

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

**In the Matter of** )  
 )  
**ENCRYPTION OF AMATEUR RADIO** ) **RM-11699**  
**COMMUNICATIONS** )

**To: The Chief, Wireless Telecommunications Bureau**  
**Via: Office of the Secretary**

**COMMENTS OF ARRL, THE NATIONAL ASSOCIATION  
FOR AMATEUR RADIO**

ARRL, the national association for Amateur Radio, formally known as the American Radio Relay League, Incorporated (ARRL), by counsel and pursuant to the *Public Notice*, Report No. 2983, released June 7, 2013,<sup>1</sup> hereby respectfully submits its comments in response to the *Petition for Rule Making* (the “Petition”) filed on or about March 28, 2013 by Mr. Don Rolph, AB1PH of East Walpole, Massachusetts. Mr. Rolph seeks to amend the Part 97 rules governing the Amateur Radio Service so as to permit encryption of certain Amateur Radio communications during emergency services operations and related training exercises. For its comments on Mr. Rolph’s well-stated Petition, ARRL states as follows:

**I. Introduction.**

1. The subject of encryption of Amateur Radio communications has been debated several times in the past. It is an issue about which there currently seems to be some factual misunderstanding within the Amateur Radio community. While Mr. Rolph has concisely stated his argument, it is ARRL’s considered view that there is no factual or legal basis for the assumption that encryption of transmissions (in order to obscure the meaning thereof) is

---

<sup>1</sup> Because these comments are being filed within thirty days of the date of the Public Notice, these comments are timely filed pursuant to Section 1.405(a) of the Commission’s Rules.

necessary in order to continue and enhance the utility of Amateur Radio emergency and disaster relief communications. Nor is there evidence of which ARRL is aware that served agencies are in fact unwilling or reluctant to utilize Amateur Radio as part of their emergency or disaster relief communications plans because of the encryption restrictions in the Part 97 rules. There is, moreover, a widespread, erroneous assumption that the Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191, and/or state privacy statutes<sup>2</sup> applicable to health care providers require encrypted wireless communications when transmitting private or patient information by radio. This mistaken assumption leads to the conclusion that the inability of Amateur Radio operators to encrypt the content of their transmissions in order to obscure the meaning of the transmissions renders Amateur Radio less (and decreasingly) useful to served agencies than it would be if encryption of those transmissions was permitted. For a number of reasons discussed in detail below, this conclusion is unfounded. It is *extremely* important to insure that Amateur Radio remains useful to served disaster relief and emergency communications agencies, which include health care facilities. It is just as important to insure that regulatory impediments to that volunteer work be minimized *to the extent consistent with the nature of the Amateur Radio Service*. However, in ARRL's view, after extensive review of the issue, the utility of Amateur Radio to served agencies is high indeed, and is at the present time unfettered by the inability to encrypt transmissions. Therefore, the relief sought in the instant Petition is unnecessary and contrary to the well-established character of the Amateur Service. Because the factual and legal premises for the Petition are not supportable at the present time, ARRL urges that the Petition be dismissed without action.

---

<sup>2</sup> ARRL is not aware of any instance in which any state statutory obligation has been cited as a reason for not using Amateur Radio emergency communications by any served agency or group.

### **III. Regulatory Status and History of the Encryption Prohibition.**

2. Article 25 of the international Radio Regulations (RR25.2A) includes the following provision, which constitutes a treaty obligation of administrations: “Transmissions between amateur stations of different countries shall not be encoded for the purpose of obscuring their meaning, except for control signals exchanged between earth command stations and space stations in the amateur-satellite service.”<sup>3</sup> This treaty obligation applies only to international Amateur Radio communications. Domestically, however, Section 97.113(a)(4) of the Commission’s Rules in its present iteration uses similar phraseology. Prohibited transmissions in the Amateur Radio Service include those “messages encoded for the purpose of obscuring their meaning, except as otherwise provided herein.” 47 C.F.R. § 97.113(a)(4). Until 2006, FCC rules prohibited the transmissions of messages *in codes or ciphers which are intended to obscure the meaning thereof*, except as otherwise provided in the FCC Part 97 Rules. That rule also prohibited the use of “*false or deceptive messages, signals, or identification.*” The rule section was revised by *Order*, DA 06-79, 21 FCC Rcd. 278, released January 19, 2006.<sup>4</sup> That Order amended numerous rule sections in Part 97 to conform to the current language of the International Radio Regulations, which were amended substantially at the 2003 World Radiocommunication Conference (WRC-03).

3. RR25.2A was one of the provisions of the international Radio Regulations that changed at WRC-03. Previously, RR25.2 stated "When transmissions between amateur stations of different countries are permitted, they shall be made in plain language and shall be limited to messages of a technical nature relating to tests and to remarks of a personal character for which, by reason of their unimportance, recourse to the public telecommunications service is not

---

<sup>3</sup> *WRC-03 Final Acts*, RR25.2A.

<sup>4</sup> *Amendment of Part 97 of the Commission's Rules to Implement Certain World Radio Conference 2003 Final Acts*, 71 Fed. Reg. 25981.

justified."<sup>5</sup> RR25.2A was modified at WRC-03 to read as it does now: "*Transmissions between amateur stations of different countries shall not be encoded for the purpose of obscuring their meaning, except for control signals exchanged between earth command stations and space stations in the amateur satellite service.*" Thus, the 2006 change to Section 97.113(a)(4) of the Commission's Rules was for the purpose of conforming the Part 97 rules to the amended Radio Regulations. In doing so, the Commission dropped the former "codes and ciphers" language, and amended the rule to prohibit Amateur stations, while exchanging messages with Amateur stations in other countries, from making transmissions that are "encoded for the purpose of obscuring their meaning," except for control signals exchanged between earth command stations and space stations in the amateur-satellite service. With regard to the exception in the Radio Regulations for encoded control signals exchanged between earth command stations and space stations in the amateur-satellite service, that exception was already included in the Commission's Rules<sup>6</sup> so it stayed the same.

4. The Commission, in that January, 2006 *Order* also revised Section 97.117 of the Commission's Rules<sup>7</sup> to reflect the current language of RR25.2A of the Radio Regulations.<sup>8</sup> RR25.2A, as revised at WRC-03, now states "*Transmissions between amateur stations of different countries shall be limited to communications incidental to the purposes of the amateur service, as defined in No. 1.56 [which defines the Amateur Service] and to remarks of a personal character.*"<sup>9</sup> Section 97.117 of the Commission's Rules formerly stated that "transmissions to a different country, where permitted, shall be made in plain language and shall be limited to

---

<sup>5</sup> 2000 Radio Regulations, RR25.2.

<sup>6</sup> Specifically, this exception is codified in Section 97.211(b), which provides that an Amateur Radio Station that is controlling an amateur service space station may transmit special codes intended to obscure the meaning of telecommand messages transmitted to the space station.

<sup>7</sup> 47 C.F.R. § 97.117.

<sup>8</sup> See WRC-03 Final Acts, RR25.2.

<sup>9</sup> *Id.*

messages of a technical nature relating to tests, and, to remarks of a personal character for which, by reason of their unimportance, recourse to the public telecommunications service is not justified." In order to conform Section 97.117 to the amended Article 25 of the Radio Regulations, the Commission amended Section 97.117 to state that Amateur stations may transmit communications "*incidental to the purposes of the amateur service and to remarks of a personal character.*" So, the "plain language" provision is gone internationally and domestically and the language in Section 97.117 is arguably more flexible than it was with respect to the content of communications. However, what remains in the United States is the absolute prohibition of the transmission by Amateur stations of messages "encoded for the purpose of obscuring their meaning" in Section 97.113(a)(4) of the FCC rules, a provision that is backed by (and modeled after) a U.S. treaty obligation applicable to international communications which cannot be waived by the Commission.

### **III. There is No Expectation of Privacy in the Amateur Radio Service.**

5. ARRL in 2005 investigated the encryption issue with two goals in mind: (1) to determine whether data transmitted by Amateur stations *in emergencies*, consistent with HIPAA and other privacy requirements, necessitates encryption; and (2) to determine whether medical data transmitted by Amateur stations in disaster relief situations must be protected, to the extent that it is private information subject to state privacy statutes. The premise for this was a widespread assumption and an oft-recited claim that served agencies engaged in disaster relief communications were increasingly reluctant to involve radio Amateurs in emergency traffic handling and operational communications because of the absence of any encryption opportunity. That 2005 study has recently been revisited, and the conclusions then and now are the same.

6. There has not, to the best of ARRL's knowledge, after extensive inquiry, been found any documented instance in which Amateur Radio was not used specifically because of the inability to encrypt data prior to being transmitted by radio on behalf of served agencies. ARRL was not aware of any such instances in 2005, when this issue was first studied, and it is not aware of any such instance at the present time. Nor has any emergency communications plan that has come to ARRL's attention disqualified Amateur Radio volunteers from participation for any reason whatsoever. There is every indication in fact that Amateur Radio was heavily used in hurricane relief without privacy concerns in the Gulf Coast in the fall of 2005, and it has been extensively deployed in the aftermath of major disasters since that time including Hurricane Sandy last year and in the aftermath of recent Midwestern tornadoes. Those who voice the concern have typically done so in very general terms and by references to "trends" without providing any specific example or instance of the alleged problem. Because it makes logical sense to think that an obligation to protect patient privacy would necessitate encryption of patient data before transmitting it by radio, many *radio Amateurs* do have the view that HIPAA creates an obligation to avoid using Amateur Radio because of the encryption prohibition.<sup>10</sup> The assumption is not correct as a matter of law, as is discussed below. Nor is there any quantifiable evidence of a *de facto* reluctance to incorporate Amateur Radio in emergency communications planning by medical agencies due to HIPAA requirements.<sup>11</sup>

7. It is longstanding Commission and court jurisprudence that there is no expectation of privacy with respect to the content of Amateur Radio communications. The content of Amateur

---

<sup>10</sup> There is no evidence of which ARRL is aware that this is a widespread assumption among medical professionals.

<sup>11</sup> It is impossible to evaluate or quantify the claim that health care agencies subject to HIPAA are or might be unwilling or reluctant to utilize Amateur Radio in emergency communications and disaster relief planning because of the lack of privacy inherent in the Service. Permitting encryption might remedy the concern as a practical matter, if the concern exists. Because of the complete dearth of even anecdotal evidence of the existence of that concern, however, it is not possible at this time to justify a proposed rule change to permit encryption on that basis.

communications is not protected against interception by third parties. That is a fundamental component of the Service. It is evidenced by rules, statutes and case law. The two “secrecy of communications” provisions in the United States Code are 47 U.S.C. § 605, pertaining to unauthorized publication or use of intercepted communications, and 18 U.S.C. § 2510 *et seq.* the Electronic Communications Privacy Act (ECPA). Section 605 of the Communications Act of 1934 makes it unlawful to receive (or transmit) any interstate or foreign communications by wire or radio, and then to divulge the existence, contents, substance, or meaning of that communication to third parties. However, Amateur Radio communications are *specifically exempt from this provision*, as are other communications “intended for use by the general public.” Similarly, the ECPA, which includes in the United States criminal code a prohibition of the interception of certain communications including radio and other electronic transmissions, *exempts Amateur Radio communications* from those restrictions.<sup>12</sup>

8. The public nature of Amateur Radio communications is clear from these statutes, both of which differentiate Amateur Radio from other types of communications, the contents of which are expected to remain private. This illustrates Congress’ understanding of the fundamental nature of Amateur Radio as being a radio service whose communications are *not entitled to privacy*. That holding was clear as well from several court decisions which, long ago, established that there is no expectation of privacy in Amateur Radio communications. In *United States v. Rose*, 669 F.2d 23 (1st Cir. 1982), *cert. denied*, 459 U.S. 828, 103 S. Ct. 63, 74 L. Ed. 2d 65 (1982), the 1<sup>st</sup> Circuit United States Court of Appeals held that there is no reasonable expectation

---

<sup>12</sup> There are practical difficulties in enforcement of the secrecy of communications provision of the Communications Act. It does not proscribe interception *per se*, but only interception coupled with subsequent disclosure. The ECPA does proscribe interception *per se*. Because there is no recourse at all against someone who divulges the content of an Amateur transmission, health care providers subject to HIPAA could be reluctant as a matter of fact to incorporate Amateur Radio in emergency communications planning in advance of an emergency. ARRL does not have facts quantifying this concern, however.

of privacy in communication transmitted by ham radio. In that case, an employee of the Enforcement Bureau of the Commission intercepted a suspicious radio transmission, which he determined had been transmitted by an Amateur radio station. He turned the transmission over to the United States Coast Guard, which determined the message to be related to a scheme for the delivery of illegal drugs. The Coast Guard agents subsequently arrested the appellants involved in the illegal transaction and recovered marijuana. As part of their case at the trial court, the appellants filed a motion to suppress the discovery of the marijuana as an evidentiary matter, arguing that the FCC's interception of the information violated the federal wiretapping statute, 18 U.S.C. § 2510 *et seq.* The trial court found that the appellants had no subjective or reasonable expectation of privacy. The Court of Appeals agreed and upheld the ruling of the lower court. *Id* at 27. In reaching their conclusion, they stated that a reasonable person would not expect his or her words voiced over an Amateur radio frequency to be heard only by the few people for whom the message was intended. *Id* at 26; See also *United States v. Sugden*, 226 F.2d 281, 286 (9<sup>th</sup> Cir. 1955), *aff'd*, 351 U.S. 916, 76 S. Ct. 709, 100 L.Ed. 1449 (1956). Therefore, even if the Commission was to modify the rules regarding encryption, that would not, in and of itself, change the well-established premise that *there is no expectation of privacy in the Amateur Service*. The public nature of Amateur Radio communications is an inherent characteristic of the Service. It is also a component of the self-regulatory history of Amateur Radio. The ability to monitor ongoing Amateur communications, to determine, if for no other purpose, whether or not the ongoing communications are between or among licensed radio amateurs, is of value. It is for this reason that the Commission requires that, where unspecified digital codes are used by radio amateurs, the characteristics of digital emissions should be published and therefore available to radio Amateurs generally. *See*, 47 C.F.R. § 97.309(b) and the discussion *infra*.

#### **IV. Not All Encryption is Prohibited in the Amateur Radio Service.**

9. Not all encryption of Amateur Radio communications is prohibited by Section 97.113(a)(4). At the same time that ARRL was studying the encryption issue from the perspective of emergency communications, some radio Amateurs interested in High Speed Multimedia (HSMM) and experimentation with broadband digital wireless communications expressed concerns that their inability to make broad use of encryption generally for computer-to-computer communications inhibited that experimentation. They were especially concerned with encryption for purposes of authentication and passwords to keep unlicensed users out of Amateur digital communications networks. At the time, however, encryption of the text of messages in computer-to-computer Amateur communications seemed to directly challenge the “codes and ciphers” prohibition in the rules, since the specific intention appeared to be to obscure the meaning of the communication. However, the ability to encrypt for the purpose of authentication of users in a data network, as discussed below, appears to be permissible, and the current Section 97.113(a)(4) has not been determined (to date) to inhibit HSMM/ wireless broadband experimentation in the Amateur Radio Service.

10. The Part 97 rules permitting the use of encoding of transmissions *for control purposes* are specific exceptions to the general prohibition of messages which are encoded to obscure their meaning. However, it can be inferred reasonably from these exceptions that some encoding does not come within the prohibition of Section 97.113(a)(4) of the Commission’s rules. ARRL has previously advised members, following discussions with Commission Enforcement Bureau and Wireless Bureau staff, that encoding *exclusively for authentication purposes* does not violate Section 97.113(a)(4). The use of encryption to authenticate the identity of participants who are entitled to use Amateur Radio data networks, for example, is not intended

to obscure the meaning of a transmission. Rather, it is for the purpose of insuring control and prohibiting unauthorized access to Amateur stations and networks of stations. Therefore, encryption for purposes of authentication of a user and prevention of access by unlicensed or unauthorized persons is arguably the same as the goal of the encryption prohibition in Section 97.113(a)(4) in the first place: It allows Amateurs to police their own allocations and prevent intruders, as indeed they must do in order to maintain control of their licensed facilities.

11. While Section 97.113(a)(4) is and always has been apparently tied to the Radio Regulations, and it is most directly applicable to High Frequency band (HF) communications (much of which is international), the Commission's Rule is not limited only to HF, or to domestic communications.<sup>13</sup> It is applicable to all communications. The Commission has expressed less concern in recent years about the "monitorability" of Amateur communications at 50 MHz and above (which are primarily, *though not exclusively* domestic in nature).<sup>14</sup> However, the authority for the use of unspecified digital codes is not a *carte blanche* to use encryption, even above 50 MHz. Section 97.309(b) carefully does not permit an Amateur licensee to use an unspecified digital code for the purpose of obscuring the meaning of *any* communication. The Commission attempted to reach a balance between allowing experimentation with new digital

---

<sup>13</sup> The Commission in the past took the position that the old, now-deleted "codes and ciphers" prohibition of 97.113(a)(4) was based on the international Radio Regulations, and was premised on the fact that some Amateur communications are international, rather than domestic. In an Order, DA 95-2106, released October 11, 1995, the Commission approved the use of CLOVER, G-TOR and PACTOR digital codes. In that proceeding, the Commission said that the primary purpose of those digital modes is to facilitate communications using already authorized digital codes, emission types, and frequency bands. It noted that the technical characteristics of those operating modes had been documented publicly for use by Amateurs, and commercial products are already available using these codes. Therefore, it found, including the three codes in the Part 97 rules would not "conflict with the Commission's objective of preventing the use of codes and ciphers intended to obscure the meaning of the communication." In a footnote to that statement, the then-Chief, Wireless Telecommunications Bureau, stated that the HF bands are widely used for international communications. It cited the Radio Regulations as requiring that transmissions between amateur stations of different countries be in plain language. Therefore, it stated, Section 97.113(a)(4) prohibited amateur stations from transmitting messages in codes and ciphers intended to obscure the meaning thereof.

<sup>14</sup> See 47 C.F.R. § 97.309(b).

codes and continuing to prohibit the use of encryption to obscure message content. The available evidence indicates that it has succeeded in this effort.

## **V. HIPAA Requirements Do Not Necessitate Encryption of Amateur Radio Communications.**

12. The Health Insurance Portability and Accountability Act of 1996 has no application to Amateur Radio *per se*. The “covered entities” that are obligated to follow its requirements do not include Amateur Radio licensees. Covered entities are as specified below:

---

### **A Covered Entity is one of the following:**

#### **A Health Care Provider**

This includes providers such as:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

...but only if they transmit any information in an electronic form in connection with a transaction for which the Department of Health and Human Services has adopted a standard.

#### **A Health Plan**

This includes:

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans’ health care programs

#### **A Health Care Clearinghouse**

This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Amateur Radio operators themselves therefore have no obligations under HIPAA whatsoever, because they are not “Covered Entities.”<sup>15</sup>

---

<sup>15</sup> As discussed earlier, it is not clear to what extent covered entities might perceive their obligations to protect patient privacy to involve the exclusion of Amateur Radio because Amateur Radio communications have no expectation of privacy and no ability to encrypt for the purpose of obscuring the content of a transmission. However, as stated above, this perception would be false as a matter of law, impossible to quantify in any case, and as such should not form the basis for a regulatory change in Part 97 by the Commission.

13. Under HIPAA, Covered Entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by administrative agency rules adopted pursuant to the Statute. The Department of Health and Human Services (HHS), which administers HIPAA and has rules which apply it, does not consider facility restructuring to be a requirement under HIPAA. For example, the Privacy Rule adopted by HHS does not require the following types of structural or systems changes:

1. Private rooms.
2. Soundproofing of rooms.
3. ***Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.***
4. Encryption of telephone systems.

Therefore, it is not necessary for Covered Entities to utilize encrypted wireless communications to avoid interception by third parties. Neither do telephone systems used for electronic transmission of private patient information need to be encrypted. However, Covered Entities must implement reasonable safeguards to limit incidental, and avoid prohibited uses and disclosures, but the HHS privacy rule does not require that all risk of protected health information disclosure be eliminated. Covered Entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, Covered Entities are admonished to assess potential risks to patient privacy, as well as to consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered Entities also may take into consideration the steps that other prudent health care and health information professionals are taking to protect patient privacy. *There is no literature that ARRL has found after diligent inquiry that would suggest that Covered Entities should not, during or after*

*emergencies, utilize Amateur Radio to transmit via radio unencrypted, protected health information.* ARRL has not to date encountered any Covered Entity which has taken the position that using Amateur Radio unencrypted communications should be avoided in order to reasonably safeguard protected health information. Nor in ARRL's experience is there any widespread or systemic plan to exclude the use of Amateur Radio communications in emergencies as a means to insure the protection of health information.

#### **VI. The Premises for the Petition Are Not Supported.**

14. The instant Petition cites Paragraph 39 of the Commission's *Report* in Docket 12-91, 27 FCC Rcd. 10039 (2012) (Report to Congress on Amateur Radio emergency communications) for the proposition that certain cited impediments to enhanced Amateur Radio emergency communications work can be addressed through the rulemaking process. Paragraph 37 of that Report states as follows:

The Commission's rules prohibit the transmission by amateur stations of "messages encoded for the purpose of obscuring their meaning." Commenters argue that transmission of sensitive data, such as medical information that is subject to privacy requirements, is often a necessary aspect of emergency response, and therefore the use of encryption should be permitted under appropriate circumstances, such as by credentialed operators.

(footnotes omitted)

The Petition then cites the Commission's admonition from the Docket 12-91 Report that: "Commission rules that may be an impediment to enhanced amateur service emergency communications can, as the ARRL notes, be considered through the Commission's rulemaking process". The Petition then cites Section 97.113(a)(4) of the Rules and requests modification thereof regarding encryption. It notes that encryption is permitted for satellite control link communications pursuant to Section 97.211(b) and as well for model craft radio control pursuant to Section 97.215. It argues (without citation of authority for the assertion) that "agencies served

by amateur radio communication during emergencies perceive” that encryption is required, including “specific patient information covered by HIPAA, identification of sheltered persons, etc.” The Petition argues as well (again without citation of authority) that certain emergency information is required for tactical purposes to be encrypted, such as “logistical information: (movement of food, medical supplies, certain movements of personnel).” It further suggests that for “national security” reasons certain emergency communications should be encrypted.

15. Finally, the Petition argues that Australian Amateur Radio rules are more appropriate than are current United States Amateur regulations on this issue. Australia’s rule on encryption is very much like Section 97.113(a)(4), except that among the exemptions from the prohibition of encoding for the purpose of obscuring the meaning of the signals are “intercommunications when participating in emergency services operations or related training exercises.” The Petition asks for similar wording, so that exempt from the encryption prohibition in Section 97.113(a)(4) would be “intercommunications when participating in emergency services operations or related training exercises which may involve information covered by HIPAA or other sensitive data such as logistical information concerning medical supplies, personnel movement, other relief supplies or any other data designated by Federal authorities managing relief or training efforts.”

16. While the fundamental premises for the relief requested in the instant Petition for Rule Making are not illogical, neither are they evidenced by any facts or legal requirements. The Petitioner assumes, but does not demonstrate, that there is a problem for some served agencies in utilizing Amateur Radio communications in emergency and disaster relief situations, and there is a reluctance to incorporate Amateur Radio communications in emergency communications plans due to the inability to encrypt those communications in such a way as to obscure the meaning of the communications. ARRL would suggest, with due respect for the Petitioner’s good-faith effort

here, that there is insufficient evidence of his premises to warrant the relief requested in the Petition, as argued above.

## **VI. Conclusions.**

17. Permitting encryption for the purpose of obscuring the meaning of an Amateur Radio transmission in international communications would be contrary to the international Radio Regulations, which are treaty obligations of the United States and are binding on the United States. The domestic regulation applicable to all Amateur Radio communications regulated by the Commission is modeled after the Radio Regulations. Permitting encryption generally would be contrary to the well-established premise that there is no expectation of privacy of Amateur communications. The case law establishing that Amateur Radio communications are not entitled to privacy would not change merely because encryption may be permitted by the Commission.

18. Communications encrypted for the purpose of obscuring the meaning of a transmission are and have been consistently prohibited by the Commission's Rules for the purpose of preventing abuses by non-licensees. No action should be taken in any event which might detract from effective efforts to improve the level of enforcement in the Amateur Service. A rule change broadly permitting encryption which might make enforcement more difficult should not be effectuated without a much more compelling factual record than now exists.

19. Not all encryption is prohibited by the current rules. Commission staff has informally taken the position in the past that encryption of Amateur communications for authentication, such as the use of passwords and digital coding of transmissions so that an Amateur Radio data network can verify and regulate the identity of persons accessing the network (to insure, for example, that they are in fact Amateur Radio licensees), is not prohibited by the Commission's rules. It is easily arguable in any case that encryption for authentication is necessary in order to

protect the integrity of the network itself, and specifically to insure that control is maintained over the network, as the licensees who are the control operators of transmitters in that network are obligated to do pursuant to Section 97.105 of the Commission's Rules. Nor does that constitute encryption for the purpose of obscuring the meaning of the communications. It has long been held that repeater operators can use authentication codes for control functions for repeaters, and the Part 97 Rules specifically allow encoded transmissions for control of Amateur space stations and model craft.

20. The reason why encryption for those specific purposes is permissible, however, is solely because the transmissions are not encrypted "for the purpose of obscuring the meaning of a message." Instead the encryption is intended only to prevent unauthorized access, and the encryption of control signals and coding for authentication of a transmission is not related to the message transmitted, which cannot be obscured intentionally. To the extent that the interpretation of the Section 97.113(a)(4) rule is based on an individual's intent relative to the "meaning" of a message, the rule is somewhat subjective and it does not lend itself to a "bright line" application. Neither, in effect, are the obligations on medical facilities under HIPAA specifically articulated. It is clear that radio Amateurs have no obligations under HIPAA because they are not Covered Entities. There is no evidence that ARRL has discovered to date that any Covered Entity subject to HIPAA perceives its obligation to protect patient privacy to necessitate the exclusion of Amateur Radio because Amateur Radio communications have no expectation of privacy or because Amateur licensees who are volunteers have no ability to encrypt for the purpose of obscuring the content of a transmission. While it is a reasonable argument that obscuring patient data by encryption would not be equivalent to obscuring the meaning of a transmission (because the remainder of the transmission is not obscured and it is clear that it would be an Amateur

transmission), the Commission has not *formally* spoken on that issue. If at some time in the future it is deemed necessary for radio Amateurs to protect the privacy of individuals whose medical data may be transmitted by Amateur Radio in the context of an emergency or disaster or in the aftermath of one, the Commission may be asked to revisit this matter. It is urgent that Amateur Radio continue to be an essential component of disaster and emergency communications planning and that served agencies, including medical facilities, perceive that the utility of Amateur Radio is unfettered by regulations prohibiting encryption. At the present time, however, there is no factual justification for the relief requested that ARRL has been able to find. Nor is there any evidence apparent to ARRL of the perception that privacy obligations in emergency communications or disaster relief communications, including HIPAA obligations attendant to Amateur Radio communications on behalf of Covered Entities, are an inhibiting factor in the incorporation of Amateur Radio in emergency communications planning. HIPAA cannot reasonably be argued to necessitate encryption in the Amateur Service. Quite the contrary: Amateur Radio is highly, and increasingly relevant to emergency and disaster relief planning.

Therefore, given the foregoing, ARRL, the national association for Amateur Radio respectfully requests that the instant Petition be dismissed without further action.

Respectfully submitted,

**ARRL, THE NATIONAL ASSOCIATION FOR  
AMATEUR RADIO**

225 Main Street  
Newington, CT 06111-1494

By: Christopher D. Imlay  
Christopher D. Imlay  
Its General Counsel

BOOTH, FRERET, IMLAY & TEPPER, P.C.  
14356 Cape May Road  
Silver Spring, MD 20904-6011  
(301) 384-5525

July 8, 2013

**CERTIFICATE OF SERVICE**

I, Christopher D. Imlay, pursuant to Section 1.405(a) of the Commission's Rules, do hereby certify that I caused to be mailed, via first class U.S. Mail, postage prepaid, a copy of the foregoing to the following Petitioner, this 8<sup>th</sup> day of July, 2013.

Mr. Don Rolph, AB1PH  
8 Patty Ann Place  
East Walpole, MA 02032

---

Christopher D. Imlay