November 6, 2015

VIA ELECTRONIC FILING

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: Notice of Oral Ex Parte Presentation
ET Docket No. 15-170 (Amendment of Part 0, 1, 2, 15 and 18 of the Commission’s Rules regarding Authorization of Radio frequency Equipment)
RM-11673 (Request for the Allowance of Optional Electronic Labeling for Wireless Devices)

Dear Ms. Dortch:

On Wednesday, October 22, 2015, I met with Gigi Sohn of Chairman Wheeler’s office, Julius Knapp and Walter Johnston of the Office of Engineering and Technology, and Chief Technologist Scott Jordan regarding the above referenced proceedings.

I reiterated a number of the points the raised in an October 9, 2015 filing concerning the modification and security of Wi-Fi routers. Specifically, I expressed concern that in the past, some manufacturers of Wi-Fi routers have used the existence of FCC rules as a pretext to lock down their devices’ firmware, and that some of the language in the Commission’s NPRM may compound this problem. I urged the Commission to provide clear guidance so that particular vendors no longer continue “hiding under [the FCC’s] skirts.”

I then discussed my larger concern about the security (or lack thereof) in router firmware, and that in many of the devices currently on the market, that security gets worse over time. To that end, I encouraged the Commission to find ways to work with me and others in the engineering community to build a faster, safer, better maintainable Internet – and in particular, make Wi-Fi faster, safer and more reliable while still staying within the bounds of regulatory constraints. The specifics of what I urged the Commission to do with regard to router firmware performance and security is in the document attached to this letter, and expounded in much more detail in the October 9 filing.

This notice is being filed in the above-referenced dockets for inclusion in the public record.

Sincerely,

/s/ Dave Taht

cc. Gigi Sohn
Julius Knapp
Walter Johnston
Scott Jordan

---

1 See Comments of David Taht, Vint Cert, et al., ET Docket 15-170, RM-11673 (filed October 9, 2015)
Future Goals in collaborating with the FCC

What we (the Bufferbloat project) would like to see happen: Find ways for all stakeholders to work together to build a faster, safer, better, maintainable internet – and in particular, make wifi faster, safer, and more reliable while still staying within the bounds of regulatory constraints.

1. SPECIFIC ASK: Open hearings, form a standing committee to investigate – and to advise industry and the government on best practices, regulation, legislation and policy.

1. The FCC should embrace enough of the principles set out here and as they evolve for chipmakers and vendors to no longer claim that “The FCC won’t let us do that”, with clear policies and unambiguous guidance to those corporations, researchers, engineers, and third party firmware projects to allow for future positive directions for the Internet.

2. OVERALL DIRECTION (including objective for the committee) - Make the world of home routers, gateways, and IoT switch from “default, closed”, to “default, upgradable”, and encourage following best engineering practices such as the usage of source code control systems. This allows for patches for regulatory problems, bugs, upgrades, and security flaws to be much more easily distributed to the field.

1. END SALE OF VULNERABLE DEVICES: Stop the flood of devices not following best practices from entering the country and being hooked up to the internet, and left there, unsecured, and unmaintained.

2. VERIFIABLE SOURCE CODE: Additionally the security community would like firmware that can be verifiably produced from its actual source code, enabling the engineering, research, and third party firmware communities to resume working directly on the latest generations of wifi hardware (in particular).

3. ACCESS TO CODE ENABLES BETTER PERFORMANCE: Access to code would further enable installed modems to perform much better: for example, adding ~50 lines of code to the lowest layer of the DSL interfaces can make DSL modems to perform much better (lower delays / latencies in throughput) with ~1,000 lines higher up the stack. Cable modems and fiber interfaces are more complex but the amount of actual code is similar. However, vendors and network operators have few incentives to perform these upgrades.

1. Find ways to improve upcoming devices, and those already in the field (DSL, Fiber, Cable, Wifi) to reduce their latency under load (e.g. bufferbloat remediations). This will require that some core binary blobs be revised and distributed while somehow retaining or regaining FCC certification along the way.
4. **ACCESS TO CODE ENABLES MINIMIZATION OF FREQUENCY CONFLICTS**: Doing things like DFS are much harder than merely ensuring the right power/channel combination. Having a standardized software library and interfaces for DFS detection would be good to work on.

5. **(REDUCE ATTACK SURFACES)** Make it possible for single CPU versions of wifi-connected devices to still exist, with the associated lowering of overall cost, the reduced latency, and the increased security and auditability that existed before 802.11ac started to deploy, as opposed to the baseband co-processor model used elsewhere in the wireless field.

---

**Bufferbloat Project (And CeroWrt) Accomplishments**

2011-2015

- Came up with a simple, deployable algorithm, “BQL”, for making low rate edge devices (such as DSL) behave much better at lower rates.
- Developed and tested multiple AQM and Fair Queuing algorithms (notably fq_codel) on top.
  
  This has appeared in multiple commercial products (ubnt edgerouters as “fq_codel), rebranded as “Streamboost”, Netgear “Dynamic QoS”, ASUS (“adaptive QoS”), in addition to nearly every major third party firmware.

  Also fq_codel is now the default queuing algorithm across many modern mainstream Linuxes
- Provided existence proof that these algorithms can be successfully deployed in low end network connected products such as home gateways and CPE.
- Inspired major manufacturers to adopt these changes
- Added these algorithms to major research tools such as ns2, ns3, mahimahi and click
- Inspired ISPs to make these changes – DOCSIS 3.1 has the PIE algorithm standard, and fq_codel was deployed 3 months after it shipped into free.fr’s Revolution V6 equipment.
- Developing a successor algorithm (cake), which takes care of edge cases like ethernet offloads, further CPU reductions, and added support for classification and more robust fair queuing.
- Arranged for DNSSEC support to appear in the most common (1b users) DNS forwarder, dnsmasq
- Worked with the OpenWrt communities to make signed, secure remote updates possible
- Spawned the IETF AQM working group
- Influenced the IETF homenet working group – helping develop and test all the code in the relevant ipv6 related RFCs.
  
  - In particular the routing protocol hardened in CeroWrt (babel) is now mandatory to implement in order to be compliant with the homenet standards.
- Helped make many improvements to TCP across the linux and BSD stacks
- Dramatically reduced latency under load everywhere it could be easily fixed
- Helped provide router code for the Bismark project, and ultimately the broadband america studies
- Spawned 450+ papers on the subject
- Developed measurement tools such as “flent.org”, as well as inspiring large studies of the problem via measurement sites such as dslreports.com. Project Bismark, Measuring Broadband American and others.