Dear FCC,

Mandating (or even encouraging) the lock-down of router firmware is, I suggest, a terrible idea for the following reasons;

a) Chip vendors and router manufacturers will see a financial benefit in this, if they control the firmware with an iron fist they get to sell more hardware;
a1) Enforcing price-tiered levels of functionality in devices which differ only in the firmware.
a2) Built-in obsolescence - "gotta buy a new router to get X"

While both of these are legal business strategies, effectively enforcing them with regulation is not the job of the FCC and is against consumer interests.

b) A substantial percentage of factory router firmware has been found over the years to suffer from individual security issues and implementation bugs; furthermore the near-universally adopted standards of WPS & WEP turned out to have catastrophic security flaws meaning those devices are essentially "wide open" to external attackers and hence not just obsolete but downright hazardous to deploy. If they cannot be upgraded they must be thrown away and replaced.

Manufacturers have an *appalling* track record of releasing security fixes for even current-model hardware, let alone old ones - they have absolutely no motivation to do so as they can profitably sell brand new devices to users instead.

Personally I install OpenWRT or DD-WRT on all my devices and will not buy a new router unless it's supported by those builds. I will only deploy devices with open source firmware to ensure security, flexibility, features and especially upgradeability.

c) At present some manufacturers (e.g. Buffalo, Linksys) are motivated to ship their devices with upgradable open-source firmware as a selling point; they are aware there is a useful portion of the market who view this as a significant advantage in a product and they wish to capture those sales - the epitome of the free market at work. However, if all manufacturers are encouraged (or mandated) by FCC regulations to employ technical measures to prohibit installation of user-supplied firmware, they have no motivation to compete in this way - natural market forces will be distorted by regulation.

It's worthwhile to note that to be effective in preventing user-reflashing of consumer devices, technical measures must be taken wifi chipset manufacturers (of which there are maybe six worldwide) NOT the dozens of router vendors. If the FCC mandates the implementation of secure bootloaders and chain-of-trust for devices sold in the USA it will - without a shadow of a doubt - have a chilling effect on every citizen of every country.

d) There are literally tens of millions of routers already deployed which are readily reflashed with user supplied firmware. If a user desires to modify a wifi router such that it operates outside the strict lines drawn up by FCC regulations, it will always be possible (to some degree, see next point) - this genie cannot be put back in the bottle.

e) FCC regulations already strictly define the capabilities of consumer RF products. While it is true that many common devices may be reprogrammed to operate slightly - and only slightly - outside the public frequency bands allocated by the FCC, it is most uncommon that they may be software modified to a degree that causes real world issues. The reasoning here is fairly simple - significantly extending the usable frequency range or substantially increasing the TX power of a device beyond legitimate levels requires adding extra components to a device and hence increased manufacturing cost, yet the device cannot be sold in a form that makes use of them.

f) There are a very small number of wifi devices sold that do contain power

amplifiers capable of transmitting at levels significantly beyond FCC regulations, however these are essentially "pirate radio" devices and will continue to be available "under the counter" (e.g. mailed direct from China) regardless of FCC rules, much as illegal Cellular and GPS jammers are still obtainable. There can be no doubt that such devices will where possible ignore any FCC ruling about locked-down firmware much as they ignore rules about TX power, hence additional firmware regulations will simply damange the interests of legitimate users (as argued above) while having no effect on "pirate wifi" operators.

h) It is also well worth mentioning that in real world situations it is very rarely even useful to run a wifi router outside FCC limits!

With the sole exception of a tiny number of home-made point-to-point data links (which almost without exception use highly directional antennas - a good thing), practically all wifi routers are utilized to interoperate with off-the-shelf laptop computers and (ever increasingly) smartphones, both with integrated wifi which is almost NEVER modified by the user.

Modifying router firmware to operate anywhere outside the licensed frequency bands simply makes the router invisible - and hence destroys interoperability - with any legitimate wifi device. It's just not a useful thing to do in practice!

Secondly, increasing TX power of a router is largely a fool's errand because - although the router's SSID may be visible over a wider area - a two-way connection is not possible as the return signal from legitimate devices at longer ranges is beneath the noise floor of the router. There is of course no way to "hack" a wifi device to increase its receive sensitivity - manufacturers always ship hardware operating at the technical limit of its RX capabilities.

i) This discussion is about the 2.4Ghz and 5Ghz bands which are very significantly attenuated by physical obstacles (and the atmosphere) and do not propagate widely. Furthermore those bands are already extraordinarily heavily used by legitimate wifi devices (and bluetooth, microwave ovens, baby alarms, etc) and clearly will always remain so. They are a true digital "citizen's band" and provide literally incalculable benefit to those citizens (far beyond what the old 27Mhz CB band ever did).

In summary:

I applaud the effectiveness of the FCC in policing the RF emissions of devices sold to consumers, however mandating locked-down software in such devices is futile, dangerous and anti-competitive as arged above.

I urge the FCC to consider the fact that the effectiveness of current frequency band & TX power regulation in consumer mobile devices (laptops, tablets & phones) - which are almost never software-modified - makes almost all "router hacks" of tx band & power useless as they naturally break interoperability. The number of rogue operators running hacked firmware on BOTH ends of a wifi link are in practice absolutely miniscule.

Thank you for your consideration of these points,
Sincerely,
Richard Aplin