

**Before the  
Federal Communications Commission  
Washington, DC 20554**

In the Matter of

Equipment Authorization and  
Electronic Labeling for Wireless  
Devices

ET Docket No. 15-170

**REPLY COMMENTS OF NEW AMERICA’S OPEN TECHNOLOGY  
INSTITUTE**

**I. The Proposed Rule Could Have Severe Negative Unintended  
Consequences and Would Not Adequately Address the Problem of  
Interference**

In initial comments, New America’s Open Technology Institute (“OTI”) argued that “the Commission risks creating a scenario where, to guarantee compliance, the manufacturers have the incentive to implement restrictive software-based solutions that preclude the kind of tinkering and innovating that generates enormous public interest benefits.”<sup>1</sup> It is clear, based on initial comments, that this is not an isolated concern—a large number of other commenters express related concerns. For example, commenters from the Department of Computer Science at the University of Colorado, Boulder argue that regardless of the rule’s intention, as written it would “likely be implemented as a general-purpose limit on all firmware modification

---

<sup>1</sup> Comments of New America’s Open Technology Institute, ET Docket No. 15-170, RM-11673 (Oct. 9, 2015), at 5 [hereinafter Comments of OTI].

as a matter of practicality or cost.”<sup>2</sup> According to group comments led by Vint Cerf, the rules would cause vendors to keep code secret and unmodifiable, which “could prevent anyone other than the original vendor from making modifications,” thus “locking in” problems contained on the original firmware and software.<sup>3</sup> The Center for Democracy & Technology concurs, noting that even though the proposed new certification rules are not designed with the intent of banning modification or installation of third-party or open-source firmware, “security researchers and others are understandably concerned that this will be its unintended effect. Even the Commission has acknowledged that locking down a router to prevent any modification would be an expedient way to comply with the rule.”<sup>4</sup> Beyond the potential for restrictions on end user or third-party modification in general, many commenters specifically cite the rule as a threat to open source.<sup>5</sup>

---

<sup>2</sup> Comments of Andy Saylor, Matt Monaco, and Dirk Grunwald, ET Docket No. 15-170, RM-11673 (October 9, 2015), 3 [hereinafter Comments of Saylor et al.].

<sup>3</sup> Comments of Vint Cerf et al., ET Docket No. 15-170, RM-11673 (October 9, 2015), at 3-4, 8 [hereinafter Comments of Cerf, et al.].

<sup>4</sup> Comments of the Center for Democracy & Technology, ET Docket No. 15-170, RM-11673 (October 9, 2015), 2 [hereinafter Comments of CDT].

<sup>5</sup> Comments of Google, Inc., ET Docket No. 15-170, RM-11673 (October 9, 2015), 7 [hereinafter Comments of Google] (“certain proposals to protect portions of the radio spectrum could hamper use of open source software to advance important objectives in the public interest”); *see also* Comments of CDT at 4; *see* Comments of Bruce Perens, ET Docket No. 15-170, RM-11673 (October 9, 2015), 1 [hereinafter Comments of Perens]; Comments of the Information Technology Industry Council, ET Docket No. 15-170, RM-11673 (October 9, 2015), 7 [hereinafter Comments of ITI].

The harms that commenters in this proceeding forecast as possible results of the proposed new certification requirements fall into three general categories:

- *Security*: If, in order to comply, vendors build in mechanisms to prevent end user modification or update of what is often buggy and insecure software,<sup>6</sup> commenters argue that this would harm cybersecurity.<sup>7</sup>
- *Functionality*: Blocking third-party updates would stop improvements that enhance functionality.<sup>8</sup>
- *Innovation and Development*: Limits imposed by the rule would obstruct research and development. This obstruction would occur with regard to both technical research,<sup>9</sup> and general innovation.<sup>10</sup>

---

<sup>6</sup> Comments of Cerf et al. at 11; Comments of Perens at 4-5; Comments of Google at 8; *Comments of Susan Sons*, ET Docket No. 15-170, RM-11673 (October 9, 2015), 3 [hereinafter Comments of Sons].

<sup>7</sup> Comments of Google at 8 (“The open source community and academics, among others, have stepped up to fill [routers’ security] gap. Using open source resources generated by these parties, Wi-Fi vendors have been able to improve their existing routers by flashing firmware on them”); Comments of Cerf et al. at 8; Comments of Sayler et al. at 2, 4; Comments of Consumer Electronics Association, ET Docket No. 15-170, RM-11673 (October 9, 2015), 15, [hereinafter Comments of CEA].

<sup>8</sup> Comments of Google at 8; Comments of Shure Incorporated, ET Docket No. 15-170, RM-11673 (October 9, 2015) at 6.

<sup>9</sup> Comments of the Boeing Company, ET Docket No. 15-170, RM-11673 (October 9, 2015), 8 (“[T]he NPRM appears to contemplate requiring restrictions on the modification of certified equipment by third parties, which could cause substantial disruption to research and development of wireless technologies”); Comments of the National Association for Amateur Radio, ET Docket No. 15-170, RM-11673 (October 9, 2015), 2.

<sup>10</sup> Comments of CEA at 12 (“[D]eveloping a new and secure method of distributing firmware updates to retail consumer devices would be expensive and would require significant phase-in time, thereby slowing the flow of innovative new products”); Comments of Cerf et al. at 1; Comments

Beyond the general benefits of modification and updates from either end users or third parties, the comments of Cert, et al. in particular note the importance of giving end users the power to examine systems, and verify their legitimacy, stating, “Only by having software systems be open, inspectable, and verifiable *by the owner of the equipment* can compliance be ensured.”<sup>11</sup> Highlighting the recent Volkswagen emissions scandal, this comment asserts that providing the end user with the capacity for inspection is the best way to ensure compliance with manufacturing requirements.<sup>12</sup>

A number of commenters also argue that the proposed new certification requirements would not prevent harmful interference from taking place or replace the need for effective enforcement. For example, Bruce Perens characterizes the proposed new certification requirements as “ubiquitous law enforcement” that would devote excess costs in an unnecessary attempt to “prevent law violation before the attempt,”<sup>13</sup> arguing that it would be more efficient and effective to find and cite violators.<sup>14</sup> The Telecommunications Industry Association contends that existing measures are sufficient.<sup>15</sup>

---

of SFLC at 7; Comments of Mozilla, ET Docket No. 15-170, RM-11673 (October 9, 2015), 5; Comments of Sayler at 2.

<sup>11</sup> Comments of Cerf et al. at 3 (emphasis in original).

<sup>12</sup> *Id.*

<sup>13</sup> Comments of Perens at 8.

<sup>14</sup> *Id.*

<sup>15</sup> Comments of the Telecommunications Industry Association, ET Docket No. 15-170, RM-11673 (October 9, 2015), 13-14 (“[T]he basic requirements for software security are already codified in various parts in the Commission’s regulations, specifically Part 2.944 (b), Part 15.15 (c) Part 15.202, and more recently in Part 15.407 of the rules; in addition there are requirements established in KDB 594280. The Commission’s proposal to the possible

Additionally, the University of Colorado commenters argue that the proposed rule is not guaranteed to accomplish its goal and prevent improper modifications.<sup>16</sup> OTI agrees with other commenters that the proposed new requirements will not be sufficient to prevent problematic interference, and that a focus on enforcement will ultimately prove more effective.<sup>17</sup>

## **II. The Commission Should Instead Focus on Responsive Measures that Mitigate Risk Without Causing Significant New Harms**

Rather than expanding certification requirements in ways that could encourage vendors to lock down firmware and middleware against all forms of modification and experimentation, the Commission should instead focus on responsive measures that will mitigate the concern at issue without causing the same problems. This would prevent overreach, a key consideration given the magnitude of potential harms of the proposed rule raised by many parties.

In particular, the Commission should devote resources to responsive actions recommended by numerous commenters:

---

elimination of the SDR certification process includes requiring the SDR software security process to apply to all wireless devices. TIA argues the rules as noted above already require manufacturers to include a statement in their approved equipment manuals warning that unauthorized changes could void the grant of certification, as well requirements established in the KDB 594280 that include specific information that must be part of the application process concerning the software security”).

<sup>16</sup> Comments of Saylor et al. at 5.

<sup>17</sup> See Comments of OTI at 8-9 (“Ex ante enforcement may allow the Commission to both mitigate the more egregious interference risks, without using additional prior restrictions that would hamstring innovation, and tie the hands of developers, researchers innovators, or other users of RF-Enabled devices.”).

- *Work with relevant communities to prevent improper use:* Multiple commenters suggest an alternate approach of working with communities that build and maintain RF-enabled device software to support regulatory compliance.<sup>18</sup>
- *Focus on enforcement against violators:* Many commenters support a focus on enforcement against violations as the most effective method,<sup>19</sup> including OTI.<sup>20</sup>

This approach will address anticipated problematic interference stemming from modification of approved software-defined radio devices, while also avoiding the harms associated with the proposed new certification requirements.

### **III. Any Rule Promulgated in this Proceeding Should Make Clear that It Does Not Prohibit Certain Important Activities**

If the Commission does choose to move forward with updated certification requirements similar to those proposed, it is important that application of the new policy only apply in a narrow manner that does not prevent legitimate activities with significant social utility. The Commission could best achieve the requisite clarity through a clear statement that the rule does not prohibit certain activities.

---

<sup>18</sup> Comments of CDT at 4; Comments of Sayler et al. at 7-8.

<sup>19</sup> Comments of Perens at 8 (“The commenter strongly advises FCC not to turn to embedded enforcement mechanisms as a substitute for finding and citing violators as FCC does today. Certainly the relatively minor offenses theorized in the rule-making text do not mandate it”); Comments of Mozilla at 5; Comments of Sayler et al. at 9.

<sup>20</sup> Comments of OTI at 7-8.

Consistent with the suggestions of several commenters, the Commission should provide a clear and formal statement that the proposed rule does *not* restrict certain activities, specifically to 1) use open source<sup>21</sup> and 2) upgrades or replacement of firmware.<sup>22</sup> The Commission should make a similar clarifying statement that its proposed rule only applies only to hardware.<sup>23</sup> These statements of clarification are not mutually exclusive. The Commission would best mitigate the risks previously described<sup>24</sup> by including statements on all these points in any preventative rule on software-defined radio.

### **Conclusion**

As indicated by the many initial comments filed in this docket, there is widespread concern regarding the potential harms that could stem from adoption of the proposed new certification requirements for software-defined radios. OTI appreciates the significant problems that could arise from inappropriate interference caused by modified devices; however, protection against these problems should not come at the expense of invaluable innovation in the wireless space. The Commission should carefully weigh the risks to future innovation and development in the myriad RF-enabled device markets with the modest risk of potential interference harms.

---

<sup>21</sup> Comments of ITI at 7; Comments of Cerf et al. at 13; Comments of Google at 22.

<sup>22</sup> Comments of Cerf et al. at 1; Comments of SFLC at 4.

<sup>23</sup> Comments of CEA at 12; Comments of ITI at 7; Comments of OTI at 7.

<sup>24</sup> *See supra*, Sec. I.

We appreciate the Commission's efforts and attention to these concerns, and look forward to continued collaboration on this issue to support use of communications technologies.

Respectfully submitted,

/s/

Jake Laparruque, Program Fellow  
Laura M. Moy, Senior Policy Counsel  
Sarah J. Morris, Senior Policy  
Counsel

New America's Open Technology  
Institute  
740 15th Street NW, Suite 900  
Washington DC, 20005  
(202) 986-2700

Filed: November 9, 2015