digital connection

BY DON ROTOLO,* N2IRZ

Data Encryption is Legal!

Just like Dorothy returning to Kansas, it turns out we've been able to do it any time we wanted to. Data encryption for our intended purposes *is already permitted* under Part 97 of the FCC rules. We just hadn't realized it. Read on for the details.

Data encryption has been a hot topic for some time in the digital community. We discussed both sides of the issue in the past two columns. In this month's column we'll be putting the topic to rest, once and for all.

The basic point is that our ham bands are not *meant to be secure against casual listening.* However, when we are providing communications for some agency or organization, such as for disaster relief, those agencies have some expectation of confidentiality. Information about people, as well as movement of supplies and resources, is not meant to be heard by the general public. Unlicensed Part 15 users are afforded the opportunity to encrypt this information to protect privacy, so why not Part 97 users?

Until now, the "common wisdom" has been that Section 97.113(a)(4) of the FCC rules, which prohibits *"messages in codes or ciphers intended to obscure the meaning thereof, except as otherwise provided herein...,"* made it illegal for hams to encrypt any information that wasn't specifically exempted, even passwords to prevent non-amateurs using Part 15 devices on shared frequencies from accessing Part 97 networks, even though another paragraph of §97.113, paragraph (e), says that except for a few specific exemptions, *"No station shall retransmit programs or signals emanating from any type of radio station other than an amateur station..."*

Paul Toth, NA4AR, a member of the ARRL's High-Speed Multimedia (HSMM) Working Group, a former ARRL Section Emergency Coordinator, and a recipient of the 2005 NOAA Environmental Hero award for his volunteer amateur radio work at the National Weather Service office in Ruskin, Florida during the 2004 hurricanes, posed some arguments for allowing limited encryption, which are excerpted here:

> Commercial Part 15 operations have brought with them many benefits to society. Wireless networking has enabled greater use of the Internet and the volumes of information that are available there ... IEEE 802.11 devices, wireless telephones and dozens of other types of unlicensed, Part 15 radio emitters have become so pervasive they now number in the tens of millions. And that is just in the United States.
>
> 802.11 Wireless Access Points (WAPs), by default, are configured to act as repeaters. Most of these Part 15 WAPs are equipped with security features that comply with IEEE standard 802.1x to limit access. When enabled, these 802.1x security features will repeat only those operators whose stations meet the encrypted access authentication criteria programmed into the WAP. Part 15 operators are free to use 802.1x security as well as WEP and WPA to limit access to their WAPs. Amateur Radio operators operating WAPs under Part 97 rules without encryption switched on are likely to violate 97.113(e) by inadvertently re-transmitting Part 15 signals. But 97.113(a)(4) prohibits encryption.
>
> Two years ago, before Charley, Ivan, Katrina, Rita, Wilma, and the other hurricanes that made landfall in the US in 2004 and 2005, the ARRL Board voted unanimously to petition the FCC for a rules change on encryption. The proposal sought to legalize the use of "industry-standard security and encryption protocols" for *domestic* communications on all bands above 50 MHz. Such a change in the rules would allow amateur operations to utilize spectrum shared with commercial operators without fear of violating 97.113(a)(4) or 97.113(e) and address the growing need for secure disaster response communications. However, at its January 2006 meeting, after hearing a report from ARRL General Counsel Chris Imlay, W3KD, on "the background for and implications of moving forward with" filing such a petition, the ARRL Board effectively rescinded its earlier motion, voting "to relieve the General Counsel of the *requirements*" to seek a rules change on this matter. Meanwhile, FEMA and the Department of Homeland Security have sought out organizations like Part15.org to explore emergency communications contingencies on frequencies licensed to the Amateur Radio Service.
>
> No one is suggesting relocation of Part 15 users to other radio spectrum. Hams, of course, are just as free to operate an 802.11 or 802.16 station under Part 15 rules as are non-licensees. But why should we? After all, we hold licenses to operate on these bands. That license is supposed to afford Amateur Radio operators priority as well as the privilege of operating with higher transmitter power than Part 15 operators. What is holding hams back are antiquated rules written without recognition of the mixed spectrum utilization now in place. A change in the rules to permit the use of industry standard security and encryption protocols on domestic transmissions can, once again, open these bands to those who hold a license to use them.

After reading Paul's comments, we at *CQ* began some follow-up work to try to tie up loose ends. The result was that a variety of strings began to come together, leading to the conclusions presented here. My thanks to Paul for his willingness to share his thoughts and keep the issue on the table long enough to get the ball rolling. Let's review Paul's basic points and how they led to a rather startling conclusion:

It's Been Legal All Along!

Note: The following was developed from a series of discussions, both public and private, with numerous hams, including some with authoritative knowledge on these matters who asked not to be quoted at this point, as the discussions were

*P.O. Box 114, Park Ridge, NJ 07656
e-mail: <n2irz@cq-amateur-radio.com>

still ongoing. It started with Paul's comments above and reaches the conclusions below. While it would be impossible to acknowledge everyone involved, much of the credit goes to the members of the High Speed Multimedia (HSMM) Working Group.

Paul's primary point in advocating encryption under Part 97 is the need for *network security,* which is to prevent non-hams from accessing amateur equipment (inadvertently or on purpose), which could result in a violation of the FCC rules. His conclusion is that some encryption is absolutely necessary for amateurs today. Also, as Paul stated two years ago, the ARRL Board of Directors agreed that it was a good idea to petition the FCC to permit limited data encryption. The digital and emergency communications communities had convinced the directors that such an action would further the Amateur Radio Service. What, then, changed their minds in 2006?

Well, it turns out that there's no need for a petition because **there's nothing in the rules preventing the use of data encryption for the purposes we're discussing,** specifically protecting the network from unauthorized intrusion and usage, as well as the more general purpose of supporting emergency communications while maintaining the privacy of disaster victims—both in actual emergencies and in practice drills. (That last bit is important: While the emergency communications exemption in 97.401(a) essentially suspends all the rules when necessary, drills are not an emergency, and it is absolutely essential to practice with a system regularly if you expect it to work when there is an emergency.)

Network Security

First, let's discuss network security. What we're trying to accomplish here is to prevent outsiders from accessing the network, as required by 97.113(e) and implied in 97.105 and elsewhere. If this can be accomplished with a password, then there is nothing in the rules preventing us from encrypting that password. I compare that to keeping the control codes for a repeater secret: It is clear to anyone monitoring as to who is transmitting and the general purpose of the transmission, so the exact password that is being transmitted is not that important.

However, more than a password is needed to secure an 802.1x network. WEP (Wireline-Equivalent Privacy), for example, prevents anyone not using the proper key from associating with the

WAP (Wireless Access Point). That means if we enable WEP, we are effectively preventing Part 15 users from accessing—inadvertently or on purpose—a network operating under Part 97 rules.

The *Purpose* is What Matters

The key here is that the *purpose* of encrypting is *not* to obscure meaning. It is to *secure the network* from unauthorized access. Let's take a look at Section 97.113(a)(4) again, which states that no amateur station shall transmit "*...messages encoded for the purpose of obscuring their meaning....*" The key word here is *purpose*. This rule is not regulating a method or practice; it regulates a purpose or intent.

For the communications purposes we are discussing–network security and access control, emergency communications, and practice for same—our *purposes* in using encryption are the *security* of the network and the *privacy* of third-party information. In either case, the purpose is *not* to obscure meaning. We have to assume that the rules were written very carefully, and they mean what they say. It might seem kind of odd that the rules deal with intent, rather than practice, but they are what they are: **If the purpose of encryption is not to obscure meaning, then it is permitted.** This carries over to any encryption method, on any frequency, including HF.

The FCC's main concern is knowing who transmitted a particular signal. Then, if there are problems or questions, the Commission would know whom to contact for more information.

Caveats

Well, there's no such thing as a free lunch. Of course, there are limits to how we carry this out, both operationally and from a practical standpoint.

The first caveat is that nothing relieves amateur radio operators from the requirement to identify their stations, at least every 10 minutes and at the end of each contact. With 802.1x gear the simplest method is to set the SSID to your callsign. If you use something different, you may need to work out some other methods to accommodate whatever system you decide to use.

The second caveat is that you still need to comply with Section 97.309 (a)(4), which states that "An amateur station transmitting a RTTY or data emission using a digital code specified in this paragraph may use any technique whose technical characteristics have been documented publicly...." Whatever encryption methods you use —WEP, WPA, WPA2, or whatever—it *must* be publicly documented. Please note that this specifically means the encryption *algorithm*, ***not*** the encryption *key*. Making the key public is no security at all!

The third caveat is that you should probably refrain from attempting encrypted communications with other countries, since their FCC-equivalents may not permit it. At the very least, tread carefully here.

Finally, it would be good amateur practice to document the encryption key being used in your station logbook, and perhaps also a general characterization of the purposes for using encryption. It would also be good practice, particularly in a real emergency, to maintain copies of transmitted messages for possible future FCC inspection. Most e-mail programs do this automatically, unless you turn off the feature. It would be best to leave it on.

HSMM Leads the Direction

By the time you read this, the HSMM Working Group will have posted some new guidelines for the use of encryption on amateur frequencies. While this was still pending as I write this (mid-June), an update was expected by July. Have a look at the League's website for the latest news.

Again, my thanks to Paul Toth, NA4AR, for continuing the debate on encryption in the ham bands, and to all those I spoke with, especially those on the ARRL's HSMM WG, for the lively, spirited, and very intelligent discussion of this month's topic. The members of ARRL Board of Directors, even if you might not agree with everything they do, should certainly be thanked for their work to reach this point. This didn't happen in a vacuum, and it is only through the hard work of many that the amateur community can now celebrate the best possible outcome for this debate: It's been legal all along, so go out and have fun and/or provide the emergency communications services your community needs and that ham radio has traditionally been able to offer.

Finally, I thank everyone who takes the time to write to me with comments, suggestions, ideas for future columns and yes, even complaints. We're used to two-way communications, and this column isn't any different. See what it did this month?

Until next time . . .

73, Don, N2IRZ