

I strongly oppose this rule change.

I find this whole argument with Marriott about security and safety to be a joke.

I used a well-behaved (i.e. no malware) laptop on vacation in 2013. I used it exactly once, to connect to my desktop at home via RDP on a hotel's WiFi system. I connected with the credentials I was given, the only browser pages that was exposed on that laptop belonging to the hotel. I then RDP'ed into my desktop and proceeded to do my business on it, not the laptop. When we arrived home from that vacation and started using the laptop on our home system, it was acting very peculiar, and my wife ran a malware scan and found that malware had indeed been installed on the laptop. The date was the date that we had connected to that hotel's WiFi. Neither my wife or I was impressed. Nor were we impressed with the response we received from the hotel chain when we reported it to them. Which boiled down to "tough cookies". I will withhold the name of the chain, but a) I never plan on staying there again, ever and b) if I do have that kind of need again, I will tether my cellphone to the laptop to avoid problems like that. And Marriott would certainly (try?) to take away my second plan.

When a hotel can not even make sure that it's login page and/or landing page after login do not contain malware, I don't understand how blocking other WiFi radios will make ANYBODY secure.

Also, I do not believe that security and children are the real driving matter of this. It is flat out to make sure that they can get their usurious fees for using their WiFi.

The unlicensed network is doing what it should be doing under the current rules. I see zero need for those rules to be changed just so that a big corporation can make sure that I turn even more of my hard earned money to them for absolutely no real reason at all.

Nobody should be able to block "unwanted" unlicensed networks just because they pass through or on their property.