

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Amendment of Parts 0, 1, 2, 15 and 18 of the Commission’s Rules Regarding Authorization of Radiofrequency Equipment)	ET Docket No. 15-170
)	
Request for the Allowance of Optional Electronic Labeling for Wireless Devices)	RM-11673
)	

To: The Commission:

**Additional Reply Comments of Nickolaus E. Leggett, Certified Electronics Technician,
Amateur Radio Operator (N3NL), GROL Licensee, Inventor, and Analyst**

I am a certified electronics technician (iNARTE and ISCET) and an Extra Class amateur radio operator (call sign N3NL). I also hold an FCC General Radiotelephone Operator License with a Ship Radar Endorsement. I am an inventor holding three U.S. Patents. My latest patent is a wireless bus for digital devices and computers (U.S. Patent # 6,771,935). I have a Master of Arts degree in Political Science from the Johns Hopkins University.

I am one of the original petitioners for the establishment of the Low Power FM (LPFM) radio broadcasting service (RM-9208 July 7, 1997 subsequently included in MM Docket 99-25). I am also one of the petitioners in the docket to establish a low power radio service on the AM broadcast band (RM-11287). I have filed a total of well over 200 formal comments with the FCC over the years since the 1970s. I have filed comments with other Federal agencies as well including the USPTO, NASA, FAA, FERC, EPA, and the TSA.

This is my additional set of reply comments responding in general to the comments filed in this docket. Many of the problems with sealed technology have not been addressed in the comments filed so far. These comments address these problems.

Reply Comments – Liability Aspects

Depending on the scope of the rules, blocking the user or owner from having the authority to service his equipment (either directly or through third-party maintainers) probably transfers liability issues to the manufacturer since the user is locked out of servicing his equipment. This is of special importance if the equipment must operate very reliably and must be serviced rapidly. Examples of this situation can be seen in hospitals, emergency responders, air traffic control, railroad dispatching, crop harvesting, etc.,

Guaranteed Points of Failure

Blocking users from servicing their equipment leads to a situation where numerous service technicians in the market place are replaced by a very limited set of service technicians working for the equipment vendor. This narrowing of the service capability cripples the capability of the owners' communications system and reduces the effectiveness of their communications.

The lack of authorized service technicians makes the equipment more vulnerable and it reduces the ability to respond to major emergencies up to and including solar geomagnetic storms and electromagnetic pulse (EMP) events.

Increased Opportunity for Criminal and Disruptive Activity

Since the servicing and modification of the equipment is restricted to the vendor's technicians, there will only be a limited set of technicians who can detect and defeat the intentional misuse of the equipment. This would provide some additional opportunities for

organized crime as well as other bad actors. These criminals could blackmail the legitimate users of the equipment by shutting down the equipment remotely unless a payment or cooperation is provided. Criminals could sabotage the equipment remotely as a service for competitive purposes. There would be a seriously reduced set of knowledgeable technicians to counter these actions.

Similar actions could be taken by nation states and by sub-national organizations for political power purposes.

Increased Hardware Hacking and Violation of the Law

Demand for quick maintenance will lead to a growing underground economy of technicians breaking open sealed technology. This underground economy will operate without any government oversight and without any taxation by the Internal Revenue Service (IRS). In addition, there will be a growing disrespect for the law and regulation similar to what happened during Federal prohibition of alcoholic beverages.

The de-facto criminalizing of independent servicing of equipment will motivate talented service technicians to work for organized crime. This will increase the technological capabilities of organized crime and make it far harder to control. Organized crime will be attracted to criminal use of the radio spectrum. Technologies such as spread spectrum and encrypted transmissions would support these criminal uses. These technologies could be combined with other new technologies such as small-scale armed drones. This type of radio-controlled drone has been built and publically demonstrated.

Monopoly Consequences

Independent equipment servicing companies, as well as equipment owners, will bring litigation cases to court. They will challenge the practice of restricting servicing to the vendor's

own agents. These cases will challenge the restriction on servicing as an adhesion contract that unfairly limits the rights of the equipment owners and the rights of independent service companies. Over time, the number of cases will increase due to the vendors' inability to provide quick service throughout the nation including widespread rural areas as well as urban areas.

Even governmental organizations will be vulnerable to pressure from vendors who operate sealed technologies. Some of these vendors will be foreign-owned corporations that will have special leverage with the American government.

Government Control of Monopoly Suppliers of Servicing

Government will need a new regulatory structure to control the monopoly suppliers of maintenance services. The following specific controls are essential.

1. Automatic shutdown of inadequate monopoly suppliers of maintenance services.
This should be due to an inability to supply rapid service to the customer base.
Also in cases of national security, the monopoly needs to be disabled.
2. Blocking of failed monopolies from the market place for a specified number of years.
3. Restoration rules and standards for failed monopoly suppliers that want to return to the market place.
4. Mandatory supply of software bypass modules to the equipment owners for emergency situation override of sealed technologies.
5. Override of monopoly service suppliers for national defense and infrastructure defense purposes.

Respectfully Submitted,

**Nickolaus E. Leggett, N3NL
1432 Northgate Square, #2A
Reston, VA 20190-3748
(703) 709-0752
leggett3@gmail.com**

November 3, 2015