

**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 Permit Greater Flexibility in Data Communications	)	WT Docket No. 16-239
	)	
Petition for Rulemaking Filed by Amateur Radio Station Licensee Ron Kolarik (K0IDT)	)	RM-11831
	)	
Petition for Rulemaking Filed by the American Radio Relay League, Inc. (ARRL)	)	RM-11828
	)	
Petition for Rulemaking Filed by the American Radio Relay League, Inc. (ARRL)	)	RM-11759
	)	
Petition for Rulemaking Filed by the American Radio Relay League, Inc. (ARRL)	)	RM-11708
	)	

**PETITION FOR DECLARATORY RULING**

On behalf of New York University and pursuant to Section 1.2 of the Federal Communications Commission’s (“FCC’s” or “Commission’s”) rules,<sup>1</sup> the undersigned respectfully submit this Petition for Declaratory Ruling, which seeks a ruling that Section 97.113(a)(4) of the Commission’s rules prohibits the transmission of effectively encrypted or encoded messages, including messages that cannot be readily decoded over-the-air for true meaning.<sup>2</sup> For years, certain amateur licensees have violated Section 97.113(a)(4) by relying on an interpretation that contravenes the two bedrock principles – openness and transparency – that have enabled amateur radio licensees to self-regulate the Amateur Radio Service bands effectively. This interpretation has restricted Amateur Radio Service licensees’ efforts to

---

<sup>1</sup> 47 C.F.R. § 1.2.

<sup>2</sup> See 47 C.F.R. § 97.113(a)(4) (“No amateur station shall transmit . . . messages encoded for the purpose of obscuring their meaning, except as otherwise provided herein.”).

effectively self-police the amateur bands, thus enabling the continued violation of *many other* amateur rules. Accordingly, the Commission should eliminate the lingering uncertainty regarding Section 97.113(a)(4)'s meaning and clarify that the rule prohibits the transmission of effectively encrypted or encoded messages, including messages that cannot be readily decoded over-the-air for true meaning.

**I. SECTION 97.113(a)(4) PROHIBITS THE TRANSMISSION OF EFFECTIVELY ENCRYPTED OR ENCODED MESSAGES, INCLUDING MESSAGES THAT CANNOT BE READILY DECODED OVER-THE-AIR FOR TRUE MEANING.**

Section 97.113(a)(4) explicitly prohibits the transmission of “messages encoded for the purpose of obscuring their meaning, except as otherwise provided [in the rules].”<sup>3</sup> Importantly, the Commission has described Section 97.113(a)(4) as a “prohibition on encryption.”<sup>4</sup> Over time, the Commission has implemented and revised Section 97.113(a)(4) so that “the amateur service rules . . . conform to the language of the international *Radio Regulations*.”<sup>5</sup> The international *Radio Regulations* “prohibit[] amateur stations from transmitting messages in codes or ciphers intended to obscure the meaning thereof.”<sup>6</sup> Therefore, decades-long rule

---

<sup>3</sup> 47 C.F.R. § 97.113(a)(4).

<sup>4</sup> *Don Rolph Petition for Rulemaking to Amend Part 97 of the Commission's Rules Governing the Amateur Radio Service to Provide for Encrypted Communications*, Order, 28 FCC Rcd 13366, ¶ 4 (WTB 2013) (DA 13-1918) (“2013 Order”).

<sup>5</sup> *Id.* n.3; see also *Amendment of Part 97 of the Commission's Rules to Implement Certain World Radio Conference 2003 Final Acts*, Order, 21 FCC Rcd 278 (WTB 2006) (DA 06-79) (revising Section 97.113(a)(4) “to conform to the current language of Radio Regulations Article 25.2A”); see also Letter from Michael J. Marcus, Sc.D, F-IEEE, Director, Marcus Spectrum Solutions, LLC, to Marlene H. Dortch, Secretary, Federal Communications Commission, WT Docket No. 16-239, RM-11831, and RM-11828, at 2 (Oct. 13, 2019) (discussing relationship between FCC amateur rules and ITU Radio Regulations) (“Marcus *Ex Parte*”).

<sup>6</sup> *Amendment of the Amateur Service Rules to Clarify Use of CLOVER, G-TOR, and PacTOR Digital Codes*, Order, 10 FCC Rcd 11044, n.6 (WTB 1995) (DA 95-2106) (“PacTOR 1 Order”).

interpretations have stressed the need for open, transparent communications in the amateur bands.

For years, certain amateur licensees have skirted these requirements,<sup>7</sup> sending and receiving communications over amateur bands using communications modes that incorporate dynamic compression techniques<sup>8</sup> and, by extension, effectively encrypt or encode the communications.<sup>9</sup> These amateur licensees combine dynamic compression with Automatic

---

<sup>7</sup> See Letter from Ari Q. Fitzgerald, Counsel to New York University, to Marlene H. Dortch, Secretary, Federal Communications Commission, WT Docket No. 16-239, RM-11831, RM-11828, RM-11759, and RM-11708, Attachment at 4-6 (Oct. 8, 2019) (discussing “long standing problems” in the Amateur Radio Service); Reply Comments of Theodore S. Rappaport, N9NB, PS Docket No. 17-344, WT Docket No. 16-239, RM-11708, and RM-11306, at 9-10 (highlighting the longstanding efforts of certain amateur licensees to effectively encrypt communications and advocacy to permit effectively encrypted communications).

<sup>8</sup> “Compression” is a technique that reduces the number of bits needed to send a particular message, which conserves bandwidth and improves spectrum efficiency. See Theodore S. Rappaport, *WIRELESS COMMUNICATIONS: PRINCIPLES AND PRACTICE*, Ch. 7 (1<sup>st</sup> ed. 1996). Almost all of today’s Amateur Radio Service data modes use static compression with publicly known static compression tables, which allows all Amateur Radio Service licensees to listen to messages over-the-air for true meaning under reasonable propagation conditions. Where static compression is used, a known, fixed, and well-documented mapping of bits is defined for any symbol of the alphabet. By contrast, dynamic compression formulates a new, unique compression table each time a message is sent. Each formulated compression table is unique to each individual message. Aspects of the dynamic compression “key” are sent as part of the unique message itself and are not known universally. If any bits are lost by an Amateur Radio Service licensee attempting to listen to the message over-the-air, it is virtually impossible for the licensee to understand the message. Therefore, dynamic compression provides a “moving target” that makes it extremely difficult – if not virtually impossible – for an Amateur Radio Service licensee attempting to listen to the message to decompress the message for true meaning.

<sup>9</sup> Winlink is an example of a system that has contravened the Commission’s requirements. Winlink is a “worldwide radio email service” that relies on amateur radio bands. See Winlink Global Radio Email, *News*, <https://www.winlink.org/> (Sept. 11, 2019). Winlink utilizes certain communications modes that compress email communications to send them more efficiently over amateur radio bands (e.g., PacTOR, PACTOR 2, PACTOR 3, PACTOR 4, WINMOR, ARDOP, and VARA). Aside from PacTOR, which was open-source and approved for use by the Commission in 1995, the communications modes have not been publicly documented in a way that allows amateur operators or the public to understand messages sent by the Winlink system over amateur frequencies and are therefore not subject to the Commission’s exception that would permit their use. See 47 C.F.R. § 97.309(a)(4) (permitting use of “any technique whose technical

Repeat Request (“ARQ”), which allows only two linked stations to complete a transmission without error. For other amateur licensees who attempt to “hear” a message sent using dynamic compression and ARQ, fading and interference will prevent those licensees from receiving an error-free copy of the message, thus effectively obscuring the dynamic compression key and the messages themselves for anyone other than the two locked stations. Other licensees will thus be unable to reconstruct the decoding and compression scheme and, by extension, unable to decode the message for true meaning.<sup>10</sup>

---

characteristics have been documented publicly” and listing PacTOR as an example, but not PACTOR 2, PACTOR 3, PACTOR 4, WINMOR, ARDOP, or VARA); *see also PacTOR 1 Order* (approving use of open-source PacTOR).

While software has apparently been developed very recently to decode Winlink communications when sent using different PACTOR modes, the software’s efficacy and availability is unclear when applied to existing PACTOR-capable modems. If any bits or letters are missed or corrupted during the reception – as would be expected under HF propagation – the message cannot be realistically decoded. *See* Letter from Hans-Peter Helfert, DL6MAA, to Scot Stone, Federal Communications Commission, WT Docket No. 16-239, RM-11831, at 3 (Oct. 22, 2019) (“Decoding will be performed properly until there is a gap in the input data stream. Missing data in the received data stream thus . . . leads to an abort of decoding.”) (“Helfert *Ex Parte*”). Furthermore, no decoding has been developed for other Winlink communications modes (*i.e.*, VARA, ARDOP, and WINMOR).

<sup>10</sup> At least two commenters have claimed that Winlink messages may be monitored over-the-air, albeit under unrealistic, controlled conditions that do not represent reasonable propagation conditions. *See* Helfert *Ex Parte* at 3 (“Decoding will be performed properly *until there is a gap in the input data stream.*”) (emphasis added); Comments of Gordon L. Gibby (KX4Z), RM-11831, at 1 (Apr. 9, 2019) (allegedly demonstrating over-the-air monitoring under highly controlled conditions) (“Gibby Comments”). If the alleged monitoring solutions work as claimed, these commenters should have no objection to the Commission issuing the requested declaratory ruling.

While one might argue that it is also virtually impossible to monitor point-to-point amateur transmissions in microwave bands if high gain/narrow beam antennas are used in a point-to-point transmission, this can be differentiated from effective encryption because: (1) such point-to-point radio paths are very efficient, have a small impact on other spectrum users, and generally do not cover distances more than a few kilometers; (2) such point-to-point radio paths would occur at UHF frequencies and above, where there is significantly more Amateur Radio Service spectrum than at HF frequencies; and (3) the narrow beamwidths resulting from such antennas may produce some privacy away from the direct line-of-sight path but still allow third parties to monitor for true meaning via radio propagation caused by antenna sidelobes, scattering, moving

The amateur licensees that rely on dynamic compression techniques have justified the use of these compression techniques by stating that, although they make it virtually impossible to readily decode the communications for true meaning, the compressed messages are not “encoded *for the purpose of obscuring their meaning.*”<sup>11</sup> Under this conveniently narrow interpretation of Section 97.113(a)(4),<sup>12</sup> dynamic compression techniques (and resulting encryption that minimizes openness and transparency and prevents effective self-policing of the amateur bands) are justified and defended as simply a byproduct of an intent to use limited spectrum resources more efficiently.<sup>13</sup>

Despite claims that the relied-upon communications modes are not *intended* to obscure the meaning of messages, users of these communications modes have publicly acknowledged precisely the opposite. For example, users have stated that the communications modes – and the dynamic compression techniques on which they rely – are used in order “to reduce spectrum use *and to enhance privacy.*”<sup>14</sup> This public admission demonstrates an intent to “obscure” the messages’ meaning from others who are self-policing the amateur bands, in violation of Section 97.113(a)(4). By linking compression to efficient spectrum use *and* privacy, the admission also

---

a receiver into the main beam, or other propagation mechanisms, while also allowing significant decreases in required transmitter power with less interference to other spectrum users in the area.

<sup>11</sup> 47 C.F.R. § 97.113(a)(4) (emphasis added).

<sup>12</sup> See Marcus *Ex Parte* at 1 (describing Part 97 rules as “anachronistic provisions that made sense when they were adopted decades ago *but are ambiguous or problematical today*”) (emphasis added).

<sup>13</sup> See, e.g., Helfert *Ex Parte* at 2 (The compression techniques “ha[ve] nothing to do with encryption or obfuscation, but only serve[] to reduce the amount of data.”); Gibby Comments at 2 (stating that certain amateur licensees rely on “compression techniques to speed transfer and result precious bandwidth-time utilized”); Comments of SCS, RM-11831, at 2 (Apr. 15, 2019) (discussing how “onboard” and “outboard” compression efficiently utilize shortwave spectrum).

<sup>14</sup> See, e.g., ARRL Maryland-District of Columbia Section, *Winlink 2000 Radio-E-mail System Overview*, <http://www.arrl-mdc.net/Winlink/MDCWL2KOVwAM.htm> (Sept. 15, 2019) (emphasis added).

highlights how amateur licensees may easily evade Section 97.113(a)(4)'s prohibition on messages "encoded for the purpose of obscuring their meaning." Without clarification from the Commission that Section 97.113(a)(4) prohibits the transmission of messages that cannot be decoded over-the-air for true meaning under reasonable propagation conditions, amateur licensees will continue to evade the Amateur Radio Service's self-enforcement mechanisms by simply stating *another* purpose for using technologies that render messages extremely difficult to decode, even with additional software and hardware converters.

Furthermore, while spectral efficiency has been cited as the reason for relying on many of these communications modes, the actual efficiencies gained do not outweigh the costs associated with eliminating effective self-policing of the amateur bands. The compression techniques are used largely for non-time sensitive applications (*e.g.*, email), and the time saved can be measured in mere fractions of a second, or a few seconds at most. At the same time, the cost of implementing a static and public compression solution that would allow amateur licensees to intercept and decode messages for true meaning is minimal. Amateur Radio Service licensees already rely on many other published communications modes that use public, static compression,<sup>15</sup> which allows all users and the public to intercept messages over-the-air and decode them for true meaning under reasonable propagation conditions. An entity relying on communications modes that effectively encrypt messages could easily switch out the code that implements dynamic compression techniques for code that implements static compression, and this switch can easily be made through a software update. Therefore, entities using communications modes that effectively encrypt messages could push a simple software update to their users; provide and widely demonstrate a public, static compression method that may be

---

<sup>15</sup> Examples include JT-65, WSPR, PSK-31, CW, FT-8, and FT-4.

used by the broad Amateur Radio Service community to decode messages for meaning over-the-air under reasonable propagation conditions; and comply with Section 97.113(a)(4)'s openness requirement.

## II. THE RECORD DEMONSTRATES THAT VIOLATIONS OF SECTION 97.113(a)(4) ENABLE VIOLATIONS OF OTHER RULES GOVERNING THE AMATEUR RADIO SERVICE.

As the above example demonstrates, a narrow interpretation of Section 97.113(a)(4) renders Section 97.113(a)(4)'s prohibition on "messages encoded for the purpose of obscuring their meaning" toothless. A narrow interpretation undermines amateurs' efforts to self-police the amateur bands, consistent with long-standing Commission policy,<sup>16</sup> and enables the violation of other amateur rules, including:

- **47 C.F.R. § 97.113(a)(3)**, which prohibits "[c]ommunications in which the station licensee or control operator has a pecuniary interest, including communications on behalf of an employer." For example, Winlink's current enforcement mechanism reveals that e-mails traveling through Winlink's system violate Section 97.113(a)(3).<sup>17</sup> Unfortunately, Winlink's current enforcement mechanism requires users to log in online and review messages after the messages have traveled over-the-air, therefore rendering traditional, contemporaneous Amateur Radio Service enforcement efforts (*e.g.*, interception over-the-air and decoding for true meaning) ineffective.
- **47 C.F.R. § 97.113(a)(5)**, which prohibits "[c]ommunications, [made] on a regular basis, which could reasonably be furnished alternatively through other radio services." For example, Winlink transmits regular e-mail communications, including commercial e-mail communications,<sup>18</sup> over the amateur frequencies. There are many other FCC-regulated radio services available for regularly sending these data communications.<sup>19</sup> The rules

---

<sup>16</sup> See 2013 Order ¶ 6 ("[T]he amateur community has a long tradition of self-regulation.").

<sup>17</sup> See, *e.g.*, Reply Comments of Janis Carson, Ron Kolarik, Lee McVey, and Dan White, WT Docket No. 16-239, RM-11708, RM-11759, and RM-11831, at 29-60 (July 19, 2019) (providing extensive evidence in FCC Enforcement Bureau Ticket No. 3184322 that recent e-mails traveling through the Winlink system violate amateur service rules).

<sup>18</sup> See *id.* at 29-60 (providing evidence of commercial e-mail communications traveling through the Winlink system).

<sup>19</sup> See, *e.g.*, SailMail, <https://sailmail.com/> (Oct. 14, 2019) ("SailMail supports email communications using every internet communications device in all oceans of the world."); Iridium, Iridium GO!, <https://www.iridium.com/products/iridium-go/> (July 15, 2019) (offering

governing the other radio services do not require the same level of openness and transparency as the rules governing the use of amateur frequencies. The Commission is clear that the Amateur Radio Service is not like other radio services. In dealing with petitions seeking to broadcast music or bulletins over the amateur bands, the Commission has reinforced the need for the Amateur Radio Service to serve strictly as a hobby, without providing access to or services via the amateur radio spectrum by or for the public.<sup>20</sup> The Commission has also expressed its “strong commitment to maintaining the unclouded distinction between the amateur service and other radio services.”<sup>21</sup> Faced with incontrovertible evidence that Winlink is rendering indistinct the barrier between the Amateur Radio Service and other radio services, the Commission should now reaffirm its commitment to this principle.

- **47 C.F.R. § 97.115(a)(2)**, which restricts third party communications to stations in only certain, specified jurisdictions. The Commission lists countries with which U.S. amateur stations may transmit messages for a third party.<sup>22</sup> Winlink’s current enforcement mechanism reveals that e-mails have traveled through the Winlink system that violate the third party restrictions.<sup>23</sup>
- **47 C.F.R. § 97.115(b)(1)**, which requires that, with regard to third party communications, the “control operator [be] present at the control point and is continuously monitoring and supervising the third party’s participation.” For example, many of Winlink’s control operators are not “continuously monitoring and supervising” to determine whether third party participation complies with the amateur service rules. Instead, these control operators are relying on automatically controlled digital stations (“ACDS”), which send e-mail messages over the amateur bands that may violate the Commission’s rules.

---

satellite-based text, call, e-mail, and web browsing); Globalstar, Sat-Fi2 Satellite Wi-Fi Hotspot, <https://www.globalstar.com/en-us/products/voice-and-data/sat-fi2> (July 15, 2019) (offering “e-mail, text, talk, . . . [and] access to the web”); and OCENS, Inc., OCENSMail, <https://www.ocens.com/e-mail.aspx> (July 15, 2019) (“Complete e-mail solution for satellite and other low bandwidth connections”).

<sup>20</sup> *Amendment of Part 97 of the Commission’s Rules Governing the Amateur Radio Services, et al.*, Notice of Proposed Rulemaking and Order, 19 FCC Rcd 7293, ¶ 39 (2004) (FCC 04-79) (“The Commission adopted this prohibition to ensure that amateur service frequencies were not used as a substitute for other communication services.”).

<sup>21</sup> *2013 Order* ¶ 6.

<sup>22</sup> See Federal Communications Commission, Wireless Bureau, Mobility Division, Amateur Radio Service, *International Arrangements*, <https://www.fcc.gov/wireless/bureau-divisions/mobility-division/amateur-radio-service/international-arrangements> (Oct. 14, 2019).

<sup>23</sup> See Letter from Ari Q. Fitzgerald, Counsel to New York University, Theodore S. Rappaport, N9NB, Director, NYU WIRELESS, and Michael J. Marcus, N3JMM, to Marlene H. Dortch, Secretary, Federal Communications Commission, WT Docket No. 16-239, RM-11831, RM-11828, RM-11759, RM-11708, at 6 (July 24, 2019).



- **47 C.F.R. § 97.105(a)**, which requires that control operators ensure “the immediate proper operation of the station, regardless of the type of control.” Failure to comply with Section 97.115(b)(1) also leads to violations of this more general provision.
- **47 C.F.R. § 97.101(b)**, which prohibits the exclusive use of a frequency. The use of an ACDS to operate part of the Winlink system can cause the commandeering of certain amateur frequencies, effectively shutting out other amateur users and making exclusive use of the frequency.

A narrow interpretation of Section 97.113(a)(4) that requires specific intent to obscure a message's meaning and thus allows for the effective encryption of messages – so long as the sender can cite *another* purpose for relying on communications modes that effectively encrypt the message – enables the clear violation of numerous other rules governing the Amateur Radio Service. When it drafted Section 97.113(a)(4), the Commission could not reasonably have intended for its Amateur Radio Service rules and the Amateur Radio Service’s primary enforcement mechanism (*i.e.*, the self-policing by other Amateur Radio Service users) to be rendered toothless. The Commission can correct course by clarifying that Section 97.113(a)(4) prohibits the transmission of encrypted or encoded messages, including messages that are effectively encrypted or encoded and cannot be decoded over-the-air under reasonable propagation conditions for true meaning.

### **III. CONCLUSION**

The Commission previously has recognized the Amateur Radio Service’s “long tradition of self-regulation.”<sup>24</sup> For years, certain parties have undermined this tradition by relying on an ahistorical interpretation of Section 97.113(a)(4) that contravenes the two bedrock principles – openness and transparency – that have enabled amateur radio licensees to effectively self-regulate. Failure to clarify that the rule prohibits the transmission of effectively encrypted or encoded messages that cannot be readily decoded over-the-air for true meaning has restricted

---

<sup>24</sup> 2013 Order ¶ 6.

amateur licensees' self-enforcement efforts, thus enabling the continued violation of other rules. Accordingly, the Commission should eliminate the lingering uncertainty regarding Section 97.113(a)(4)'s meaning and clarify that the rule prohibits the transmission of effectively encrypted or encoded messages that cannot be readily decoded over-the-air for true meaning.

Respectfully submitted,

/s/ Ari Q. Fitzgerald  
Ari Q. Fitzgerald  
John W. Castle  
HOGAN LOVELLS US LLP  
Washington, DC 20004  
Tel: (202) 637-5423  
Fax: (202) 637-5910  
ari.fitzgerald@hoganlovells.com

*Counsel to New York University*

Theodore S. Rappaport, N9NB  
Founding Director, NYU WIRELESS  
David Lee/Ernst Weber Professor of  
Electrical Engineering  
New York University  
2 MetroTech Center, 9<sup>th</sup> Floor  
Brooklyn, NY 11201  
Tel: (646) 997-3403  
tsr@nyu.edu

Michael J. Marcus, N3JMM  
Sc.D. Fellow IEEE  
Marcus Spectrum Solutions, LLC  
8026 Cypress Grove Lane  
Cabin John, MD 20819  
Tel: (301) 229-7714  
mjmarcus@marcus-spectrum.com

October 24, 2019