

Before the Federal Communications Commission
Washington, D.C. 20544

In the Matter of

Amendment of Parts 0, 1, 2, 15 of the Commission’s Rules regarding Authorization of Radio-frequency Equipment for Wireless Devices))))))	ET Docket No. 15-170
Request for Allowance of Optional Electronic Labeling for Wireless Devices)))	RM-11673

Reply Comments of:
Stephen Satchell, private citizen
9350 Double R Blvd, #2217
Reno NV 89521-3824

Re: Reply to the 332 “non-brief” Comments on the above Docket as of Saturday, 17 October 2015

Table of Contents

Introduction.....2

Questions asked in the Notice.....3

Paragraph 58: “...When a party other than the grantee of certification modifies a device under the authority of the original grantee...”.....

Paragraph 69: “To ensure that the party responsible for the modification of a certified device is clearly identified, we believe modifications by third parties should not be permitted unless the third party receives its own certification. ...”.....

Paragraph 70: “Second, we propose to codify a uniform application process that applies in instances where parties other than the original grantee wish to make changes to certified devices. ... We propose to require that all parties making changes without the authorization of the original grantee of certification must obtain a new grant of certification and a new FCC ID. ...”.....

Paragraph 71: “...must include documentation substantiating that the original grantee has given permission to the new applicant to reference its original filing. ...”.....

Paragraph 74: “We also propose that when third parties repair or refurbish certified equipment to the device’s original specification without the grantee’s permission, we should require an application for certification for the equipment or take other action that would allow us to readily identify the third party and be assured that the repair does not serve to impermissibly modify the device.”.....

21.The point about the difficulties of obtaining permission is extremely important to many members of the Internet community, who would like to see “network trash” removed – preferably without using the “dumpster solution” for perfectly good hardware when less environmentally (and consumer) unfriendly solutions are available.....

Paragraph 78: “We also ask, more generally, about the information required when parties make changes to certified devices or file applications that rely on pre-existing certifications. ... What portions of the application should the new responsible party always be required to submit to obtain a new grant of certification? ...”.....

E-Labeling:.....

Summary of other points of interest, made in previously filed comments:.....5

34.Part 97 operators would be hurt by paragraphs 58, 69, and 70 as written.....

37.“Requiring signed firmware or similar is going to cause some problems similar to what we’ve seen recently where signing keys are stolen and then it becomes next to impossible to determine if you have legitimate drivers, firmware, etc. and makes it easier for malware to infect and retain persistence.”.....

- 42. “Zero of these violations [Weather Radar Interference Enforcement] named a non corporate entity as a cause[,] and point solely to commercial entity cause.” (Emphasis added. -- STS).....
- 43. “The recent Volkswagen case shows that using closed and uninspectable source code can lead to devices (vehicles) operating out of specification. Similarly, the inability to inspect the RF-controlling source code of routers makes it impossible to determine whether they are operating within specifications under all circumstances.”.....
- 45. Manufacturers of radio-based access points are incorporating Open Source software into their products, but in so doing they are violating the copyright terms applied to that software. Specifically, Version 3 of the GNU Public License mandates that parties who incorporate software that is covered by the license must also include all source, plus the toolchain and utilities to build and install that software into the target hardware. (This is in conflict with the Commission’s desire to “lock down” radio products. -- STS).....
- 47. “We have had, for nearly a decade, the Linux source code to access the regulatory database available, and it is already widely -- almost universally -- used. (see <https://wireless.wiki.kernel.org/en/developers/regulatory>).”.....

Comment posted to the Web but not seen on the Electronic Comment Filing System.....6

- 48. <https://www.iab.org/2015/10/07/iab-comments-on-proposed-fcc-rules-regarding-authorization-of-radiofrequency-equipment/> “On 7 October 2015, the IAB provided comments to the FCC on their proposed Amendment of Parts 0, 1, 2, 15 and 18 of the Commission’s Rules regarding Authorization of Radiofrequency Equipment (FCC 15-92)”.....

Partial list of open source projects affected by this Docket.....6

Further Discussion.....7

Proposal Option 1:.....7

- 56. If the combination of the hardware and the driver could be submitted for certification by the manufacturer, importer, and/or grantee, then changes to the other parts of the device could be made by anyone, with the driver enforcing any constraints.....

Proposal Option 2:.....7

- 61. For open-source software that does not investigate new modes of radio operation, the development for the radio-controlling part of a project could be broken out as its own source tree.....

Introduction

1. As part of this reply comment, I reviewed most of the of the comments already filed (other than brief comments and “vote” comments), and extracted what I believe other people have specifically said regarding the questions I have abstracted below. I will be adding my own comments, and also any further questions I have, about the questions I have selected for which you have requested comment. I believe the paragraphs from the original Notice I have abstracted below are of particular interest, not only to me but other members of the Internet Community at large.
2. I have also selected phrases from Comments with which I agree and that I believe should be considered, with side notes as appropriate.
3. I make no guarantee of the completeness of my summation here. This Reply Comment cannot be used as a substitute for a thorough examination of all of the comments in this Docket.
4. (NOTE: I did read all the comments, except the ones flagged with “Numerous” as the author and those considered brief -- this is supposed to be a discussion about the Commission’s proposal, as opposed to a vote. My sympathies to the person at the FCC who had to read every single one of the submissions. “Hate crimes”?)
5. How many comments or reply comments, if any, were submitted under seal?
6. Last, a general introductory observation: Many of the non-industry, non-Amateur-Radio comments concern indoor wireless access points. My research strongly suggests that the original problem relates to interference, by outdoor radio-based equipment, with TWDR weather radar (<https://www.fcc.gov/encyclopedia/weather-radar-interference-enforcement>). However, document FCC-15-92A1.pdf does not make this clear, and the proposed Rules reach far beyond the problem surface (which may be an unfortunate byproduct of the rule-making process).

Questions asked in the Notice

7. The Commission's questions of particular interest from the original document (FCC-15-92A1.pdf in <http://apps.fcc.gov/ecfs/comment/view?id=60001094486>) that I believe should be answered:

Paragraph 58: "...When a party other than the grantee of certification modifies a device under the authority of the original grantee..."

8. What happens if the original grantee has abandoned the device, or if the grantee itself has gone to corporate heaven and no longer exists in the form of a legal entity?
9. This question applies to several of the additional paragraphs in Section III-A-3, including, but not limited to, paragraphs 61, 63, 64, 65, 73, 75.
10. The issue of abandoned equipment is a serious one, especially in view of the home market for such radio devices. The existing tax code suggests that businesses should replace equipment periodically; however, the individual has no such incentive to "upgrade". The result is that equipment remains in service in the home for a much longer time, and is likelier to lag behind advances in technology and in regulations.
11. None of the industry commenters appeared to have addressed the issue of abandoned equipment.

Paragraph 69: "To ensure that the party responsible for the modification of a certified device is clearly identified, we believe modifications by third parties should not be permitted unless the third party receives its own certification. ..."

12. This is the crucial question for the Internet community, and is the focus of this Comment.
13. Agreed, explicit identification is the most desirable condition. But by which route(s)? Fresh certification, "delta" certification, or some other form of identification?

Paragraph 70: "Second, we propose to codify a uniform application process that applies in instances where parties other than the original grantee wish to make changes to certified devices. ... We propose to require that all parties making changes without the authorization of the original grantee of certification must obtain a new grant of certification and a new FCC ID. ..."

14. This point is the other side of the coin described in paragraph 69, and therefore is part of the crucial question.
15. I believe that the Commission's proposed change is the nexus of a solution for the problem of Open Software replacements for grantee firmware. The "Further Discussion" section below, in which I lay out my proposals, will make reference to paragraphs 69 and 70.

Paragraph 71: "...must include documentation substantiating that the original grantee has given permission to the new applicant to reference its original filing. ..."

16. What happens if the grantee is not available to give such permission? Or if the grantee is unwilling to grant permission to a piece of equipment that is at, or reaching, the end of its service life?
17. Several commenters mentioned that grantees have no incentive to make updates on older products, and may well have no incentive to authorize third parties to implement fixes. Indeed, grantees could plausibly have disincentives to grant such permission, namely, because doing so would cut into their sales of replacement products.
18. As one commenter pointed out, router vendors could hold innovators hostage, e.g., "You must assign to us all rights to your software in order for us to sell it."
19. The problem of obtaining permission from the original grantee appears to be analogous to the problem of obtaining republication rights to a book after the author has died. Sometimes it's almost impossible to locate the heir to the rights. Consider, for example, the copyright case currently swirling around the song "Happy Birthday to You".

Paragraph 74: “We also propose that when third parties repair or refurbish certified equipment to the device’s original specification without the grantee’s permission, we should require an application for certification for the equipment or take other action that would allow us to readily identify the third party and be assured that the repair does not serve to impermissibly modify the device.”

20. What is the definition of “original specification”? Does this refer only to the radio portion of a single-software flash load, or does the original specification include all of the non-radio crapware that may be in the original code – potentially with obsolete, missing, or buggy non-radio parts (such as incorrect TCP/IP stack implementations, missing IPv6 support, buffer bloat, security vulnerabilities, and operational errors)? What about changes that bring the radio portion into compliance with FCC rule changes, and the original grantee is absent or non-existent?
21. The point about the difficulties of obtaining permission is extremely important to many members of the Internet community, who would like to see “network trash” removed – preferably without using the “dumpster solution” for perfectly good hardware when less environmentally (and consumer) unfriendly solutions are available.
22. Regarding being able to identify the responsible party, I’m all for it. When things break, I do want to be able to locate and contact the person who broke it.
23. One commenter pointed out that the Internet community has no more IPv4 addresses to give out, and that IPv6 support in today’s AP/routers (i.e., radio-based access points) ranges from poor to none.
24. This comment is from the NANOG mailing list: “North American Network Operators Group has been discussing the IPv6 provisioning problem at length, with regards to how to deploy IPv6 faster – we are 17 years into the process! Specifically mentioned in the discussion was the lag in working IPv6 support in wireless access points as a stumbling block.” (This issue was not brought up in any of the comments I read, so I raise this new issue here.)
25. Many commenters have pointed out that the open-source software available today is of high quality. For example, the Linux operating system is in widespread use in large mission-critical corporate systems. Indeed, much of the wired Internet is stitched with versions of Linux and the Berkeley System Distribution (BSD) operating system.
26. Some critics of the Open Source philosophy point to the “Heartbleed” security vulnerability as a negative. However, what is important is that *the fix for the problem was released very, very quickly*. The vulnerability was detected on 1 April 2014, and a fix was released on 7 April. Internet servers with actively maintained distributions were updated with a day of release. For servers running OS distributions beyond end of life – not unlike the problem with older Wi-Fi radios and access points – the update history is more spotty. Many of these out-of-date systems were updated expeditiously by system administrators who replaced the distributor-version-controlled version of SSH with locally compiled versions of the open-source project code. This is the most recent industry precedent that shows the need for alternative sources for updated software.
27. Speaking more generally of the Internet: it’s a constantly moving target. I have watched and participated in the development of the Internet every since its early incarnation as the ARPAnet, for which I worked on the development of the Graphics Network Protocol. It was a swiftly moving target even then. Operators and researchers learn new things about this monster every single day. What we learn then has to be put into practice, i.e., by being installed in the network software.
28. Network operators regularly install updated software provided by the vendors of routers, security appliances, network switches/hubs, enterprise WiFi equipment, and servers, as the academic community continues its research on making the Internet perform better and in ever-broader classes of applications. The Commission has seen some of the results of these improvements, including telephony over IP, not only by individuals, corporations, and institutions, but by the telephone companies themselves.
29. Unlike the classic broadcast/two-way radio market, there is a considerable amount of “churn” in the vendor population. Companies are like flowers: some are perennial, while others are annuals and die in the fall, with new flowers taking their place in the spring. We are not talking about Motorola, Collins Radio, or Gates Radio here.

Paragraph 78: “We also ask, more generally, about the information required when parties make changes to certified devices or file applications that rely on pre-existing certifications. ... What portions of the application should the new responsible party always be required to submit to obtain a new grant of certification? ...”

30. A very good question. My opinion is that the amount of information to be provided should be limited to the “delta” between the original filing and the current filing.

31. One commenter says that the new-responsible-party applicant should be able to reference all exhibits in the original grantee's filing. I agree strongly with this point, because it's a cornerstone for a possible solution to Open Source replacement-ware. (see Proposals below.)

E-Labeling:

32. I have skipped over the questions you have asked about E-labeling, because I believe that the comments you have already received on the subject fully cover the needs of the Internet and the research communities.
33. However, I would note that if Web-based labeling is used exclusively for Open Source "products", there needs to be a way for the new software to access the certification of the underlying hardware and proprietary radio-controlling software (if any). If the certified portion consists of both hardware and a grantee-provided "blob" of software, then the API to the blob needs to provide all of the certification information for display.

Summary of other points of interest, made in previously filed comments:

34. Part 97 operators would be hurt by paragraphs 58, 69, and 70 as written.
35. Requiring software support by the grantees for 5 or 10 years is beyond the charter of the Commission.
36. "... operating ANY transmitter outside of the authorized specifications is already against the law, and such persons should be sanctioned under the law."
37. "Requiring signed firmware or similar is going to cause some problems similar to what we've seen recently where signing keys are stolen and then it becomes next to impossible to determine if you have legitimate drivers, firmware, etc. and makes it easier for malware to infect and retain persistence."
38. "We are working on a small wireless mesh project with the goal of providing low-cost community-run internet for our neighborhood. We are using routers from which we remove the factory software and install free software provided by Commotion Wireless."
39. "As a U.S. service member stationed overseas, I rely on custom firmware for my routers so I can operate within the guidelines of the host country I live in."
40. "Almost every wireless LAN device allows the consumer to disable operation on a band (such as 2.4 GHz), and thus would be affected by this proposed rule change." (*The law of unintended consequences in action. -- STS*)
41. "Mandated open source for firmware. It's not just a good idea, it should be the law. " (*I believe this would also be beyond the scope of the Commission's charter. -- STS*)
42. "Zero of these violations [Weather Radar Interference Enforcement] named a non corporate entity as a cause[,] and point solely to commercial entity cause." (*Emphasis added. -- STS*)
43. "The recent Volkswagen case shows that using closed and uninspectable source code can lead to devices (vehicles) operating out of specification. Similarly, the inability to inspect the RF-controlling source code of routers makes it impossible to determine whether they are operating within specifications under all circumstances."
44. The Commission should require, from open-source projects, "that the source-code of the WiFi drive[r]s be approved by a software developer holding a General Radio Operator's License with Ship Radar Endorsement (GROL+Radar), and that source code should include a statement of approval and contact information for that developer." (*see the Proposals section below for a modification to this idea. -- STS*)
45. Manufacturers of radio-based access points are incorporating Open Source software into their products, but in so doing they are violating the copyright terms applied to that software. Specifically, Version 3 of the GNU Public License mandates that parties who incorporate software that is covered by the license must also include all source, plus the toolchain and utilities to build and install that software into the target hardware. (*This is in conflict with the Commission's desire to "lock down" radio products. -- STS*)
46. "[The Internet Community] presently gets these horrible dumps of code in compliance with the GPL's mandate -- huge tarballs, no commit logs. It takes years, sometimes, for the community to sort them out. That needs to end." (*Emphasis in original*)

47. “We have had, for nearly a decade, the Linux source code to access the regulatory database available, and it is already widely -- almost universally -- used. (see <https://wireless.wiki.kernel.org/en/developers/regulatory>).”

Comment posted to the Web but not seen on the Electronic Comment Filing System

48. <https://www.iab.org/2015/10/07/iab-comments-on-proposed-fcc-rules-regarding-authorization-of-radiofrequency-equipment/> “On 7 October 2015, the IAB provided comments to the FCC on their proposed Amendment of Parts 0, 1, 2, 15 and 18 of the Commission’s Rules regarding Authorization of Radiofrequency Equipment (FCC 15-92)”
49. “The IAB welcomes the focus on security, but notes that software security features of this type must be broad enough to permit device firmware updates by parties other than the manufacturer itself.”
50. Reply Commenter completely agrees with the Internet Architecture Board.

Partial list of open source projects affected by this Docket

51. I am not yet a participant in the development of software for access points, so I am not aware of all the projects that currently exist. However, Wikipedia (https://en.wikipedia.org/wiki/List_of_router_firmware_projects) lists the following ones:

OpenWrt	https://openwrt.org/
Commotion Wireless	https://commotionwireless.net/
DD-WRT	http://www.dd-wrt.com/site/index
Gargoyle	https://www.gargoyle-router.com/
libreCMC	https://librecmc.org/
Wifidog	http://dev.wifidog.org/
Roofnet	(dead link, see https://en.wikipedia.org/wiki/Roofnet)
CeroWRT	http://www.bufferbloat.net/projects/cerowrt
DebWRT	http://www.debwrtnet/
HyperWRT	Superseded by Tomato
Tomato Firmware	http://www.polarcloud.com/tomato
Serval Project	servalproject.org

52. I was disappointed that the list of 332 comments and reply comments did not include anyone specifically identified with any of the projects listed above. (I learned that some representatives from these projects did collaborate on the comment from Dave Täht – see <http://apps.fcc.gov/ecfs/comment/view?id=60001303221>.) I would suggest that the Commission invite the sponsors of these projects to participate in this Docket, or a subsequent revision of this Docket, so that all of the affected parties can be heard.
53. Remember, many of the non-industry commenters are individuals who tossed off quick remarks opposing the proposed rules, rather than being paid to take the time to dissect Dockets like this one. (For the record, I have not been paid by *anyone* to prepare and submit this document.)

Further Discussion

54. **Non-profits:** One issue with the Docket proposal as original written is that the content is directed almost exclusively toward the commercial product community, with even the Amateur Radio operators being given very short shrift. This Proceeding appears to ignore completely the role of non-profit players in the development and advancement of radio-based networking, and networking in general. Moreover, some of the decisions made by the existing grantees exacerbate the problem. I would posit that very few changes, augmentations, and expansions are required to satisfy the Part 97 operators and the many users of WiFi devices (such as WiFi routers). The seeds of a solution are in the Notice; now we need to nurture those seeds so that they can sprout.
55. **Software/System design:** The typical WiFi access points contain a great deal of software that does *not* involving the radio. A certain amount of this software sets up the frequency, power, and modulation parameters, as well as the parameters for special activities like DFS, that directly affect the transmitter. A system-level view of one of these devices in a consumer configuration, reveals the radio hardware, the radio software (driver), and the upper-level software that, for example, involves data transfer on the over-the-air network. If the first two elements could be considered a modular radio, then it's possible to divorce radio control from data control and from the user interface.

Proposal Option 1:

56. If the combination of the hardware and the driver could be submitted for certification by the manufacturer, importer, and/or grantee, then changes to the other parts of the device could be made by anyone, with the driver enforcing any constraints.
57. One way to do this would be for the grantee to submit the combination of hardware and driver to the FCC and receive certification for the combination. The grantee would need to build an instrumented scaffold for the driver so that all of the pertinent operations could be performed and so that the in-device measurements could be taken.
58. In the case of open-source software, the driver would be provided by the grantee in the form of a software “blob” that would be maintained by the grantee. The applications program interface (API) for the blob would ensure that all requests for settings would comply with the rules. Indeed, the API could provide information about legal settings, so that the GUI portion of the device could display the available options for the operator to select.
59. The advantage to this approach is that the non-profit projects would not need to submit certification documents, because the underlying hardware and radio-controlling software would already be certified.
60. The disadvantage of this approach is that FCC rule change implementation would depend on the original grantee – if that grantee can be located. Another disadvantage is that a grantee might need to provide multiple blobs, one for each regulatory region.

Proposal Option 2:

61. For open-source software that does not investigate new modes of radio operation, the development for the radio-controlling part of a project could be broken out as its own source tree.
62. Like Option 1 above, it separates the radio-controlling development from the non-radio-controlling development of a project. Indeed, because the radio-controlling would be a separate tree, the results of that development could be shared among multiple projects.
63. Instead of requiring each project to deal with re-certification, the one radio-controlling software project could jump through all of the necessary procedural and document-generation hoops in order to satisfy the rules proposed in the Docket without any special carve-outs, other than expanding the idea of “Family of Products” to allow the Internet Community to have such a family. Any costs could be shared among the various projects. Further, because the developers of the radio-controlling software would be dedicated, they would be in a position to respond very quickly to FCC rule changes.
64. This proposal also facilitates certification for manufacturers who, instead of developing their own software, choose to use the open-source software. In particular, such an adoption would expedite the certification process, because the manufacturer could then “piggy-back” on the certification by the open-source project’s work and filing.

65. I would suggest that the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and/or the Internet Architecture Board (IAB) would be the proper body to co-ordinate such a project. Much of the work on the Internet is channeled through these organizations. As an American National Standards Institute (ANSI) recognized Standards Provider, the IEEE or IETF could codify the API of such a project so as to minimize confusion and duplicated effort. Once that's done, the IEEE or IETF could go through the proper channels to present that standard to the International Telecommunication Union, so that a worldwide standard could be established.
66. This second option also re-opens the ability of Part 97 operators to re-purpose consumer-grade devices for use in the Amateur Radio bands.
67. Another advantage of this particular option is that researchers who want to experiment with novel modes of radio operation can do so, performing their experiments in RF isolation so that their emissions will not interfere with anyone else, while leverage the existing radio-controlling code. In other words, why re-invent the wheel?
68. The disadvantage of this approach lies in the cost and effort on the part of the radio-controlling software development team.

Respectfully submitted,
Stephen Satchell