Sudomesh recognizes that, although NPRM 15-92 may be motivated by genuine concerns, its implementation would have broad negative consequences, including hindering the charitable efforts of our organization and others like it. While this NPRM may address important aspects of the FCC's duty to protect the spectrum, it does so at the expense of other, equally important aspects of the FCC's mission, such as supporting innovation and providing broadband services. A more nuanced approach is needed.

Sudo mesh is a project that shares many goals with the FCC itself. We are building a community-maintained wireless network in Oakland, California; as our network is built out, it will bring inexpensive Internet to numerous citizens, provide opportunities for many individuals and organizations to develop innovative network-based projects, and support public safety as a redundant network service in case of Internet failure.

But if put into effect, portions of this NPRM would render unlawful our core activities, and the associated public benefits we anticipate.

Our purpose in creating this network is multi-faceted, and aligns strongly with the FCC's own mission:

- Our network offers an affordable alternative to broadband Internet in Oakland.
- Since residents of Oakland can engage in building the technical and social infrastructure of our project, Sudomesh actively promotes the innovation called for in the FCC's mission.
- Mesh networks like ours (when more complete) can offer a resilient network that can be an important alternative to centrally-controlled telecom services. During Superstorm Sandy, infrastructure similar to what we are building was useful to communities in Brooklyn, which were able to stay in touch when Internet and telephone services failed.

~~The FCC's mission to "make available so far as possible, to all the people of the United States, without discrimination ... rapid, efficient, Nationwide, and world-wide wire and radio communication services with adequate facilities at reasonable charges" resonates strongly (...)~~

Sudomesh is currently developing firmware based on OpenWRT for commercially available off-the-shelf wireless devices which can be used to deploy mesh networks using an experimental Internet routing protocol called Babel.

The proposed rules, specifically in paragraphs 4(i) and 8(e), require that manufacturers lock their devices so as to prevent unauthorized software from controlling certain radio parameters. These rules, in turn, stifle innovation, hinder learning, and introduce risks similar to those seen by other strictly closed source and proprietary technologies that community oversight and common ownership. The resulting unknown backdoors into home and community radio networks pose far more intimate risks than those posed by technologies like Flash or Windows XP. Networks and backup networks need to be remain available and uncompromised because they facilitate more functions of infrastructure and have access to most network devices. In addition, the software "must not allow the installers or end-users to operate the transmitter with

operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved." Insights from those who are not formally “authorized” are often what keeps things working; a great deal of high quality networking infrastructure in the modern era would not exist if not for open, collaborative efforts. In many cases, the authors and innovators of unauthorized software are end-users.

Although the NPRM does not specify the reason for the proposed rule-making, it is widely believed that the FCC is acting on behalf of other users of the U-NII bands, and specifically terminal Doppler weather radar (TDWR). Although U-NII devices are required to employ dynamic frequency selection (DFS) to avoid radar operating on these bands, the architecture of modern 802.11 transceivers is such that almost all time-insensitive functions are handled in software, including DFS, and can be disabled if the user has full control of their device.

To better grasp the scope of this issue, consider that the user of almost every WiFi-enabled computer running an open source operating system can, in theory, perform this modification. The NPRM goes on to stipulate means for preventing such modifications "including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device[...]." This would amount to a form of digital rights management (DRM), and would render unlawful the use of any third party software with low-level access to radio parameters.

But software control of these radio parameters has been used in creative and beneficial ways, which are only now beginning to be exploited. There are active open source projects which have brought innovations such as polling/time-division multiple access algorithms for channel management, improved link negotiation for long point-to-point links, better security, the ability to deploy highly redundant mesh networks quickly (for example 802.11s), and many more. And we believe that we have only scratched the surface. In addition, given current prevalent hardware architectures it is not feasible to prevent access to only low-level radio parameters without also removing root-level access which inadvertently prevents a wide range of non-radio-related software modifications that fall outside of the scope of the regulatory mandate of the FCC.

Our position regarding this NPRM is that

(1) it would stifle the innovation which has been building around the use of high-bandwidth unlicensed wireless networking, ~~effectively~~ rendering projects such as ours and OpenWRT unlawful.

(2) there are ways to achieve the desired control of the U-NII bands in hardware, which would be specific to those bands; such an approach would address the spectrum issues that NPRM 15-92 aims to address, but is highly preferable because it would have fewer negative impacts on areas like innovation and public safety

(3) these rules would leave innovation in the wireless world to the large companies which can afford the development and certification process required; that would be irresponsible and inefficient.

Comments from Joshua Gay, Free Software Foundation (and author of the LibrePlanet letter linked below), 10/9/15:

> You should be quoting exact sentences of the proposed rules you are opposing. You mention UNII bands, but those are not covered by this NPRM specifically. You should state that the UNII rules passed in 2014 (cited) were required to go into effect in June 2015 on new equipment and in July 2016 for old equipment (you should double check dates/phrasing) and that these UNII rules are already leading mabufacturers to lock down all software on the system and not only the software that specifically controls the radio. Point out that the NPRM in question updates equipment authorization using the same software protection strategies used in the UNII rules already passed. Yet the commission has not ....

Used the opportunity to actually check on industries response to those UNII updates. This is irresponsible and already hindering innovation, creating vendor lockin, and denying users freedom and control. The Commission has not even taken the time to see the damage they have done with the more narrow application of the rules before going ahead and applying those pronciples to these more general equipment authorization rules that will effect many classes of devices in a variety of form factors.

Emphasize that the Commission is naive if they believe locking down only the radio software will not result in hardware sellers locking down other system software as well. It will have this result and the UNII rule updates in 2014 which are just going into effect now prove this point as increasingly sellers of wireless routers/access points do not know how to comply with those rules without a system wide lockdown. Some don't care because it doesnt hurt their profits, it in fact may help them to be able to sell more devices without having to worry about providing user instalable system updates. Now the same vendor lockin will inevitably happen if these proposed rules are passed, only it will be across many more kinds of electronic devices. Etc

Also, again, just make sure you specify why the exact language of this NPRM will deny your ability to modify software in ways that will prevent you from doing the things you want to do. The reply comments are going to focus on how the radio parameters and radio software can be locked down to only function according to FCC rules. You need to show that you are not advocating running software that would have the radio operate outside of the rules, but that the lockdowns are (from 2014 UNII updates) already beginning to prevent innovation on manybaccess points and will (with this NPRN) begin preventing mesh innovation on even more kinds of wireless devices because they prevent modifying software that is intimately and inextricably coupled with the software that directly controls the radio.

PETE: Is signing multiple letters detrimental? We were wondering

> No
>
> It is common to endorse other comments when doing your own comment and so it is fine signing others

I know other orgs who will be signing multiple different comments ... So if I am wrong, a lot of us will be in the same boat smile emoticon

I got word that the software freedom law center intends to sign and submit their own. They are pretty good when it comes to regulatory matters

Security Link Dumps:

Security:

- http://readwrite.com/2013/04/16/beware-the-wireless-router-security-threat
- http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/
    - The report, written by research firm Independent Security Evaluators of Baltimore, found that 13 of the most popular off-the-shelf wireless routers could be exploited by a "moderately skilled adversary with LAN or WLAN access."
    - In 2011, one firmware vulnerability affecting six hardware manufacturers combined with two malicious scripts and 40 malicious DNS servers to attack 4.5 million Brazilian DSL modems, with the goal of stealing bank and credit card information.
    - Meanwhile, [Darren] Kitchen of Hak5 recommends that people make their own routers entirely. "The best that a person can do is to roll their own using the Marin, Ca.-based Untangle, which takes any spare PC and turns it into a wireless router." He also recommends Monowall and Smoothwall. Heffner at Tactical Network Solutions agreed. "The best thing you can do is install a third-party firmware, such as OpenWRT or Tomato," he said.
- http://securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php
- http://securityevaluators.com/knowledge/case_studies/routers/soho_service_hacks.php
- https://www.sohopelesslybroken.com/research.php
- https://www.sohopelesslybroken.com/news.php

Autonomy of local communities

- Meyer Memorial Trust (one of Oregon's largest foundations) supported a similar project: http://www.mmt.org/video/personal-telco-project and http://northportlandattorney.com/docs/sentinal200709.pdf and http://bojack.org/2008/06/portland_admits_it_blew_250k_o.html (Pete F cameo!) and http://www.wweek.com/portland/article-4273-mississippi_wi_fiing.html

Disaster recovery (Sandy and perhaps others?)

- GoTenna: http://www.bloomberg.com/news/2014-07-17/how-superstorm-sandy-gave-rise-to-wireless-startup.html

Other letters

CeroWRT letter (basically alternate FCC proposal)::
https://docs.google.com/document/d/1E1D1vWP9uA97Yj5UuBPZXuQEPHARp-AhRqUOeQB2WPk/edit?usp=sharing

LibrePlanet:
https://libreplanet.org/wiki/Save_WiFi/Joint_Letter

---------- brainstorm arguments

(X) Would inadvertently prevent innovation in realms beyond the scope of radio communications, leading to a stifling of innovation in such burgeoning areas as software defined networking and dynamic or “self-healing” network routing algorithms, especially relevant for the emerging market of so-called Internet of Things devices.

(X) Would inadvertently limit access to education by disallowing products made for educational purposes which provide low-level access as teaching aids for anyone from middle-schoolers to engineers in training. It is a long-standing truth that a substantial amount of the workforce within the IT and networking industry start out as self-taught amateurs by modifying and repurposing off-the-shelf and easily available computers and devices. These regulations would make such reprogrammable products much less accessible and for some types of products impossible altogether.

(X) Referring to the points made above, these regulations could put the United States at a global disadvantage with regards to innovation and education compared to countries that do not implement similar restrictions, which could lead to a long-term chronic competitive disadvantage in product development when compared to existing global leaders such as Japan and South Korea.


THE RED MENACE
IS REAL!
REPORT ALL SUSPECTED
COMMUNIST ACTIVITY!