

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

Specifically there are three changes in the NPRM of concern:

2. 1033 Application for grant of certification. Paragraph 4(i),
2. 935 Electronic labeling of radio frequency 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.

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.

Innovation in network and wireless technology depends on the ability of users and resellers to experiment with software and hardware at the deepest levels. There are many examples where the manufacturers of devices shipped devices with security and performance flaws, then immediately or after a very short time abandoned all support, upgrade, or bug fixes of the software. Also, many devices can be deployed in innovative ways not thought of by the manufacturer but developed and implemented by the owners of the device after purchase.

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. 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.

These recommendations will help to improve the NPRM:

The regulations on software defined radios should not restrict the ability to replace software on computing devices in any way. Responsibility for the device to continue to meet FCC regulations and standards, as well as local, state and federal laws is the sole responsibility of the person or company that replaced the software. 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, and modify in

60001324433.txt

whole or part the software on the devices they own.

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

I 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.

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