Before the

FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Amendment of Part 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radio frequency Equipment	)	ET Docket No. 15-170
	)	
Request for the Allowance of Optional Electronic Labeling for Wireless Devices	)	RM-11673
	)	

Comments of the Center for Democracy & Technology

The Center for Democracy & Technology submits these brief comments to request that the Commission consider either altering its proposed rules regarding modification of certified equipment by third parties or addressing the issue in a separate proceeding. Radiofrequency (RF) interference is a serious issue fully deserving of the Commission's attention. However, the proposed rule requiring "software controls that are provided to prevent unauthorized parties from enabling different modes of operation"[1] present equally serious concerns. It could interfere with efforts to improve the adaptability and security of the firmware controlling routers and other RF devices, and also needlessly subject device owners and researchers to potential liability under Section 1201 of the Digital Millennium Copyright Act.[2] While the Commission does not

[1] Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment, *Notice of Proposed Rulemaking*, 30 FCC Rcd. 7725 (2015), Appendix A, Proposed Rule 2.1033(a)(4)(i) ("NPRM").
[2] 17 U.S.C. §1201.

intend these results,[3] it is unclear how they can be avoided under the proposed rule. CDT therefore suggests that the Commission consider altering the proposed rule in further consultation with open source developers, device manufacturers, and security researchers. If that consultation would unduly delay adoption of rules that implement the E-LABEL Act[4] and carry out other important policy objectives, it may be best to address third-party modification in a separate proceeding.

The NPRM proposes requiring certified equipment to include security measures that prevent unauthorized modification of the power and frequency parameters of RF devices.[5] Although the Commission's intent is not to ban all modification or the installation of any third-party or open-source firmware, security researchers and others are understandably concerned that this will be its unintended effect.[6] Even the Commission has acknowledged that locking down a router to prevent any modification would be an expedient way to comply with the rule.[7] And the Office of Engineering and Technology's March 2015 guidance on software security requirements for U-NII devices expressly asks applicants for equipment authorization to "[d]escribe in detail how the

---

[3] *See* Karl Bode, "No, the FCC Is Not (Intentionally) Trying to Kill Third-Party Wi-Fi Router Firmware," Techdirt, September 3, 2015, *available at* https://www.techdirt.com/blog/wireless/articles/20150831/07164532118/no-fcc-is-not-intentionally-trying-to-kill-third-party-wi-fi-router-firmware.shtml.

[4] Enhance Labeling, Accessing, and Branding of Electronic Licenses Act (E-LABEL Act) of 2014, Pub. L. No. 113-197 (Nov. 26, 2014).

[5] NPRM at ¶ 46.

[6] *See* Kyle Wiens, "Hey FCC, Don't Lock Down Our Wi-Fi Routers, Wired, September 25, 2015, *available at* http://www.wired.com/2015/09/hey-fcc-dont-lock-wi-fi-routers/.

[7] Jon Brodkin, "FCC: Open source router software is still legal—under certain conditions," ArsTechnica, September 25, 2015, *available at* http://arstechnica.com/information-technology/2015/09/fcc-open-source-router-software-is-still-legal-under-certain-conditions/.

device is protected from 'flashing' and the installation of third-party firmware such as DD-WRT."[8]

Continued development and use of third-party firmware such as DD-WRT or OpenWRT should not be discouraged. The firmware that ships with some RF devices can be out of date or otherwise vulnerable to security exploits.[9] Projects like OpenWRT strive to make firmware more secure, user-friendly and adaptable to new protocols like IPv6. Because these projects are generally open source, they benefit not only the owners of RF devices but also device manufacturers and the broader research community. Despite these benefits, the proposed rules may discourage not only the installation of third-party firmware but also its continued development.

Mandating software controls on RF devices may also place device owners or researchers at risk of liability under Section 1201 of the Digital Millennium Copyright Act[10] unless they own or have express authorization to access the underlying firmware. In the absence of an applicable exception, a person who circumvents a technological protection measures controlling access to a work (including firmware) may violate Section 1201 regardless whether any copyright infringement occurs. Because Section 1201 broadly defines circumvention to mean, among other things, "to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner[,]" bypassing a software control to install third-party firmware raises a

---

[8] Federal Communications Commission, Office of Engineering and Technology, Laboratory Division, "Software Security Requirements for U-NII Devices," March 18, 2015 at 2.

[9] *See* Kim Zetter, "Why Firmware Is So Vulnerable to Hacking, and What Can Be Done About It," Wired, February 24, 2015, *available at* http://www.wired.com/2015/02/firmware-vulnerable-hacking-can-done/.

[10] 17 U.S.C. § 1201.

risk of liability under 1201. The penalties for violating Section 1201 are significant, including statutory damages of up to $2,500 per violation and possibly even criminal penalties.[11] Although circumvention may fall within a statutory exemption or a party may seek a specific three-year exemption from the Librarian of Congress, the mere risk of liability casts a long shadow on work that our laws and policies should instead encourage.

CDT does not believe the Commission intended either to deter beneficial work on open-source firmware for RF devices or to subject the individuals performing that work to potential liability. However, the proposed rules in the NPRM do not provide a clear path for that work to continue. The best prospect for finding that path while taking meaningful action to prevent harmful modification of the power and frequency parameters of RF devices may lie in further cooperation between the Commission's policy and engineering staff, device manufacturers, and the engineers, researchers, and users who work with and depend on third-party firmware. CDT therefore suggests that the Commission reconsider its rules relating to third-party modification and possibly address the issue in a separate proceeding, working with all interested parties on an alternative solution that addresses interference concerns while avoiding unintended and undesirable consequences.

Respectfully submitted,

/s/
Erik Stallman
General Counsel and Director, Open Internet Project
Center for Democracy & Technology

October 9, 2015

[11] 17 U.S.C. §§ 1203(c)(3), 1204.