

Right to Know Advisory Committee
Encryption Subcommittee
August 15, 2012
Meeting Summary

Convened 9:20 a.m., Room 438, State House, Augusta

Present:

Rep. Joan Nass (arrived 9:20 a.m.)
Linda Pistner
Perry Antone
AJ Higgins (arrived 9:30 a.m.)
Joe Brown
Mike Cianchette
Mal Leary
Judy Meyer

Staff:

Curtis Bentley

Introductions

Linda Pistner called the meeting to order at 9:20 a.m. and asked all the members to introduce themselves.

Review of federal and state laws pertaining to encryption, Curtis Bentley, staff.

At the request of the subcommittee, Curtis Bentley provided information about the applicability of federal and state laws to the encryption (scrambling) of certain police and first responder radio transmissions. The subcommittee discussed the potential applicability of Maine's Freedom of Access Act (1 MRSA, chapter 13) and Maine's law regarding the inception of wire and oral communications (15 MRSA, chapter 102). The subcommittee asked Assistant Attorney General Laura Yustak Smith about the applicability of the state prohibition against the interception of oral communications to en route radio transmissions. Ms. Smith said that encrypted radio transmissions might be considered "oral communications" as defined in the statute because the act of encrypting radio transmissions could indicate an expectation that the communications are not open to the public. Title 15 MRSA § 709, sub-§ 5 defines "oral communications" to mean "any oral communications uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."

In sum, Mr. Bentley did not find a federal or state statute or regulation that authorizes, prohibits or provides guidance on the encryption of police or first responder radio transmissions. It appears that it is within the discretion of an agency or entity making such radio transmissions whether or not to scramble a particular radio transmission.

Department of Public Safety, Maine State Police, Major Grotton, Lt. Pomelow, Col. Williams.

Major Grotton said the goal of the department is to keep general radio transmissions open and transparent to the public and that there are no plans to encrypt anything beyond what has always been encrypted. Moving to a digital system will require people who want to listen in on those calls to use a compatible scanner but nothing new will be encrypted. Major Grotton said that encrypted radio transmissions are not recorded so there wouldn't be a record for purposes of FOA. He was not aware of any agency that plans to increase its use of encryption.

Major Christopher Grotton was unaware of any investigations under the interception of wire and oral communication laws and felt that the kind of technology available today was not contemplated when those laws were enacted.

In response to a question from the subcommittee, Major Grotton estimated that approximately 1-2% of all radio transmissions (approximately 55 tactical operations annually) are encrypted. He noted that it is critical they remain encrypted and the department would be very concerned about anyone breaking into those transmissions.

Major Grotton said it is the on-scene commander who makes the decision to switch to an encrypted frequency. He thought the public would be aware of an encrypted transmission because the initial call would be audible and then there wouldn't be any other radio traffic regarding that matter. If encryption becomes too prevalent it should be reviewed as a policy issue.

Lt. Don Pomelow informed the subcommittee that the state will need a number of FCC licenses for its digital bandwidth; each municipality and county must obtain its own license. FCC licenses do not dictate the use of encryption.

Col. Williams stated that currently there isn't an issue with encryption and there are no plans to increase its use because the police derive benefits from having transmissions open to the public. He provided examples of receiving information from the public in response to radio calls and the public avoiding accident scenes. He said that there are ways for police to communicate now without the use of the radio but they want and need the public to hear what is going on.

Col. Williams cautioned the subcommittee against recommending a change in the law that would encourage officers to use private means of communication. He stated that the department only uses encryption for public safety and the safety of the department's officers and that they will continue to find ways to protect officer and public safety even if the use of encryption is regulated in the future.

Subcommittee general discussion

Mal Leary stated that there are real concerns about encryption and there needs to be accountability as encryption has been used at the federal level and by other states to avoid the detection of illegal behavior such as racial profiling and some agencies have started encrypting all calls.

A.J. Higgins suggested that there needs to be a balance between the needs of the police/first responders and public access. This is a valid issue to explore even if it isn't a huge issue right now. He felt this is a community relations issue.

Perry Antone said that there has been considerable confusion caused by the switch from analogue to digital and that going digital does not mean increased encryption. He also said there isn't anything in law that prevents the use of encryption but agencies have used it very little because it is important for them to freely share information between agencies. Radio dispatches are the most efficient way to get information to and from agencies and encryption limits that efficiency. Mr. Antone expressed concern that the subcommittee is working off assumptions that something will happen when there is no evidence that going from analogue to digital will encourage more encryption. He stated that the law doesn't need to be changed because there isn't a problem to fix and any changes could have far reaching unforeseen affects. He pointed out that if en route radio transmissions become "public records" then we will have to figure out a way to protect confidential information sent via these transmissions as is currently required for written records which isn't feasible.

Linda Pistner suggested that FOA was not intended to deal with oral communications and if there is a policy issue to resolve it may be better dealt with under some other section of law.

Judy Meyer reiterated that she just wants to maintain the current level of public access because that is working for everyone. She would like to see the current practice of encrypting put in writing either in policy or statute so everyone is aware of the protocol and also to reduce the possibility that the current practices will be changed with the arrival of new technology. Ms. Meyer agreed that there isn't a problem in Maine yet but it has become one in other states so should do something now.

Joe Brown said that we need to be careful not to impede police operations by removing the ability to encrypt certain types of calls. He suggested that the subcommittee could continue to watch the issue and if a problem arises. He said there isn't a problem that needs to be addressed today.

Mike Cianchette felt that what is happening out there now is working so it might be worthwhile to ask State Police to formally adopt a policy or guidelines for encrypting transmissions. Putting the current practice on paper might be helpful.

Subcommittee actions. The Encryption Subcommittee took the following actions.

A.J. Higgins made a motion to recommend to the full committee that no changes be made to current law. The motion was seconded by Joe Brown. The subcommittee voted 8-0 in favor of the motion.

The subcommittee unanimously agreed to recommend to the full RTK Committee that it send a letter to the Board of Trustees of the Maine Criminal Justice Academy requesting that it adopt an encryption policy for police that reflects the current practice and to have the board report back to the RTK Committee on any decisions or actions taken pursuant to this request.

Next meeting.

The subcommittee did not schedule an additional meeting.

The meeting was adjourned at 11:05 a.m.

Respectfully submitted,
Curtis Bentley

G:\STUDIES 2012\Right to Know Advisory Committee\Meeting summaries\Summary Encryption Subcommittee July 16 2012.doc