Dr. Theodore S. Rappaport, PE *PO BOX 888* *Riner, Virginia 24149* *tsrwvcomm@aol.com*

November 10, 2018

Commissioners
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear FCC Commissioners:

This is a notice of ex parte, based on email communication I had with the CTO of the FCC, Dr. Eric Burger, on November 8, 2018, his reply on November 10, 2018, and my reply on November 11, 2018. The email communication is centered around a posting that appeared on the FCC ECFS system on November 7, 2018, and is part of an ongoing proceeding at the FCC, NPRM 16-239, that I and thousands of others view as a direct threat to the national security interests of the United States, as well as being detrimental to the hobby of amateur ("ham") radio.

Public comments made in FCC's NPRM 16-239, and in FCC proceedings RM-11708, RM-11759, and RM-11306 proposed by the American Radio Relay League, show the vast number of rule violations and national security threats that continue to go unaddressed by the FCC. Commenters such as me view the lack of FCC acknowledgement of these problems as jeopardizing the safety of US citizens. **NPRM 16-239 attempts to remove a limit on the baud rate of High Frequency (HF) shortwave transmissions, without first addressing ongoing rule violations pertaining to proper usage of the amateur radio service, the use of obscured, private messaging which is forbidden in Part 97 rules and creates national security concerns, as well as other violations. If allowed, NPRM 16-239 would perpetuate the current violations, and would authorize obscured transmissions of unlimited bandwidth over the global airwaves, further increasing the danger to our national security, since these transmissions cannot be intercepted or eavesdropped by other amateur radio operators or the FCC.**

The public records in the above cited proceedings make clear how the evolution of undocumented, proprietary transmission technologies such as Pactor and Winlink, ARDOP, Winmor, STANAG, and other HF transmission schemes that use controlling software (e.g., Winlink, which was designed for secure commercial and government maritime mobile radio systems) have created a national security problem in the amateur radio service, such that 3rd parties (e.g. other ham radio operators, or the FCC listening stations, themselves) cannot intercept and decode over-the-air transmissions when used in the popular Automated Repeat Request (ARQ) mode. Thus, Winlink with Pactor, and Winlink with ARDOP, Winmor, STANAG, or other modulations, cannot be intercepted or deciphered, over-the-air, by other amateur radio operators or the general public, thereby enabling users of the amateur radio service to provide obscured, private communications. In my personal conversations with FBI and FCC officials, they admit they also are unable to readily decode these types of transmissions. In my discussions with vendors of amateur radio equipment, they tell me that they are concerned about purchases of amateur radio equipment by criminal cartels, and that they believe it is happening daily. The FCC should recognize this major deficiency, and the danger of NPRM 16-239, and should address Part 97 rules to remove this type of obscured communication and other ongoing violations, before it enacts NPRM 16-239.

This letter and ex parte communication surrounds this recent posting at the FCC ECFS from the maker of Pactor:
https://www.fcc.gov/ecfs/filing/110731917879

I am concerned that despite the thousands of objections filed over more than a decade in the above mentioned proceedings (and amongst the amateur radio community in the ARRL "Ad-hoc HF Digital Committee" that led to ARRL's authorship of RM-11306), FCC officials continue to ignore the documented problems and national security concerns. Some in the FCC, and the ARRL, continue to promote FCC rule changes such as NPRM 16-239, RM-11306 and RM-11708 that violate other sections of Part 97 that define the amateur radio service.

The FCC, and the public at large, should wonder why there has been a five month delay (June 11, 2018 is the date of the SCS email, yet it was posted at the FCC ECFS on November 7, 2018) in this contentious rulemaking procedure. This, in part, prompted my communication with Mr. Berger, provided below.

While SCS has apparently licensed its proprietary Pactor 2,3 and 4 compression scheme to a few government-interception companies that sell expensive ($20,000 US) products for the signal intelligence communities, rank and file amateur operators, law enforcement officials, the general public, and even the FCC listening posts, and other government listening posts around the world, cannot decode these transmissions for their meaning.

As publicly cited at the FCC's ECFS, there are regular rule violations from Winlink/Pactor and Winlink/Winmor transmissions on the amateur radio high frequency (HF) frequency bands (e.g regular violations of FCC Part 97.1, 97.4, 97.309, 97.113, 97.117, 97.119, 97.123 regarding the need to provide open, personal, hobby-like communications, to not obscure transmitted messages, to provide a self-policing environment so that other amateur operators may openly listen to and correct/identify/report troublesome over-the-air transmissions, to properly identify any amateur radio transmission, to avoid business use in the amateur radio service, and to avoid using the amateur radio to bypass other commercial means of communication). More violations will be occurring with VARA, ARDOP, and other commercially secure modes such as STANAG if this problem is not immediately addressed by the Commission by rulemaking in Part 97.

The email communication between myself and FCC's CTO is provided below. I remain at your service to assist in any way to ensure amateur radio and the national security of the US remains strong.

.

Sincerely,

Theodore S. Rappaport, P.E., Ph.D., N9NB

Cc: Congressman Morgan Griffith, Senator Mark Warner, Senator Tim Kaine

EMAIL COMMUNICATIONS BETWEEN Dr. Ted Rappaport and Dr. Eric Burger (CTO, FCC)

Sunday, November 11, 2018 from: tsrwvcomm@aol.com; to: Eric Burger [mailto:Eric.Burger@fcc.gov]

Dear Eric, thank you for your reply, I shall file our correspondence as an ex parte.

In my view, your proposed interpretation of FCC rules (your point 3) is dangerous to our country, not just to the hobby of amateur radio. If your point 3 is the view of the FCC in general, then I believe rules must be immediately clarified, so that a tiny minority of amateur radio enthusiasts (Winlink, Pactor, ARDOP, Vara , Winmor developers and users) are not permitted to place our country and the amateur radio service in peril.

In this ex parte, please again consider for the record my present and past communications, citing the danger of allowing transmissions on the amateur radio service that cannot be intercepted over the air, as they occur, by 3rd parties.

I shall contact my elected officials, and seek ways to have Congress investigate this interpretation, if the FCC itself will not, as I view it as dangerous to our country, and I hope other citizens (particularly, Amateur radio operators, and the popular press) will take interest in this situation, before amateur radio is used to enable harmful communications that can lead to catastrophic crimes, since the radio transmissions cannot be intercepted and interpreted over the air. Note that High Frequency ham radio transmissions easily are transmitted around the world, making encrypted transmissions around the globe a reality and a threat for international communication linked to terrorism, drug trafficking, and other crimes.

I encourage you to read Part 97 more closely. I do not believe that your Point 3 is open to interpretation when reading the Part 97 rules in their entirety, and I expressly comment here that such an interpretation is dangerous to national security, since it avoids the ability to understand the meaning of communications, as it occurs, in real time – this is a national security concern as well as a concern for the proper use of the spectrum for the amateur radio service, since such an interpretation removes the ability, at the time of transmission, anyone to intercept and act on transmissions heard over the air.

See all of the FCC Part 97 rules pertaining to the spirit and open nature of communications in amateur radio, the need to self-police, the requirement to have transmissions that are not “obscured,” the need to avoid bypass of other commercial means (e.g. no internet service provider bypass), the requirement to avoid business, pecuniary interest (e.g. hams must avoid business use with the internet).

97.309(b)(3) is also limited by Part 97.305(c) and 97.307(f)(3).

Part 97.307(f)(3) limits all of HF transmissions to “specified codes” and 97.307(f)(5)(6)(7) further limits “unspecified codes” to frequencies above 50 MHz.

PacTOR was only specified as the original Pactor 1, the openly interceptable Forward Error Control Coding made by AMTOR.

The SCS proprietary Pactor 2, 3, 4 in ARQ is not available for interception or decoding by 3rd parties over the air. Otherwise, FBI and Laura Smith in the Wireless Telecom Bureau (WTB) would be able to eavesdrop over the air when in ARQ mode. They cannot. Prove to me they can. Prove to the thousands of concerned citizens that it can be intercepted by anyone over the air when in ARQ mode. I submit you cannot prove this, since it cannot be done.

The Nov. 7, 2018 posting from SCS (made public 5 months after receipt—why the delay?) alludes to this ”trade secrets” of SCS. I and any other ordinary ham radio operator cannot build a decoder for ARQ Pactor

with Winlink and intercept the transmissions over the air. SCS probably licenses its full compression and algorithms to a couple of Signal Intelligence radio manufacturers for government use. The FBI officials I spoke to are not able to intercept these transmissions. Ham radio operators are unable to intercept these transmissions – see the comments in so many at the FCC ECFS proceedings over the years. Any communication on amateur radio should have the complete algorithm, or "as it happens", communications made available to any 3rd party. Pactor needs to provide the complete decompression algorithm for the ARQ transmissions so any 3rd party may readily decode any ARQ transmission – yet it is not available. I suspect SCS licenses this only to a tiny number of companies in the Signal Intelligence community, and most Maritime Mobile customers want to use Pactor or Winlink to ensure their transmissions are obscured to prevent eavesdropping.

Point 2. Pactor is decodable with an SCS modem but only in FEC (Unproto) mode, ARQ is NOT decodeable by an eavesdrop at a random location, a fact conveniently sidestepped by SCS and Winlink, and seemingly ignored by Scot Stone and Curt Bartholomew at the FCC, time and time again. See the Winlink intro document that says how communications cannot be read over the air (prize offered by a Winlink SysOp, but never claimed since it can't be intercepted) and the email from Lor reminding the sysops to log in to review their RMS traffic. See the history of Winlink from the New York Times article at the turn of the century. Today, many Winlink SysOps do not know what is going through their RMS! Its unmonitored in real time. It's a problem and in violation with the spirit and intent of Part 97 rules. I and others have noted this publicly at the FCC ECFS website, and in ex parte communications, but these points seemingly go ignored, again now in your email this week.

Eric, it's not just Pactor alone, it's the implementation of Pactor with Winlink. These two cannot be parsed, to assume things are ok. They are not. They work in tandem to provide an obscured transmissions method in ARQ mode, enabling secure communications for business and potentially criminal use that cannot be intercepted by others listening on the frequency.

Suggestions: Have WINLINK with SCS prove that their compressed ARQ can be intercepted over the air by any 3rd party. While you are at it, the FCC must also look at VARA and ARDOP and Winmor ARQ modes with Winlink or other software like Winlink.

I urge you and the Commissioners to change the Part 97 rules to make it very clear that such 3rd party interception, as it happens, is required of all traffic sent over the air for amateur radio. That is what Part 97 says, as a whole, but these rules are being ignored and promulgated by a few people in the FCC and by the American Radio Relay League.

If SCS is the only thing in the record that says Pactor is decodable, I'll bet that no one asked, or no information was volunteered by SCS, or Winlink about compressed ARQ. This note from SCS, posted at the FCC 16-239 ECFS website on Nov. 7, 2018, is simply disingenuous, as Pactor ARQ can be heard over the air (e.g, it can be monitored as in having a signal present) BUT, the meaning of the transmissions are not understandable ! It is obscured traffic! The record contains thousands of commenters in RM 11306, RM 11708, RM 11759, 17-344 and NPRM 16-239 that emphatically make this point and which disagree with the SCS posting of Nov. 7, 2018. These points must also be in the record.

I and others have pointed out how Mr. Waterman, the founder of Winlink, has evaded directly the "decode ARQ" question, and has been urging for the allowance of encrypted data for HIPPA and other reasons, and how Winlink advocates have taken both sides of arguments on why RM-11306 and RM-11708 should be allowed at the FCC.

Eric, you and the Commissioners must realize that if so many amateur operators have complained for so long, and have provided sincere, earnest evidence about their inability to intercept the transmissions, that there is a real problem here.

You need to insist on an experiment, a public demonstration, which I would be delighted to participate in, that shows SCS, WinLink, ARDOP, VARA all can be intercepted by an arbitrary 3rd party when they are used in the ARQ mode with Winlink.

For the sake of national security, and the future of amateur radio, the FCC must realize the above, and should count the thousands who object to your dangerous Point 3 interpretation, as being ON THE RECORD. I know that I do NOT hate Pactor – if I were a merchant marine, I would want to use it for secure HF communications. I, like thousands of others in amateur radio, simply do not want amateur radio to become a secure internet access point in the sky, providing secure/encrypted email and internet browsing for business use and, worst yet, for illegal activities that can support terrorism or other crimes, using methods that other amateur operators are unable to intercept over the air. That is the problem we have today. You must not enact NPRM 16-239 (e.g. do not remove the baud rate limit), until FIRST addressing the thousands of complains and legitimate concerns about the proper use and spirit of amateur radio, that requires open, unobscured transmissions that may be intercepted openly over the air.

73 ted N9NB

PS. I am very honored to have helped you get the "ham radio" bug that led to you getting your amateur radio license this year! Congratulations and welcome to the fraternity of ham radio. This hobby has inspired so many to do great things in electronics, science, and communications throughout the past century. I wrote a piece for the National Contest Journal that will appear in about a month, highlighting the feats of past amateur operators – welcome to this great hobby .

From: Eric Burger [mailto:Eric.Burger@fcc.gov]
Sent: Thursday, November 8, 2018 10:49 AM
To: Ted
Subject: RE: This is not accurate - be warned

1. The below seems like something that should be an *ex parte.*
2. The record appears to only have SCS' statements that Pactor is decodable. Unless there is something in the record *demonstrating* that Pactor-4 is not decodable, the lawyers in the organization are going to go with what is in the record. Assertions that Pactor-4 is hard to decode or people have trouble decoding it is not sufficient.
3. Note that one interpretation of §97.309(b)(3) states that one can use entirely proprietary (but still not encrypted) communications so long as there is a record of the communication. An example of this would be if WinLink keeps copies of email, then §97.309(b)(3) is satisfied and the fact one cannot intercept the radio communication is irrelevant. If you have an opinion about that, either that is not a reasonable interpretation, or the rule should be changed, you should file comments or a petition, respectively.

From: Ted <tsrwvcomm@aol.com>
Sent: Thursday, November 8, 2018 12:11 AM
To: Eric Burger <Eric.Burger@fcc.gov>
Subject: This is not accurate - be warned

Dear Eric:

Look carefully at this.
https://ecfsapi.fcc.gov/file/110731917879/16-239.pdf

This is very disingenuous.

Read: "corporate secrets " is why full details cannot be disclosed. This is why SCS Pactor remains secure and encrypted, through its compression algorithm.

They admit that it is a corporate secret- and this is why all the needed details to openly decipher the pactor transmissions will not be made open or shared.

They say "Easily monitored", BUT NOT easily decoded.

Hams for years have complained they can hear the signals, but CANNOT decode or intercept the transmitted Messages.

This is not from a "Pactor hater," but rather from one who abides by fcc rules, and wants to ensure all communications are open for reception and decoding by others, over the air, as required by the scope and spirit of FCC Part 97 rules.

For national security concerns, please ensure that part 97.113, 97.119, 97.221, 97.1, 97.3 and many other part 97 rules are upheld.

Do not allow 16-239 to pass.

Japan and many other Asian countries do not allow these types of transmissions, since they cannot be openly decoded over the air.

Best regards,
Ted Rappaport

Sent from smartphone, please excuse typos