RM-11831 Comments April 25, 2019

Submitted by:

James T Fortney, K6IYK
PO Box 12589
Prescott AZ 86304-2589

As an Amateur Radio Operator for over 62 years, I have actively experimented with most of the communication modes available under Part 97. For many years I have been an active leader in the Amateur Radio fraternity supporting advancement of our radio hobby.

Many instances of new techniques developed by the Amateur Radio experimenter brought into question compliance with the open communications requirement, and in almost every case the FCC has agreed that if we fully published the information needed to be able to receive our transmissions, they would be considered acceptable.

For over four decades I worked with the FCC Los Angeles Field Office Engineers-In-Charge and their staff to support meaningful Amateur Radio compliance with Part 97.

I had the privilege of participating during the 1970s and 80s in the TCP-IP transmission developments introduced by Phil Karn, KA9Q. The continued development of digital modes initiated during that period has moved Amateur Radio forward and has allowed Amateur Radio to train hundreds if not thousands of skilled individuals that now work with this technology in industry.

Mr Karn has submitted a response to the request for comments on RM-11831 which is thorough and meaningful, and which clearly describes the difference between advanced communications techniques and encryption. **I wish to endorse the comments he has submitted and encourage the Commission to consider his important presentation.**

A copy of his submittal has been attached.

Before the Federal Communications Commission
Washington DC 20554

In the Matter of

Amendment of Part 97 of the Commission's
Amateur Radio Service Rules to Reduce
Interference and Add Transparency to Digital Data
Communications

RM-11831

Comments of Philip R Karn, Jr, KA9Q

I write to oppose the arguments and proposed remedies in this proceeding regarding digital mode transparency. I am very sympathetic to the underlying principle that amateur radio must remain open, non-commercial and self-policing, but the proposed remedies are poorly considered and could have significant unintended and adverse consequences on the ability of the Amateur

Service to fulfill its Basis and Purpose.[1] I recommend that the Commission dismiss the petition, or in the alternative, modify or limit the proposal to address the concerns I raise below.

Background

I have been a radio amateur since high school in 1971. Amateur radio led directly to my career as an electrical engineer with degrees from Cornell and Carnegie Mellon Universities. I worked in applied communications research departments at Bell Laboratories, Bell Communications Research (Bellcore) and Qualcomm, from which I retired in 2011 as a Vice President - Technology. My hobby and my profession have always been closely intertwined. At Bellcore in the 1980s, I contributed to early Internet development and, on my own time, wrote the first complete implementation ("KA9Q NOS") of the core Internet protocols for the PC for amateur packet radio; it also helped launch the nascent Internet Service Provider (ISP) industry. I have been active in amateur radio satellite development; I designed and implemented three digital telemetry systems for AMSAT satellites. I implemented telemetry demodulators for the ACE and STEREO spacecraft and donated them to NOAA, and in 2014 I participated in the ICEE-3 reboot project by implementing a demodulator for its long-obsolete telemetry system.

My work on the Internet over amateur packet radio in the 1980s attracted Qualcomm's attention, and I moved there in 1991 to apply it to their CDMA digital cellular system. I continued my participation in the Internet Engineering Task Force (IETF) where I specialized in Internet access, network security and encryption protocols; I began the group that standardized virtual private networks (VPNs).

---

[1] Part 97.1(a), (b), (c), (d) and (e)

In my retirement I have again become active in amateur radio. I don't operate much, but I continue to experiment and develop open source amateur radio software for satellite tracking, error correction, digital radio modems and software defined radios.[2] I have developed a passion for amateur radio as an educational tool:[3] I mentor student amateur radio clubs at Mount Carmel High School and at UCSD. I have gone full circle back to my own start as a ham and am having a lot of fun.

Background of the (flawed) Petition

The present petition appears to be motivated by the alleged difficulty of monitoring the Winlink network in the amateur tradition of self-policing. Theodore Rappaport claims that Winlink and Pactor are "effectively encrypted" in that, while no actual encryption is used,[4] the effect is the same. I ***strongly*** disagree.

Intent is the current and correct standard

With the phrase "for the purpose of obscuring their meaning", the Commission wisely made *intent* the key element in the existing rule and it should remain so. Any problems can be addressed with the existing rules, perhaps with further clarification by the Commission.

---

[2] 97.1(c) : "Encouragement and improvement of the amateur service through rules which provide for advancing skills in both the communication and technical phases of the art."

[3] 97.1(d) "Expansion of the existing reservoir within the amateur radio service of trained operators, technicians, and electronics experts".

[4] 97.113(a)(4): "No amateur station shall transmit…messages encoded for the purpose of obscuring their meaning".

Efficient communication methods are *inherently* harder to monitor

If the rule were expanded to prohibit anything that might *incidentally* make monitoring harder, regardless of intent, little would escape its scope. Virtually *anything* one might do to facilitate communications and/or use the radio spectrum more efficiently[5] *will* have the side effect, intended or not, of making that communication more difficult for some third parties to monitor. Even a rare natural language[6] could be an "effectively encrypted" communication even if the speakers' intent is solely to facilitate communications (e.g., because it's their native tongue).

An illustrative technical example is automatic power control (APC) where the transmitter uses feedback from its intended receiver to adjust transmitted power to the bare minimum needed for proper operation at any moment.[7] Applying APC to modern digital modes would dramatically reduce average transmitter powers and signal-to-noise (SNR) ratios at the intended receiver and at any monitors. If the SNR at a monitor station falls below the necessary threshold, which would happen if it's only slightly worse than at the intended receiver,[8] the monitor could not decode the transmission. Although APC is highly beneficial in reducing interference and therefore clearly in

---

[5] 97.1(b): "Continuation and extension of the amateur's proven ability to contribute to the state of the art."

[6] Navajo, for example. It would be unfair to prohibit modern Navajo hams from speaking their native tongue just because of its historical role in World War II.

[7] 97.313(a) already requires amateur stations to use the minimum transmitter power necessary to carry out the desired communications. This rule is honored mainly in the breach because continuous manual power adjustment is tedious. Excess link margins of 10-20 dB or more are therefore not uncommon.

[8] Modern digital error coding and modulation exhibits a sharp "cliff" or "threshold" in that a slight change in received signal-to-noise ratio (e.g., 1-2 dB) can mean the difference between perfect reception and none at all. This is inherent to any scheme that approaches the theoretical (Shannon) channel capacity limit. Many people are familiar with this phenomenon as it affects digital TV broadcasting. It is also key to the efficient "repacking" of TV channel assignments now underway.

the spirit of the rules, it would be prohibited by a poorly conceived rule banning methods that incidentally impair the ability to monitor.

APC is just one simple example; *every* method for increasing spectral efficiency applies the same principle of taking into account channel properties and what the intended receiver already knows to minimize the transmitted energy to convey a new message. This is true for *every* aspect of communication, be it an antenna, a natural language, a character set, error control coding, a communications protocol — or a compression algorithm, as discussed later.

The concerns expressed by the Petitioner and others seem to consist of three elements, though they do not articulate them as such. The distinctions are subtle but critical for the future of the Amateur Service, so I will discuss each in turn.

First issue: disclosure

The first and most basic issue is *disclosure:* should the technical details of amateur communications be openly published? Here I completely agree *in principle* with the Petitioner: a full "air interface" specification for every mode used by amateurs *should* be fully disclosed. Not only would this unambiguously demonstrate lack of intent to obscure the meaning of communications, it furthers the role of the Amateur Service in promoting technical experimentation, advancement and personal education.

However, writing this into the rules would have the immediate (though unintended) effect of banning all three digital voice radio technologies already widely used by amateurs in the US and elsewhere: D*Star (iCom), DMR (Motorola) and Fusion (Yaesu).

These systems are derived from digital voice systems developed for public safety applications, e.g., APCO P25. Although amateurs do not use any optional encryption features, all three systems use versions of Advanced Multiband Excitation (AMBE), a digital voice encoder/ decoding algorithm (codec) proprietary to Digital Voice Systems, Inc (DVSI), which vigorously protects its intellectual property with both patents and trade secrets. It sells ABME *only* as a "black box": a self-contained digital signal processing (DSP) chip with firmware that cannot be read or modified. There are no public documents to enable others to write interoperable implementations, and needless to say no open source implementations are authorized.[9]

AMBE is highly controversial among some amateurs (including me) precisely because its proprietary nature conflicts with the amateur tradition of open, noncommercial experimentation and education. There are also non-proprietary and *superior* alternatives, e.g., CODEC2, developed by Australian amateur David Rowe (VK5DGR) specifically for amateur use and fully documented with open source software.

But as much as I'd personally like to see CODEC2 displace AMBE, it cannot interoperate with the dozens of models of commercially made digital voice radios with AMBE already in widespread amateur use, nor can these radios be easily modified. So as highly desirable as full open publication of all air interfaces would be, making it mandatory would effectively ban all three major digital voice systems from the amateur bands.

---

[9] Although Petitioner is motivated by the need to monitor proprietary data formats, and monitoring D*Star et al is not a problem with DVSI's products, a documentation requirement would not necessarily make this distinction. This could lead to serious unintended consequences.

For this reason I must oppose the proposed disclosure rule in its present form. I would rather make my case against proprietary technology on the amateur bands through persuasion and example than by legal force.

Nevertheless, should the Commission feel it necessary to write a disclosure rule, a question is raised: what's an adequate disclosure? Here I suggest borrowing the term "enabling" from patent law. To be valid, a patent must disclose the invention in sufficient detail to enable someone skilled in the art to make and use the invention. As applied to amateur communication modes, the disclosure should enable someone skilled in communication systems, digital signal processing and computer programming to write software that will interoperate with existing implementations, at least in receive mode.[10]

Second issue: open source software

Beyond disclosure, the Petitioner additionally recommends that "open source" software be required to be available for every digital communication mode. He does not define it further, but I'll assume he is talking about open source software as it is generally known in the computer industry, where it has become very popular.

As much as I personally believe in open source software[11] I believe this recommendation should also be rejected. It raises a long list of difficult issues such as acceptable programming

---

[10] SCS, the owner of Pactor, has already publicly documented in detail Pactor versions 2-4 and the B2F compression protocol, but objects to disclosing its proprietary software and algorithms. Much of SCS's intellectual property appears to consist of receiver channel equalization algorithms as well as software "tricks" to make their software run fast on low cost computers. They are performance enhancements not strictly required to decode a high quality recording of a transmission, as might be made by FCC monitoring facilities near a transmitter. SCS should not be required to disclose these details.

[11] I open-source all of the software I write on my own. But this is a personal decision, and I respect the choice of commercial software authors to do otherwise.

languages, libraries, compilers, operating systems and versions. Would support be required? If so, for how long? Could one charge for it?

Should any digital mode become popular enough to warrant general interest by the amateur community, I am confident that volunteers would step up and write open source software — provided the necessary documentation is available. Many such programs are already available for other amateur modes.

Third issue: dynamic compression on lossy channels

Although Pactor and Winlink do not use encryption, it has been alleged that they are difficult to monitor, thus hampering amateurs' ability to police their own ranks. Theodore Rappaport refers to Winlink as "effectively encrypted". Rappaport knows that "encryption" is a loaded word among radio amateurs, and I believe he uses it disingenuously to confuse true encryption[12] with data compression that most emphatically is *not* "encryption" by any accepted meaning of the word or under the existing Amateur rules. As an accomplished communications engineering professor, he ought to know better.

Properties of dynamic data compression

To clarify the difference with true encryption, data compression bears further discussion. As mentioned earlier, any communication requires some "common knowledge" between transmitter and receiver. Much of this can be static, i.e., fixed and widely known, but most modern text compression algorithms are *dynamic.* That is, the sender uses the data previously

---

[12] For example, the Advanced Encryption Standard (AES) with a secret shared key would clearly demonstrate an intent to conceal the meaning of a communication under 97.113(a)(4).

sent in the current compression session to efficiently encode more data. It adapts "on the fly" to the changing statistics of real data, unlike, e.g., Morse Code, which was designed with an English language letter frequency chart and never changes. Modern dynamic compression is very sophisticated, looking not only at character frequency but also longer strings or even entire repeating blocks of data. The results can be dramatic. Using the open-source Linux 'xz' utility[13] to compress Project Gutenberg's unformatted ASCII English text version of Tolstoy's *War and Peace*[14] reduces the file size from about 3.3 megabytes to 914 kilobytes, only 27.8% of the original; clearly a substantial improvement.

But even a single reception error causes the decompressor to fall out of sync with the compressor, and decoding cannot continue. This is not a problem on a reliable channel, including by radio to an intended receiver with FEC (forward error correction) and ARQ (retransmission), but it does mean that a monitor who comes into the middle of a session, or experiences any uncorrected errors,[15] will be unable to decompress any more data for the rest of the compression session. It must be emphasized that this is an inherent property of *every* dynamic compression algorithm, even when fully public.

Even voice and video codecs have this error-propagating property, but real-time delay limits usually require the compression state to be frequently reset.[16] This significantly reduces

---

[13] https://en.wikipedia.org/wiki/Xz

[14] http://www.gutenberg.org/files/2600/2600-0.txt

[15] Because the transmitting station doesn't know that the monitor is there, it cannot ensure that the monitor gets all the data correctly, e.g., by increasing power, reducing data rate, or retransmitting lost data. It can only do that for the intended receiver.

[16] This accounts for the noticeable delay (up to several seconds) when changing broadcast, satellite and cable digital TV channels. The modem retunes quickly, but the MPEG decoder must wait for the next full state transmission.

compression performance compared to an algorithm specifically designed to, e.g., play back a local computer file.

It should be noted that this problem can be entirely avoided by simply placing a receiver close enough to the transmitter to get an error-free data stream. The Commission's field offices have long had such facilities, as does (it is said) the US National Security Agency (NSA).[17] More recently, the growing popularity of "Web SDRs" (radio receivers made publicly available over the Internet) brings similar capabilities to the average amateur.

I have privately asked Ted Rappaport if he objects only to undocumented compression algorithms, or to all dynamic compression because of this error propagation property. He has repeatedly evaded the question. I am hoping that he and Petitioner will clarify their objections in their comments to the Commission. If their objections relate solely to lack of documentation, then much of this discussion becomes moot.

Respectfully submitted,

Philip R. Karn, Jr, KA9Q

---

[17] This renders moot Rappaport's rather histrionic concerns about the effect of Winlink on US national security. Terrorists now have much easier and far less conspicuous ways to communicate securely — with true end to end encryption, not just compression — than over amateur radio.