Please accept my comments against RM-11831. There are a number of issues with this petition. I have identified and addressed a few of them below.

Demanding all communications be interceptable by saying “software provided by developers must be open source, unencumbered by patent, licensing fees, royalties or copyright” will dramatically hamper progress. This eliminates many modern data modes and most voice modes. It’s simply an impractical standard. The days of hams soldering radios together is past. Now the goal is to build these into systems. DSTAR started as a sole-sourced product, now there are radios gateways and networks that use none of the original OEM hardware and software. The amateur implementation of DMR has seen similar development. If one truly wants to monitor Winlink traffic, decoding it over the air is the least efficient solution. Hosting a gateway will support the community and all the traffic will be available for review.

Pactor is quite effective but has not been popular for amateurs because of the high cost. This has created motivation within the amateur community to develop newer modes to replace it. As a result, we now have Winmor, ARDOP and VARA modes as options. These developments are in the best tradition of one of the fundamental principles of amateur radio, “Continuation and extension of the amateur's proven ability to contribute to the advancement of the radio art.” as stated in part 97.1(b). These developments are despite the antiquated symbol rate rules.

Conflating encoding and compression with encryption is either ignorant or disingenuous. Calling these “effectively encrypted” (per Prof. Rappaport) does not represent the rules as defined in part 97.113(a)(4). There is no intention to obscure the message, just transmit it efficiently. Any information security expert is quick to point out “security through obscurity is no security”. Pointing out that Winlink can be HIPPA compliant does not prove that it’s encrypted but how little it takes to satisfy HIPPA.

Using amateur radio to bypass commercial Internet services is absurd. How many would seriously substitute megabits of bandwidth for a 1200 baud Winlink email connection? This isn’t done to avoid a commercial service, it’s done because that’s the only thing available, practical or to learn and practice the technology.

Interference exists at time with all modes on all bands. As more modes become available, this is likely to increase. This is a reason to increase focus on this issue and learn to use the big knob on the radio. Eliminating a mode to eliminate the potential for interference is not a practical solution. Otherwise, we should simply surrender our licenses. Digital mode developers make efforts to insure this doesn’t happen but there are limitations. Adding this issue to the licensing questions pools seems a more effective venue for addressing this issue since the petitioner is concerned that amateurs remain self-policing. I haven’t seen any questions on this topic in the question pools when teaching licensing classes.

Using the protection of emergency communications to justify the elimination of one of the most effective tools for emergency communications is ridiculous. Emergency communications are complicated by a huge number of factors; failed repeaters, power outages, noise from local equipment, lack of trained and credentialed operators, shortage of equipment, insufficient bandwidth, interference from adjacent operations, etc. We spent quite a while during a recent federally declared disaster tracking down interference on interoperability channels. I have never experienced this on the amateur bands during an incident. The possibility that some random digital mode might cause interference is a small price to pay for the utility of these digital modes during a major incident. Dismissing this will allow amateurs to remain effective emergency communicators as stated in part 97.1(a).

Scott Honaker, N7SS

Communications Coordinator

Snohomish County (WA) Department of Emergency Management