SCS GmbH & Co. KG Röntgenstraße 36 D-63454 Hanau

Federal Communications Commission
445 F St. NW
Washington, DC 20022

SCS - Spezielle Communications Systeme GmbH & Co. KG
Röntgenstraße 36
D-63454 Hanau

Phone: +49 (0) 61 81 / 85 00 00
Fax: +49 (0) 61 81 / 99 02 38
info@scs-ptc.com
www.scs-ptc.com

May 10, 2019

Reply Comment, RM-11831,
by Hans-Peter Helfert, DL6MAA,
c/o Spezielle Communications Systeme GmbH & Co. KG, Germany

Dear Sirs and Madams,

Professor Theodore Rappaport, in his “Reply Comment” letter to the FCC on April 27, 2019, says I have written untrue and “disingenuous” statements in my Comment on RM-11831. As outlined below, his comments may be rejected as inaccurate or mis-informed and by doing so brings into question his entire 27 page filing:

https://ecfsapi.fcc.gov/file/10429199250117/FCC%20Letter%20Reply%20to%20Comments%20RM%2011831.pdf
(See section VII.)

It is possible Professor Rappaport is unfamiliar with the difference between modem onboard compression and external compression through application software or he deliberately mixes these two points to underpin his thesis of "effective encryption". Professor Rappaport's assumptions are in fact categorically false.

I will reiterate, that all SCS modems contain a monitor mode as a standard tool. This means that all parts of an **A**utomatic **R**epeat Re**Q**uest (ARQ)[1] message can be monitored entirely by third parties. This feature has absolutely no relation to the external application software connected to the modem.

The only requirement for monitoring of ARQ data by third parties using a PACTOR modem and a *simple publicly available terminal program (external application)*[2], is sufficient signal

to noise ratio, a similar requirement when attempting to listen to any transmission whether it be RTTY, CW, voice, etc. PACTOR has been designed so that each ARQ packet can be monitored. Each packet will be automatically and completely decompressed if internal compression is used, as the internal compression in the modem (Huffman, PMC) only extends over a single packet[3]. Each PACTOR information packet also has a synchronization preamble, which makes it easier to synchronize and read the data through third parties, even at high tuning offsets.

Monitoring a communication between two PACTOR modems over the air can be demonstrated using a third receiver, the modem in “PMON” mode[4], and a simple terminal program.

If an external application (software) uses common compression over an entire file (e.g. LZH, JPEG, etc.) and the payload information is transmitted via PACTOR, the compressed and initially illegible data stream can be displayed on the terminal program. In this case nearly all packets of a message must be read in order to obtain all decoding information and then completely decompress the information to read it in plain language. Again, this has absolutely nothing to do with the modem itself, but only with the application software that sends a payload to the modem for transmission.

Nevertheless, “eavesdropping" on Winlink communications between two connected stations using Winlink software with ARQ and entire-file LZH compression has been successfully demonstrated, and one such illustration has been sent as a Comment by Dr. Gordon Gibby (https://ecfsapi.fcc.gov/file/10410170249078/FCCRM11831-4.pdf),
counter to Professor Rappaport's and many other claims that it is “impossible”.

Please take these facts into consideration with your decision on RM-11831. Professor Rappaport is simply not correct in his presentation regarding "shortwave modems". He has not recognized the differences between physical, transport and application layers of modern ARQ protocols[5], like TCP, but instead conflates them to aid his invalid and loaded assertion of “effective encryption”.

Respectfully,

Hans-Peter Helfert
SCS GmbH & Co.KG

Excerpt from Professor Rappaport's letter:

Mr. Helfert claims “Through its almost 30 years of development and evolution, PACTOR has complied with US law at all times.” I and thousands of others do not believe this is true, as 97.113 has been violated through Pactor 2 and Pactor 3 messages that are obscured for meaning when sent over the air. He further claims "that our comprehensive monitoring mode allows full transparency of the PACTOR traffic, also for third parties. The monitoring mode is available as a standard tool in every PACTOR modem." This is categorically false since other operators who own Pactor modems are unable to intercept data over amateur radio using a stock Pactor modem with Winlink. Mr. Helfert’s position seems disingenuous and is part of the problem that has been created by ACDS operations by ARSFI/Winlink and SCS in amateur radio.

Mr Helfert makes the assertion that a comprehensive monitoring mode allows for full transparency of Pactor for third parties, but he might be misconstruing the term “third parties” as being a user in the closed Winlink email network that is having a message relayed within the closed private network, as opposed to a “third party” who would be an eavesdropper trying to listen to the message for meaning. There is absolutely no evidence that a random eavesdropper can intercept the compressed Pactor modem transmission. In fact, it is widely known and admitted by Winlink (see my comments in this proceeding and in RM-11828) that no one (other than signal intelligence personnel) is able to use a Pactor modem for over-the-air intercept of other Pactor stations when used with SCS compression/ARQ. This is precisely why the FCC must enact RM-11831.

Comprehensive monitoring mode allows for full transparency of Pactor for third parties, but he might be misconstruing the term “third parties” as being a user in the closed Winlink email network that is having a message relayed within the closed private network, as opposed to a “third party” who would be an eavesdropper trying to listen to the message for meaning. There is absolutely no evidence that a random eavesdropper can intercept the compressed Pactor modem transmission. In fact, it is widely known and admitted by Winlink (see my comments in this proceeding and in RM-11828) that no one (other than signal intelligence personnel) is able to use a Pactor modem for over-the-air intercept of other Pactor stations when used with SCS compression/ARQ. This is precisely why the FCC must enact RM-11831.

---

[1] ARQ
https://en.wikipedia.org/wiki/Automatic_repeat_request
[2] Freeware Terminal Program, e.g. “Coolterm”
http://freeware.the-meiers.org/
[3] PMC/Huffman packet-wise decompression source code (C language)
https://www.p4dragon.com/download/PACTOR_Advanced_Data_Compression.pdf
[4] PMON mode commands
https://www.p4dragon.com/download/Update_Info_DR7X00_Version_1_17_English.pdf
[5]OSI model
https://en.wikipedia.org/wiki/OSI_model