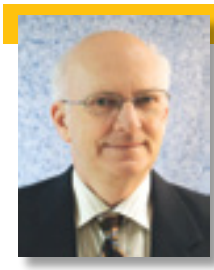

It Seems to Us

David Sumner, K1ZZ — dsumner@arrl.org
ARRL Chief Executive Officer

Privacy

"The issue of privacy — or the lack thereof — in electronic communication has been much in the news recently. It may be worth a reminder that there is no expectation of privacy *in Amateur Radio communication."*

From its earliest days radio has been used to transmit sensitive information — yet by their very nature, radio transmissions are subject to unauthorized interception. Any emission of radio frequency energy can be detected and its information content, if any, extracted.

The International Radiotelegraph Convention signed in Washington in 1927 obligated the participating governments to take steps to prevent unauthorized reception and transmission of "correspondence of a private nature" as well as the "unauthorized divulging of the contents, or simply of the existence, of correspondence which may have been intercepted by means of radio installations" as well as the "unauthorized publication or use" of such correspondence. Today's Radio Regulations of the International Telecommunication Union (ITU) contain a similar obligation with regard to "radiocommunications not intended for the general use of the public."

The Communications Act of 1934 implemented this obligation but with a specific exception for radio communication "transmitted by amateurs or others for the use of the general public." In 1982 this was amended to exempt all radio communication "transmitted by an amateur radio station operator or by a citizens band radio operator." As explained in the October 1982 issue of *QST* the reason for the amendment was "to facilitate the use of volunteers by the Commission to monitor for violations of the Commission's rules." Prior to that time it could have been argued that someone hearing a violation could not report it to the FCC or to anyone else unless the transmission was intended for the general public, which in itself would have been a violation of the rule against broadcasting. Thus, at least in the United States there can be no expectation of privacy in Amateur Radio communication. Some drug smugglers found that out the hard way when their efforts to suppress evidence gathered through interception of their radio transmissions failed to win judicial favor.

But there's more. The ITU Radio Regulations used to require that international communications by amateur stations "be made in plain language." The FCC's amateur rules of that era contained an entire section prohibiting "codes and ciphers in domestic and international communications." Since then a substitute for the "plain language" reference has been adopted: In 2003 the ITU rule was changed to "Transmissions between amateur stations in different countries shall not be encoded for the purpose of obscuring their meaning." The FCC rules were amended in 2006 to conform to the new international text but the prohibition still applies to domestic communications as well as international. So, not only are Amateur Radio transmissions not protected by law against divulgence or use by others; amateurs are also prohibited from taking steps to cloak their meaning.

In general, the principles on which these rules are based are broadly supported by amateurs — or at least, not objected to. Amateurs are very protective of the non-commercial nature of our radio service and appreciate the fact that the FCC is equally so. The ability to decipher transmissions in the amateur bands is important to guard against abuse, either by amateur licensees or by interlopers. There are limited circumstances in which the FCC rules permit encryption, either explicitly (in the case of telecommands to amateur satellites, telemetry from satellites and signals to control model craft) or implicitly (to authenticate the identity of stations in a message forwarding system). Otherwise, amateur communications must be an "open book" to listeners.

Are there additional situations when the encryption of message contents might be sufficiently desirable to outweigh our strong preference for transparency? The FCC report to Congress in response to Public Law 112-96 noted that some commenters in the proceeding, GN Docket 12-91, argued that "transmission of sensitive data, such as medical information that is subject to privacy requirements, is often a necessary aspect of emergency response, and therefore the use of encryption should be permitted under appropriate circumstances, such as by credentialed operators." The report went on to observe that this issue could be addressed through the Commission's rulemaking process.

At its March 9, 2013 meeting the ARRL Executive Committee requested that a briefing paper be prepared detailing the significant aspects of the encryption issue, particularly with respect to privacy concerns and the Health Insurance Portability and Accountability Act (HIPAA). Soon thereafter Don Rolph, AB1PH submitted a well-crafted Petition for Rulemaking to the FCC seeking an additional exception in emergency operations or related training exercises. In June the FCC assigned it a file number, RM-11699, and opened a 30-day window for public comment.

In preparing the briefing paper for the Executive Committee the ARRL General Counsel and staff confirmed that the HIPAA regulations do not require encryption of radio transmissions of medical patient information. Therefore, HIPAA is not by itself a sufficient rationale for such an exception. After consulting with the rest of the ARRL Board the Executive Committee concluded that there is insufficient justification for the proposed change and instructed that comments on behalf of the ARRL be filed accordingly. This was done, as reported in "Happenings" in last month's *QST*.

While HIPAA may not require encryption of radio transmissions it is clear that medical care providers are very protective of patient privacy. Information identifying a patient is seldom transmitted anyway. Our served agencies may well prefer that the messages we send on their behalf not be intercepted by unknown listeners. If so there are steps we can take such as using less-popular frequencies, directional antennas, minimum power and voice modes other than FM that will greatly reduce the likelihood of eavesdropping.