Received & Inspected
SEP 11 2015
FCC Mail Room

112 Belmont Road
Apple Valley, MN 55124

4 September 2015

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

Regarding ET Docket No. 15-170; RM-11673

Dear Mr. Butler

I was recently made aware of the proposed rule referenced in the above docket. This letter is a formal comment on that proposed rule, and due to the accessibility of the FCC IT infrastructure will be submitted both by mail and electronically as soon as the ability is restored.

Firstly, allow me to provide a little background information about myself. I received degrees in both Computer Science and Electrical Engineering from the University of Minnesota in 1999. I received an M.S. degree in Software Engineering in 2008, and am currently pursuing a PhD in Computer Science with an emphasis on security.

Given both my background, as well as personal reasons, the proposed rule is deeply concerning to me, for reasons to be described below. I certainly agree that the Federal Communications Commission has a legitimate interest in ensuring that the radios in wireless networking equipment operate within the parameters the Commission has authorized. However, I believe that the legitimate interest of the Commission can be served without measures such as disallowing the updating of the operating system, as the proposed rule has called out, namely by requiring the radio, either through its own standalone firmware or by settings embedded in the hardware.

The first concern I have is in fact from the perspective of security vulnerabilities. As vulnerabilities are found in the software that runs on wireless routers and access points, the manufacturers of those devices generally correct them by issuing new updates to the firmware. This is not, however always the case, particularly with older devices. Take for example the Linksys model WRT54G wireless router. Over the course of its lifetime, it has been through 12 different hardware revisions according to its support page on the Linksys web site. However, none of those versions has any updates available to the firmware anymore. At one point they did; I owned one at one time and kept the firmware updated regularly. These

No. of Copies rec'd 0
List ABCDE

devices are incredibly resilient with the first versions being released in December 2002. My parents still have one of these devices.

The problem here seems apparent; this particular model is no longer supported, so although it still works great and serves its purpose, if a vulnerability is found with it, the only recourse to protect the network it serves is to replace the router. We know that the TJX breach that allowed millions of payment card numbers to be compromised in 2007 was a result of insecurities in the WiFi systems their payment terminals were connected to. While the 2013 data breach at Target was more the result of bad network security practices than WiFi insecurities, it could have just as easily been a result of WiFi problems.

For large retailers such as Target and TJX, this isn't a problem. If an insecure device isn't supported there's always a capital budget expenditure to be made to upgrade the hardware (no doubt to the cheering of the manufacturers). However, for the mom and pop Chinese restaurant down the street with the off-the-shelf router they bought to hook up to their cable modem or DSL line, the budget is probably not there.

Because of a lack of manufacturer support for older hardware, third-party firmware packages, such as DD-WRT (which was explicitly called out in the proposed rulemaking information, and which I am a widespread user of), are often the only choice for security updates to the router software[1]. As worded, the proposed rule would prohibit users from maintaining good security practices on their networks.

Secondly, on devices for which the manufacturer does in fact provide firmware updates, it may take weeks or months for those vulnerability fixes to be released to the public. On the other hand, the version of DD-WRT I employ in my home network has fresh builds available typically weekly or more frequent if needed. While the Netgears and Ciscos of the world may take a couple of weeks to patch all their firmware against a vulnerability such as the 2014 Shellshock breach in the Unix Bash shell program (CVE-2014-6271), the third-party firmware community (as a result of being a subset of the open source software community) typically has the fix in place within hours, if not before it can even become an issue. The ability to mitigate broad security problems quickly would be outlawed if this proposed rule is adopted as is.

Third, manufacturer-provided firmware is designed to be as easy to use as possible. Since their typical user isn't necessarily a tech-savvy network administrator, this is understandable. The mom and pop Chinese restaurant wants to be able to plug in their computer, credit card terminal, maybe a Voice over IP phone or two, and other hardware and have it all just work. Maybe they want to provide free WiFi services to their customers while they dine. The typical firmware on off-the-shelf routers, for example, typically comes with a piece of software called UPnP enabled. UPnP enables programs running on the local network to open up network ports on an as-needed basis to communicate with the outside world.

---

[1] It should be noted that the firmware installed on any given router is not typically a monolithic piece of software. There is an operating system kernel, a web server to facilitate external communication, an application which processes the requests the user makes via the web server, software drivers for the various networking devices (wireless radios, Ethernet ports, etc.), various services (e.g., a Network Time Protocol client to keep the router's internal clock in sync with the world). Any one of these pieces can result in a security vulnerability with the router.

According to Netgear's page on UPnP and its routers, "Security risk associated with enabling UPnP on the router, technically a worm or malware program could use this function to compromise security for the entire LAN".

One of the fundamental tenets of computer security is at the attack surface should be as small as possible. This means only enabling pieces of the software that are necessary to meet the needs of the installation. While there may be a need for UPnP for some users, that's certainly not the case for all, and definitely not the mom and pop Chinese restaurant. The typical manufacturer firmware is the antithesis of this principle, enabling everything the end user may need, opening the router up to both the good users and the malicious ones. Third-party firmware distributions typically have distinct packages: a minimal build with just the necessary packages installed, a build which has everything installed, and something somewhere in between. Many even allow a user to install the minimal build and install only the explicit packages they need (although arguably this is not the route the mom and pop Chinese restaurant would use).

Fourth, third-party firmware enables features in commodity routers that are frequently only available in higher-priced "commercial-grade" models. One example of this is the ability to present multiple distinct networks (both wired and wireless). The mom and pop Chinese restaurant can (and if we're perfectly honest should) have a wireless network for use by its customers (if it wants to offer free wifi) that is distinct from the network it is using for business purposes. They can't do that with an off the shelf device using the manufacturer supplied firmware, but with a third-party solution like OpenWRT or DD-WRT, they open themselves to a more secure world. The customer wi-fi network can be isolated from the business wi-fi network while using a single inexpensive device rather than one costing hundreds or even a couple thousand dollars.

As another example, small offices or restaurants, and even home users use these devices as active security devices (firewalls). In reality, the manufacturer firmware seldom provides more of a firewalling capability than what can be provided with simple Network Address Translation[2]. Third-party firmware solutions enable more complex firewalling abilities, even allowing these devices to serve as Virtual Private Network end points which enable employees to work remotely while having access to the internal network. Such users are unlikely to spend the thousands of dollars necessary for a high-end solution that for which they really have no need. In the end, these users rely on the security provided by NAT, which is little more than security through obscurity, which is inherently insecure.

As a final example of features available in third-party firmware versus manufacturer firmware, I offer up my own home as an example. It is large enough that if I have a single centrally-located access point, the signal is weaker than I'd like it to be, particularly on the 5GHz band that is the subject of this proposed rule. Because of this I actually have a pair of higher-end consumer-grade NetGear R7000 routers, both running the DD-WRT firmware, stationed at each end of the house to provide complete coverage. Our

[2] Network Address Translation is a mechanism by which multiple computers on one side of a translator (in this case the consumer router) can access resources on the other side of the translator (i.e., the Internet), while appearing to share a single IP address (the public side of the router). It was developed as a stopgap method of dealing with the dwindling supply of IPv4 addresses available to end users. While it provides minimal security, as the deployment of IPv6 increases, it will become unnecessary, and that security will disappear.

home phone service comes in as Voice over IP, and we have several WiFi-based cordless phones, as well as soft-phone applications on our iPhones. DD-WRT allows me to broadcast two distinct network names, which are attached to different VLANs[3] on their uplink connections. One network is for laptops and other wireless devices to use and for guest access. The other is for the Voice over IP network. In fact I actually have a third VLAN available at the R7000's, as they are both located near our DirecTV receivers and Blu-Ray players, both of which plug into the wired Ethernet ports on the routers as a media-specific network.

Breaking my home network down into distinct VLANs allows me to prioritize the network traffic on the uplink ports so that the voice traffic gets the highest priority, followed by the laptop network, followed by the media network. With DD-WRT I have seamless integration and handoff between the two routers when a phone moves between their zones of coverage. In fact one of the advantages of using DD-WRT is that I can actually turn the transmit power down on the routers, to balance out the signal strengths better where the broadcast ranges overlap. If I were only able to use the manufacturer's firmware on these routers, I'd either lose a significant amount of control over my own network, or I'd be forced to spend several thousand dollars on an enterprise-grade system. I know this is something that's a lot more complex than a typical home user would do, but there's a legitimate case for it in the case of the mom and pop Chinese restaurant I've been mentioning, and literally millions of other small businesses across the country. Yes, these advanced networking features won't "just work" out of the box, even with a third-party firmware, but they aren't even in the box with manufacturer firmware, and they don't "just work" out of the box with an expensive solution. The difference between the expensive solution and the third-party solution being that the features are easy to configure through a web-based GUI with the third party firmware.

As a final argument against this proposed rule, a significant number of manufacturers are relying on the Linux operating system and many other open source tools that are licensed under the GNU General Public License. The reasons for this are vast, but just like the reasons customers with relatively simple needs choose off the shelf hardware instead of expensive commercial software, GNU/Linux is the software of choice because it just works. However one of the conditions of the software is that when a manufacturer customizes it and redistributes it, they are required to make their source code changes available to the end users, so that they can further customize it (this also has a side benefit of the source code being available for peer review to find security vulnerabilities). Many of these packages are licensed under version 3 of the GPL, which not only requires that the source code be made available to the consumer, but also any facilities necessary to actually use that software along with the hardware. Without changing many underlying software packages, manufacturers may not even be able to comply with the proposed rule as written because the end-user would be prohibited from using the modified software on the router. Such a rule would impose undue burdens on the device manufacturers who would now have to find different software, or write their own to replace the functionality they could no longer legally deliver due to copyright law.

---

[3] A VLAN, also known as a Virtual LAN, is a method by which network switching equipment can divide its ports into separate networks, or broadcast domains without using multiple network switches. Typically a given network port is connected to a single VLAN, however multiple VLANs can be assigned to a signle network port and aggregated over a "trunk" line between different switches.

In closing, I'd like to point out that the Supreme Court standard of strict scrutiny, *United States v. Carolene Products Company*, 304 U.S. at 155 (1938)[4], may be relevant here, as there is a potential first amendment liberty at stake. As I'm sure the Commission is already aware, strict scrutiny is a three pronged test: there must exist a compelling governmental interest, the policy must be narrowly tailored to meet that interest, and the least restrictive means of meeting that interest must be used. There is no argument that the Commission has a compelling interest in implementing this proposed rule; the RF spectrum is a limited resource, and radios which transmit at a higher power than lawfully allowed interfere with other radios. I would argue that restricting the ability of the software in consumer routers to increase the transmitter power beyond what is legally allowed is sufficiently narrowly tailored to solve the problem the rule is trying to solve. The problem with the rule, as I see it, is that outright prohibiting third-party firmware is not the least restrictive means for achieving the desired end result.

The firmware which controls the radio, and that which provides the operating system of the router, while often packaged together, end up in distinctly different locations on the hardware, and are in fact two distinct pieces of software. The radio firmware is incredibly specific to the hardware, and is typically provided as a binary blob to the manufacturer from the supplier of the actual radio hardware. Usually, the source code for this firmware is in a form proprietary to the manufacturer of the radio hardware, and useless to the end consumer of the product. It can, in fact, be deployed to the radio separate from the firmware that provides the general operating system for the device. As an example, Apple's iPhone devices receive both distinct radio firmware updates and more generic iOS updates (although on belief, the former is often contained in the latter). Router firmware updates which contain radio firmware updates update the radio firmware separately from the operating system. There is no compelling reason to prohibit consumers from installing a third party firmware in the name of limiting the radio power to that which is lawfully allowed, when that goal can be achieved through hardware means that would prevent the radio from transmitting with too high of a power level, while allowing the operating system to be modified by the user.

---

[4] There may be narrower scope for operation of the presumption of constitutionality when legislation appears on its face to be within a specific prohibition of the Constitution, such as those of the first ten amendments, which are deemed equally specific when held to be embraced within the Fourteenth. *See Stromberg v. California*, 283 U. S. 359, 283 U. S. 369-370; *Lovell v. Griffin*, 303 U. S. 444, 303 U. S. 452.

It is unnecessary to consider now whether legislation which restricts those political processes which can ordinarily be expected to bring about repeal of undesirable legislation is to be subjected to more exacting judicial scrutiny under the general prohibitions of the Fourteenth Amendment than are most other types of legislation. On restrictions upon the right to vote, *see Nixon v. Herndon*, 273 U. S. 536; *Nixon v. Condon*, 286 U. S. 73; on restraints upon the dissemination of information, *see Near v. Minnesota ex rel. Olson*, 283 U. S. 697, 283 U. S. 713-714, 283 U. S. 718-720, 283 U. S. 722; *Grosjean v. American Press Co.*, 297 U. S. 233; *Lovell v. Griffin, supra*;on interferences with political organizations, *see Stromberg v. California, supra*, 283 U. S. 369; *Fiske v. Kansas*, 274 U. S. 380;*Whitney v. California*, 274 U. S. 357, 274 U. S. 373-378; *Herndon v. Lowry*, 301 U. S. 242, *and see* Holmes, J., in *Gitlow v. New York*,268 U. S. 652, 268 U. S. 673; as to prohibition of peaceable assembly, *see De Jonge v. Oregon*, 299 U. S. 353, 299 U. S. 365.

Nor need we enquire whether similar considerations enter into the review of statutes directed at particular religious, *Pierce v. Society of Sisters*, 268 U. S. 510, or national, *Meyer v. Nebraska*, 262 U. S. 390; *Bartels v. Iowa*, 262 U. S. 404; *Farrington v. Tokushige*, 273 U. S. 284, or racial minorities, *Nixon v. Herndon, supra; Nixon v. Condon, supra:* whether prejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities, and which may call for a correspondingly more searching judicial inquiry. *Compare 17 U. S. Maryland*, 4 Wheat. 316, 17 U. S. 428; *South Carolina v. Barnwell Bros.*, 303 U. S. 177, 303 U. S. 184, n 2, and cases cited.

Relying on software to limit the output power of radio-frequency devices has a history of being problematic. Take as an example the case of the Therac 25. The hardware interlocks of the predecessor which restricted the radiation doses delivered to safe levels were replaced by software interlocks, which failed at least a half-dozen times, resulting in severe injuries and 3 deaths. Arguably that isn't a risk here given that these routers typically have a 25W power supply at best and the radios aren't physically capable of emitting that much power. But it is far from inconceivable that they could produce unwanted interference (hence the government's legitimate interest in controlling the output power). But as the proposed rule itself states there is an expectation that there will be distinct hardware produced for the US market and distinct hardware produced for the rest of the world. Under such circumstances, there is no reason that the transmit power cannot be limited physically with hardware that would otherwise be unmodifyable by the user (without explicitly triggering existing rules about transmitter medication).

As an aside, my passion for engineering grew in part because the facilities existed for me to tinker with electronic devices, such as model railroad throttles, when I was younger. Sadly, the advancing miniaturization of electronics over the past two decades has made this tinkering a lost art, not for lack of desire but because such tinkering requires such specialized tools. While I lament its loss, that loss is a contributing factor to why a hardware limitation on the transmit power is actually feasible; the average user doesn't have the tools that would be necessary to rewire a surface-mount based circuit board. There are volumes of research that have been published in the field of computer science that would not have been possible without the ability to modify the software on consumer-grade routers, unnecessarily resulting in even more innovation leaving the country for foreign lands.

While I can appreciate the goals the Commission has in mind in making this rule, I strongly encourage the Commissioners to consider reducing the scope of the prohibition on third party firmware in consumer routers.

Sincerely,

Jason Michaelson

cc: Congressman John Kline