

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Before the
Federal Communications Commission
Washington, D.C. 20554

In re Petition for Rulemaking) Proceeding RM-11699
Don Rolph) Encryption of Amateur Radio Communications
Petitioner) REPLY COMMENT
Filed June 7, 2013) to filing by ARRL, the National
Association for Amateur Radio dated
7/8/2013
)
)
)
)

I submit these Reply Comments in response to the July 8, 2013, filing by ARRL, the National Association for Amateur Radio (“ARRL”), in the captioned proceeding.

I. THE ENCRYPTION PROHIBITION DOES LEAD TO AMATEUR
RADIO NOT BEING USED IN EMERGENCIES

ARRL states that it is unaware of any evidence “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”.

In fact several filers in this proceeding cite instances where amateur radio is not used in emergencies specifically because of the prohibition against encryption¹, and other filers cite

¹ E.g., filings by Jon Perelstein (6/20/2013); Michael Brown (6/24/2013); Chris McCormick (6/25/2013); Steve Schroder (6/25/2013); and George Blakeslee (6/28/2013).

1 instances where an emergency communications need is unmet or sensitive information is
2 transmitted in the clear due to the encryption prohibition².

3
4 II. THE STANDARD FOR ADOPTION OF THE PROPOSED RULE
5 SHOULD BE "PUBLIC INTEREST, CONVENIENCE, OR NECESSITY"

6 In its filing ARRL states that since there is insufficient evidence that the encryption
7 prohibition "is a problem for some served agencies in utilizing Amateur Radio communications
8 in emergency and disaster relief situations", there is no need for the petitioner's requested rule
9 change. However, the appropriate standard for adopting a new rule should not be whether
10 there is "a problem", but rather whether the rule change would be in the "public interest,
11 convenience, or necessity"³.

12 It is in the public interest that sensitive information related to law enforcement operations
13 be kept private, as the effectiveness of the operations could be compromised if this information
14 were available to the public. It is in the public interest for logistical coordination of the
15 transportation of supplies in a disaster relief operation to be kept private, as the security of the
16 operation could be compromised (e.g., due to risk of robbery or looting) if this information were
17 to be made public. It is in the public interest for personally identifiable health information to be
18 kept private, because people deserve the privacy of this kind of personal information. And
19 these are just three examples; there are innumerable situations where the public is best served
20 by keeping sensitive information private.

21 Within the scope of the purpose of the Amateur Radio Service is providing emergency
22 communications⁴, and transmissions necessary to meet essential communication needs and to
23

24
25 ² E.g., filings by William Hecker (6/24/2013), and James Fenn (6/27/2013).

³ 47 USC § 303

⁴ 47 CFR § 97.1(a)

1 facilitate relief actions are explicitly authorized in the Commission's rules⁵. When the content of
2 a message is such that the public interest is served by keeping the content private, and when
3 the message is passed via amateur radio, it is in the public interest for the Commission's rules
4 to permit the radio operator to employ means to keep that content private.

5
6 III. PERMITTING ENCRYPTION WON'T OBSCURE THE
7 IDENTIFICATION OF THE COMMUNICATING STATIONS

8 ARRL states that the "ability to monitor ongoing Amateur communications, to determine,
9 if for no other purpose, whether or not the ongoing communications are between or among
10 licensed radio amateurs, is of value." However, permitting encryption of certain communications
11 would not relieve the operator of the responsibility to identify his station "for the purpose of
12 clearly making the source of the transmissions from the station known to those receiving the
13 transmissions"⁶. The effect of this rule is that required station identification would not be
14 encrypted.

15 Furthermore, in the event the Commission were to have any concern about whether the
16 content of a transmission – whether or not encrypted – is in compliance with the Commission's
17 rules, the Commission can simply contact the licensee and request such information as it
18 deems appropriate for its investigation⁷.

19 Even if the content of a transmission is encrypted, there are many ways to detect an
20 inappropriate use. In the case of a *bona fide* emergency, the existence of that emergency
21 would be well known. Since training would only occur from time to time, any regular or recurring
22 encrypted use of amateur radio channels would indicate that a rules violation has likely occurred
23 and that further investigation by the Commission may be warranted.

24
25

⁵ 47 CFR § 97.111(a)(2)

⁶ 47 CFR §97.119(a)

⁷ 47 USC 403

1 It is relevant to note that any regular or recurring use of encryption to communicate
2 prohibited content would require the conspiracy of at least two amateur operators (since there
3 no point in transmitting encrypted content when there is no recipient); based on the historical
4 compliance history in the Amateur Radio Service, this is extremely unlikely to occur at all, and
5 would certainly not occur often enough to be an impediment to permitted communications.

6
7 IV. HIPAA⁸ COMPLIANCE OFTEN DOES REQUIRE
8 ENCRYPTION OF RADIO TRANSMISSIONS

9 ARRL incorporated in its filing content from a Department of Health and Human Services
10 (HHS) webpage⁹ which seemed to state that HHS does not require encryption of wireless or
11 other emergency medical radio communications which can be intercepted by scanners. That
12 webpage content does not have the force of law, and unfortunately the web content is not as
13 clear as it could have been about HIPAA requirements.

14 Two provisions of HIPAA relevant to transmission of Protected Health Information over a
15 radio channel are the Security Rule¹⁰ and the Privacy Rule¹¹. The Security Rule explicitly
16 applies to Electronic Protected Health Information (“EPHI”)¹², which is defined as information
17 that is transmitted by or maintained in electronic media¹³. Included within the scope of EPHI is
18 “information that is created, received, maintained, or transmitted by or on behalf of the health
19 care component of the covered entity”¹⁴. The Security Rule requires that a covered entity or
20 business associate “implement a mechanism to encrypt and decrypt electronic protected health
21
22

23 ⁸ The Health Insurance Portability and Accountability Act of 1996,

⁹ <http://www.hhs.gov/ocr/privacy/hipaa/faq/safeguards/197.html>, retrieved 7/23/2013

24 ¹⁰ Codified at 45 CFR § 164.302 *et seq*

¹¹ Codified at 45 CFR § 164.500 *et seq*

¹² 45 CFR § 164.302

25 ¹³ 45 CFR § 160.103, definition of *Electronic Protected Health Information*

¹⁴ 45 CFR § 164.105(a)(2)(i)(D)

1 information¹⁵. In summary, the Security Rule *does* require the encryption of EPHI sent over
2 any electronic medium, including a radio channel that can be intercepted by a scanning
3 receiver.

4 However, the Security Rule does not apply to certain transmissions if the information
5 being exchanged did not exist in electronic form immediately before the transmission¹⁶. For
6 example, the Security Rule would not apply to a voice transmission over a radio channel, *but*
7 *the Privacy Rule would still apply to this kind of voice transmission.*

8 The Privacy Rule provides that a covered entity must have in place appropriate
9 administrative, technical, and physical safeguards to protect the privacy of protected health
10 information; a covered entity must reasonably safeguard protected health information from any
11 intentional or unintentional use or disclosure that is in violation of the standards, implementation
12 specifications or other requirements of this subpart; and a covered entity must reasonably
13 safeguard protected health information to limit incidental uses or disclosures made pursuant to
14 an otherwise permitted or required use or disclosure¹⁷. Although the Privacy Rule doesn't
15 *explicitly* require that encryption be used on a voice channel, in some cases of emergency
16 communications over an Amateur Radio Service channel (when no other suitable
17 communications channel is available) *the only practical way to comply with the Privacy Rule will*
18 *be the use of encryption.* Therefore, when protected health information must be communicated
19 (e.g., to assist with the treatment of a specific individual for whom medical records are only
20 available at a remote location), it is in the public interest to permit encryption to comply with the
21 Privacy Rule.

22
23
24
25

¹⁵ 45 CFR § 164.312(a)(2)(iv)

¹⁶ 45 CFR § 160.103, definition of *Electronic media*

¹⁷ 45 CFR § 164.530(c)

1 V. CONCLUSION

2 For the reasons stated in these Reply Comments, the Comments filed by ARRL (and by
3 many others expressing essentially the same views) do not impeach the arguments stated in
4 Mr. Don Rolph's Petition for Rulemaking that it is clearly in the public interest to permit the use
5 of encryption or other means to obscure the meaning of messages transmitted via the Amateur
6 Radio Service in certain emergency operations (and in training exercises for such operations).

7
8 Dated this 23rd day of July, 2013.

9 Respectfully,

10
11 /signature/

12 David A. Behar
13 P.O. Box 40204
14 Spokane, WA 99220

15 I have mailed a copy of this Reply Comment to ARRL via USPS First Class Mail before
16 submitting this filing.

17 /signature/

18 David A. Behar
19 P.O. Box 40204
20 Spokane, WA 99220
21
22
23
24
25