

1612 Bellechasse Dr.
Raleigh NC 27615
September 2, 2015

Received & Inspected

SEP 08 2015

FCC Mail Room

Brian Butler
Office of Engineering and Technology
Room 7-A267
445 12th Street SW
Washington, DC 20554

Re: ET Docket No. 15-170; RM-11673

NOT TO BE COPIED ORIGINAL

Dear Mr. Butler:

I am motivated to make my first comment on a proposed federal rule after reading some of the comments about the one cited above by notable organizations in the free software and open source software community. Some of the language below is adapted from comments by others.

Why do I care? I have a Ph.D. in Computer Science, and these proposed rules adversely affect my ability to do research, my ability to keep my equipment secure, and the ability of the U.S. military and other U.S. Government agencies to keep their equipment secure. I urge the rejection of the proposed rule cited above.

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the user's needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for the U.S. military, U.S. government, and large companies, security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, the U.S. government will be put at risk of espionage and large American companies will be put at risk of industrial espionage.

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. Without the ability to change the software on the device, any number of innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Sincerely,



Frank Anderson Smith, Ph.D.

No. of Copies rec'd 0
List ABCDE