

Dear FCC,

**Summary:**

This draft KDB provides a useful guidance for ensuring product compliance in multiple markets using the same hardware and software but with different regulation. It seems however that this KDB aims to solve non-compliance issues on the US market by putting additional requirements on already compliant equipment. One example is the requirement for a WLAN client to ensure that the access point is used in an indoor location. Such information is not possible for any client device to ensure.

Below you will find more specific comments to the parts where we see a potential issue in our current line of products. All our products are aimed for consumers and does not provide any possibilities for end users to change the software. Location data is directly received from the products internal design and can not be potential changed by end user settings.

**Client device operations control**

4a defines the rules for a master device and it's clear that such device is not allowed to be manipulated in any way for allowing unauthorized band usage nor RF power levels.

4a defines the rules for a client device as of section 15.202.

This writing is basically putting additional requirements on all products using WLAN as client devices. Only a few of this product categories has the possibility to use additional sources for determine the correct area for compliance settings. Many consumer products are today using WLAN and are portable for use in different locations. Different game products and portable computers are typical products where no additional information can be received except from the master device they connect to. They are also designed to cover the full range of WLAN channels on the 2.4 GHz band and mostly they have active scanning on channels 1-11 and passive for channels 12-13.

Second bullet is referring to different supplemental information such as geo-location data and refers to one or more of the following:

- Global navigation satellite system or
- MCC and MNC or
- other suitable geo location data based on IP address

This is somewhat unclear as the bullet refers to one or more of the listed methods while the each listed method seems to be sufficient by it self as by adding "or" after the two first one. It needs to be clarified if only one method is required or if additional methods need to be used as well. And if so, what are the criteria that must be fulfilled by the geo-location data in order to determine if only one method is sufficient or additional methods must be used as well.

Using IP based geo-location data is only possible if you have actually been connected to a network. In such cases you must presume that the connection is in compliance with the regulation and the IP based geo location data is in principal useless.

## **MCC and MNC**

From this we understand that using MCC and MNC to determine if the geo-location data is an acceptable option for FCC at least for determine that the location is outside of USA as the default setting must be FCC compliant. If the product only need to determine the geographical area for its operation it's sufficient to use only. We propose that the wording is changed to reflect this. (... with the use of MCC.....)

4.c.i is referring to a clear operational descriptions of failsafe mechanism to address reception of conflicting codes within USA. Our understanding is that this refers to reception of non USA MCC information while located in USA. In such cases there is a risk for a changed RF settings based on if the received MCC information is valid code. If the code is not valid a default settings to FCC compliance would still be valid. In case of a direct faulty MCC information transmitted by one base station can cause RF settings to be changed to a non-compliance setting inside USA. This should however be corrected by receiving additional MCC information from other base stations in the area.

It's unclear on what type of fail safe precautions that can be accepted under this circumstances. Using geo-located data can of course be used but it might also be blocked by end user settings and should only be seen as a complement and not a failsafe handling.

## **5.1 GHz devices**

4b ii refers to client devices in 5.1 GHz band. They must determine that a master device is located at an indoors location. It's very unclear how a client device can control that the master device is in compliance to the FCC regulation.

A portable device can be prevented to act as a master device unless it's connected a mains charger. This will of course be a primary requirement for approving portable master devices. It must however be a requirement on the master devices to only have the possibility for indoor operations. It's not possible for a client device to determine if the master device is in compliance to the current regulation.

The only way for a client device to ensure this is if the client user can locate the master device and ensure it's placed in a correct environment. In practice, no end user will ensure this. Putting an administrative requirement on the end user by different type of statements in the user guide is in addition causing more confusion at the end user as the device is only capable of connecting to an approved master device. Please see also previous submitted KDB inquiry, tracking number **584204**.

We strongly recommend that this requirement is removed. (*"For client devices operating under the control of a master must ensure that the master device is operating indoors."*)