

FCC RM 11699
ENCRYPTION OF AMATEUR RADIO COMMUNICATIONS

Comments of Mark Richards, K1MGY
9 July 2013

I believe that this proposal has merit when the “Basis and Purpose” of the Amateur Radio Service is considered. Part 97.1(c) states this as, “Encouragement and improvement of the amateur service through rules which provide for advancing skills in both the communication and technical phases of the art”. Part 97.3(4) defines the Amateur Service as, “A radiocommunication service for the purpose of self-training, intercommunication and technical investigations carried out by amateurs, that is, duly authorized persons interested in radio technique solely with a personal aim and without pecuniary interest.” The use and further development of encryption methods do not appear to conflict with these principles, yet this concept is not advanced by the Petitioner nor remarked upon by the ARRL in its comments of 8 July 2013.

Unfortunately the development of the Petitioner’s ideas have not matured to a level which the Commission would likely view as compelling. Such maturation might best take place within the entire community, led by the ARRL or other national group.

The League mentioned their 2005 study which examined (a) whether HIPPA requires encryption and (b) whether medical information transmitted via Amateur Radio in an emergency should be protected. It is not known if the League argued in favour of experimentation and technical investigation by licensed Amateurs in its inquiry.

The ARRL sets forth its arguments against the proposed rule in Part VI of their filing. I believe that the following are most relevant:

1. No Expectation of Privacy

The League leans upon the understood premise that there is no expectation of privacy in Amateur Radio communications, while the petitioner suggests that in certain circumstances a necessity for privacy may exist and should be supported. The proposal for use of encryption between two or more stations appears to be a means of bridging this gap. That there is no expectation of privacy does not preclude the reasonable development of means which would secure such privacy, provided these are used according to current limited purposes.

2. Obscuring the Meaning of Communications

The DSTAR Codec, a proprietary encryption method, is the basis of many VHF and UHF Amateur Radio communications systems. Lacking the necessary hardware, DSTAR most effectively obscures the meaning of communications. The only difference between DSTAR and the use of other encryption methods is that in the former the encryption key may be purchased and used by any person. The type of encryption as proposed by the Petitioner would instead only be available to those who possess the key by which the transmission was encoded, and this key would be in the exclusive control of the

transmitting station.

Encryption therefore only obscures the meaning of communications where the encryption key (used to decode the communications) is unavailable.

Locks, as we well know, only keep the honest at bay and as other comments have noted come in many forms (a simple WEP key, for example, can be decoded using published technique). A sanctioned and published encryption method would provide for monitoring of communications by those with technical ability.

3. **Encryption .v. Obscuration**

The distinction between encryption to (a) obscure the meaning of a message and (b) to prevent unauthorized access seems one of semantic; relevant to the intention of the encryption itself. As the League suggests, the current regulations appear to provide some wiggle room for a subjective analysis on the part of the licensee. Clarity on this point might be better found through specific language rather than a pile of court cases, and therefore is encouraged.

4. **Self-Regulation**

In my experience the Amateur Radio community in a public service role already maintains vigilance as to the transmission of personal information related to health matters. In recent events in which I participated (notably the 2013 Boston Marathon), only the participant's "bib" number could be transmitted. Amateurs were briefed on the necessity to obscure name and other personally-identifiable information in their transmissions. Although the current health privacy law is both stringent and, as the League points out, primarily applicable to health care providers, the potential of civil action against first responders (beyond the alleged shield of "good Samaritan" status) is ever-present. I believe such a dark cloud, combined with common sense, is sufficient to provide self-regulation and prudent communications. In a national emergency of the type the Petitioner suggests, such concerns for health information privacy will naturally be balanced against exigencies.

The Amateur Service is one which robustly supports experimentation, yet in the area of encryption for other than currently-permitted use, or development of encryption methods or application of existing technique, furtherance of the art appears to be disallowed. As the Commission considers the proposed rulemaking, I would encourage consideration beyond the limited and somewhat untested arguments that the Petitioner put forth in order that current rules are strengthened and the foundations of the Amateur Service as to experimentation and development of the Art be considered.

Mark Richards
K1MGY