One of the problems with totally secure communication is that often communications must occur between groups such as sheriff's department, local police, state police, fire departments, and possibly other emergency personnel. Consequently, a law enforcement agency such as the sheriff's department may utilize both secure and open communication channels.

Cellular transmission tends to be fairly secure simply because it is one-to-one communications. The voice communication is not of itself encrypted, so it can potentially be monitored. However, each phone connection has a unique configuration which changes each time and consequently is difficult to eavesdrop. (Most eavesdropping occurs on either end when other people overhear the conversation.)

Radio and satellite transmission utilize standard frequencies, and this is difficult to make it secure. However, there are digital and encrypted devices that can be purchased and utilized. Data for these types of devices is Where can be encrypted for transmission. Laptop computers inside police vehicles can be set up with digital certificates and SSL transmission. The data that is transmitted is encrypted and secure. Again for radio communications eavesdropping can occur when the officer has his radio communication transmitted on a loud open speaker. Officers could be provided with earplug speakers for more secure conversations.