use it and the more interesting things happen.

Music technology happens to be my field of expertise, but I see many other reasons why rather than locking down on technologies, both public and private entities would benefit from increased abilities to fine-tune the radio-able hardware and software we use everyday in the western world. Rather than imposing DRM on radio software, requiring educational programs to include information on best practices in communication technology (analog and digital) would allow us to better understand the technology we rely on everyday (wifi and cellphones), resulting in better use, more efficient research, resulting in better devices and happier customers. People would be better able to understand and appreciate the FCC's purpose and how it affects their daily lives, and in return, respect its expertise. Understanding what kind of modifications are harmful and why is a more effective deterrent than DRM.

On a more basic level, it is the user's right to modify and use equipment the user owns, within safe limits. This philosophy has allowed HAM operators to communicate freely for decades, allowing thousands to learn about electronics and communication without bothering anyone and occasionally, helping authorities in emergency situations. Wireless networking research depends on the ability of researchers to investigate and modify their devices (implementing the rule described above would mean terminating this research, or implementing an exceptional authorization process). Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so (implementing an exceptional authorization process at this level would be absurd and unconstitutional). 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.

To my understanding, the FCC is considering " proposed rules (ET Docket No. 15-170) that will require device makers with WiFi and other Radio Frequency (RF) devices to cryptographically lock down the RF-controlling software on those devices so as to prevent users from installing the software of their choice. This means not only routers, but also many phones, tablets, laptops, and any number of new devices that are wifi capable would now be required to implement a low level DRM system that prevents users from re-flashing or modifying the operating system and/or firmware on those devices." (source: https://libreplanet.org/wiki/Save_WiFi)

if this statement is accurate, I'd like to encourage you to do the exact opposite.

In my own field of research (history of music technology) more than two thirds of major technological breakthroughs can be traced back to amateurs and professionals in the field of RF electronics design and manufacture. Without post-WW2 kits, army radio operator dads and HAM radio sheds, electronic music today would be a very different field. This is still true today with digital technology: most innovations in audio signal processing are directly related to communications an transmission research. My point is that allowing the general public to experiment within reason with consumer level technology isn't simply fun, it is incredibly productive, leading to invention in both the arts and the sciences. These innovations have overwhelmingly occurred to no negative consequence for anyone, except the occasional aesthetic divergence at thanksgiving dinner tables (yes, synthesizers are real instruments! I promise). The more people know about everyday technology, the better they use it and the more interesting things happen.

Music technology happens to be my field of expertise, but I see many other reasons why rather than locking down on technologies, both public and private entities would benefit from increased abilities to fine-tune the radio-able hardware and software we use everyday in the western world. Rather than imposing DRM on radio software, requiring educational programs to include information on best practices in communication technology (analog and digital) would allow us to better understand the technology we rely on everyday (wifi and cellphones), resulting in better use, more efficient research, resulting in better devices and happier customers. People would be better able to understand and appreciate the FCC's purpose and how it affects their daily lives, and in return, respect its expertise. Understanding what kind of modifications are harmful and why is a more effective deterrent than DRM.

On a more basic level, it is the user's right to modify and use equipment the user owns, within safe limits. This philosophy has allowed HAM operators to communicate freely for decades, allowing thousands to learn about electronics and communication without bothering anyone and occasionally, helping authorities in emergency situations. Wireless networking research depends on the ability of researchers to investigate and modify their devices (implementing the rule described above would mean terminating this research, or implementing an exceptional authorization process). Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so (implementing an exceptional authorization process at this level would be absurd and unconstitutional). 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.