(Some) Encryption is Legal!

By Don Rotolo, N2IRZ, n2irz@worldnet.att.net

In the process of verifying some assertions made by a fellow Ham regarding the need for encryption on the amateur bands, I stumbled across something almost unbelievable: Part 97 permits some encryption, such as WEP on 802.11 gear.

As incredible (literally) as that statement seems, I firmly believe it to be true. Conversations with a highly placed official at the FCC, as well as at the ARRL and in the HSMM working group, support that conclusion. I can't mention any names, because anonymity was requested, but I expect to see a statement on the topic from some credible Hams any day now.

The basic premise is that Part 97 is unusually vague and specific at the same time. In virtually every case, Part 97 discusses practice and performance, but in Part 97.113(a)(4) it specifically prohibits "...messages encrypted for the purpose of obscuring their meaning". The key word here is purpose.

It is extraordinarily rare for Part 97 to regulate purpose, not practice, and we have to assume that the rules were written to mean exactly what they say.

So, if my purpose for encrypting a signal was, for instance, to comply with Part97.113(e) (stating

"no station shall retransmit programs or signals emanating from any type of radio station other than an amateur station...") because your 802.11g Gear is surrounded by Part 15 users, then it's perfectly legal. If it so happens that to maintain that compliance you need to encrypt everything, well, so be it.

There are other instances as well. Think about it for a while, and you will come up with other purposes for needing encryption that do not involve specifically the obfuscation of meaning (although that may happen to be a by-product). Some of these purposes can be argued - privacy is a good example – but others are clearer. (Note: This isn't limited to 802.11, it applies equally to HF, so long as you keep the communications within the country. Some international agreements prohibit encryption).

Sure, there are caveats. You need to comply with 97.309(a)(4), about the modulation scheme being publicly documented, (I'm pretty sure 802.11 and WEP both comply), plus you certainly have to ID every 10 minutes. I believe it would be good amateur practice to make a note of the encryption key in your station log, too.

From the FCC's point of view, they really only need to know who is doing the transmitting. For that, I'd think setting the SSID to your callsign would be enough. If they also need to know what it is that you're transmitting, they can just ask, or even easily record the signal in full bandwidth, and stop by later to ask for the decryption key so they can play it back and see what it was. Surely the Government can do this even without your assistance, but I seriously doubt anyone would refuse to hand over the key.

As far as content is concerned, use the Grandma Test: If you wouldn't be proud to have your grandma hear what you're sending, then you probably shouldn't.

Surely this issue will be controversial, and although I can't name names, I heard it with my own ears: Some encryption is perfectly legal under Part 97. If you remain doubtful – I don't blame you – then wait a while and see what comes of this fairly recent information. For the rest of us, though, there's nothing standing in your way.

###