

Dear Commissioners,

## Overview

The Proposed Rule 80 FR 46900 will, as written, have a number of serious adverse impacts on society, as summarized here and discussed later in this submission:

1. It will have a significant adverse impact on the ability of individuals and corporations to control devices they own in ways unrelated to RF parameters, which will have serious flow on security, civil rights, and productivity implications for society.
2. It will hamper legitimate research which poses no radio spectrum concerns.
3. It will hamper legitimate commercial activities, causing a significant economic cost.

These serious adverse impacts are not justified on the grounds of minimizing interference because, as summarized here and discussed later in this submission:

1. It is not the best option for preventing unintentional operation causing interference.
2. It is not an effective solution for preventing intentional operation using unauthorized parameters.

As this proposed rule-making will have serious adverse impacts on society and will be ineffective at achieving its policy objectives, I recommend that the FCC abandon the proposed rule-making and the policy objective behind it, and look at alternative approaches to limiting harmful interference.

## **Adverse Impact on the ability of individuals and corporations to control devices they own in ways unrelated to RF parameters, which will have serious flow on security, civil rights, and productivity implications for society**

Many individuals and corporations modify wireless devices for a number of legitimate reasons that are not related to making unauthorized modifications to RF parameters. Popular after-market firmwares such as DD-WRT and OpenWRT can be installed on wi-fi routers to enhance the functionality of devices - for example, allowing for more advanced network configuration, stronger authentication and security, and features such as wi-fi hotspots and ad hoc networking. The intention of these modifications is to affect layers of the network above the physical (first) layer that is regulated by the FCC.

These legitimate modifications deliver significant value to businesses and consumers. They can help to improve network security, allowing owners to make more conservative security choices and protecting against criminal activity. They allow people to operate systems without fear that manufacturer supplied backdoors are monitoring their activities. They reduce waste by allowing devices no longer supported by the manufacturer to be updated to support new features. They allow people to tinker at higher layers of the networking stack (in ways that comply with all FCC rules), supporting education and innovation.

## **Adverse impact: Hampering legitimate research which poses no radio spectrum concerns**

Modified wireless devices can provide a platform for experimental technologies. They provide a convenient development platform containing a microcontroller / microprocessor / system-on-a-chip, with wireless connectivity devices for legitimate research. This research does not result in harmful interference, and so should be promoted and not hampered by the FCC.

## **Adverse impact: Hampering legitimate commercial activities, causing a significant economic cost**

Modified wireless devices can deliver better services to the public than a standard product available at a similar price. For example, modified devices could become a hot-spot using Open Source software such as ChilliSpot, improving public access to technology through a commercial hotspot. It could enable support of enterprise authentication, allowing it to be used for employee access in a commercial environment. Allowing these upgrades without the permission of the manufacturer allows hardware to be used, with the same authorized parameters, to its full potential - even if the manufacturer does not wish to allow that lawful usage to force certain customers to use a more expensive product. Due to the hardware being able to be used fully in a way that the businesses owning a device have control of, businesses can operate efficiently with lower costs.

## **Policy problem: It is not the best option for preventing unintentional operation causing interference**

Creating and flashing custom firmware to a device, or changing RF parameters is an inherently technical process that requires some degree of skill and knowledge. Someone with knowledge to complete such a process would be unlikely to unintentionally configure the system to use a different regulatory domain.

If the regulatory intention of the rule-making is to protect against unintentional unauthorized operation, the same policy objective could be achieved without the adverse impacts by a requirement that a legal warning be displayed before allowing firmware to be updated or parameters to be changed to values that are not approved for usage in the US.

## **Policy problem: It is not an effective solution for preventing intentional operation using unauthorized parameters**

If the intention is to prevent the intentional operation of equipment in a manner which will cause unlawful interference, a better solution would be to continue with post-hoc enforcement. Attempting to stop intentional interference by 'locking down' software on SDR (software defined radios) and non-SDR devices will be futile for the following reasons:

1. This rule would create an inherent inconsistency between basic devices that do not include a significant software component (for example, 802.11a/b/g/n wi-fi USB sticks based on the popular Realtek RTL8187 chipset family) and are connected to a general purpose computer, and more complex devices which include the same radio hardware components along with an embedded processor. The general purpose computer plays roughly the same role as the embedded processor - both can configure the regulatory domain and set RF parameters,

some of which may cause harmful interference if used in the US. The basic devices can only achieve their price point in their market by not including complex and expensive programmable components and by exploiting efficiencies of scale, allowing them to be sold globally under different regulatory domains. Banning the basic devices would cause economic harm and reduce access to technology. Locking down the software on a general purpose computer would cause immense economic damage and go far beyond the legal powers of the FCC. Therefore, there is no reasonable way to, by prior restraint, control the software controlling a basic device connected to a general purpose computer. As long as that combination exists, requiring that software on a complex approved device connected to the equivalent hardware as in the basic device is futile in preventing deliberate unlawful operation.

2. It is very likely that anyone wishing to intentionally operate a wireless device outside of approved parameters will be able to purchase a similar device without the restrictions from overseas, and that a significant number of travelers will, in fact, import such devices with their personal computers when traveling. There is very little the FCC could reasonably do to prevent this in practice without causing damage to the reputation of the US as a tourist destination.
3. Unless access to electronic components are restricted, someone wishing to intentionally operate a wireless device in contravention of the law could build their own device. Restricting access to electronic components would be inconvenient for many, and would slow innovation and hamper education.
4. It is likely that any security measures could be circumvented by someone determined to circumvent them with physical access to the device. Securing a device against someone with physical access to that device is virtually impossible and attempts to do so are potentially very expensive.

Your Sincerely,  
Dr Andrew Miller