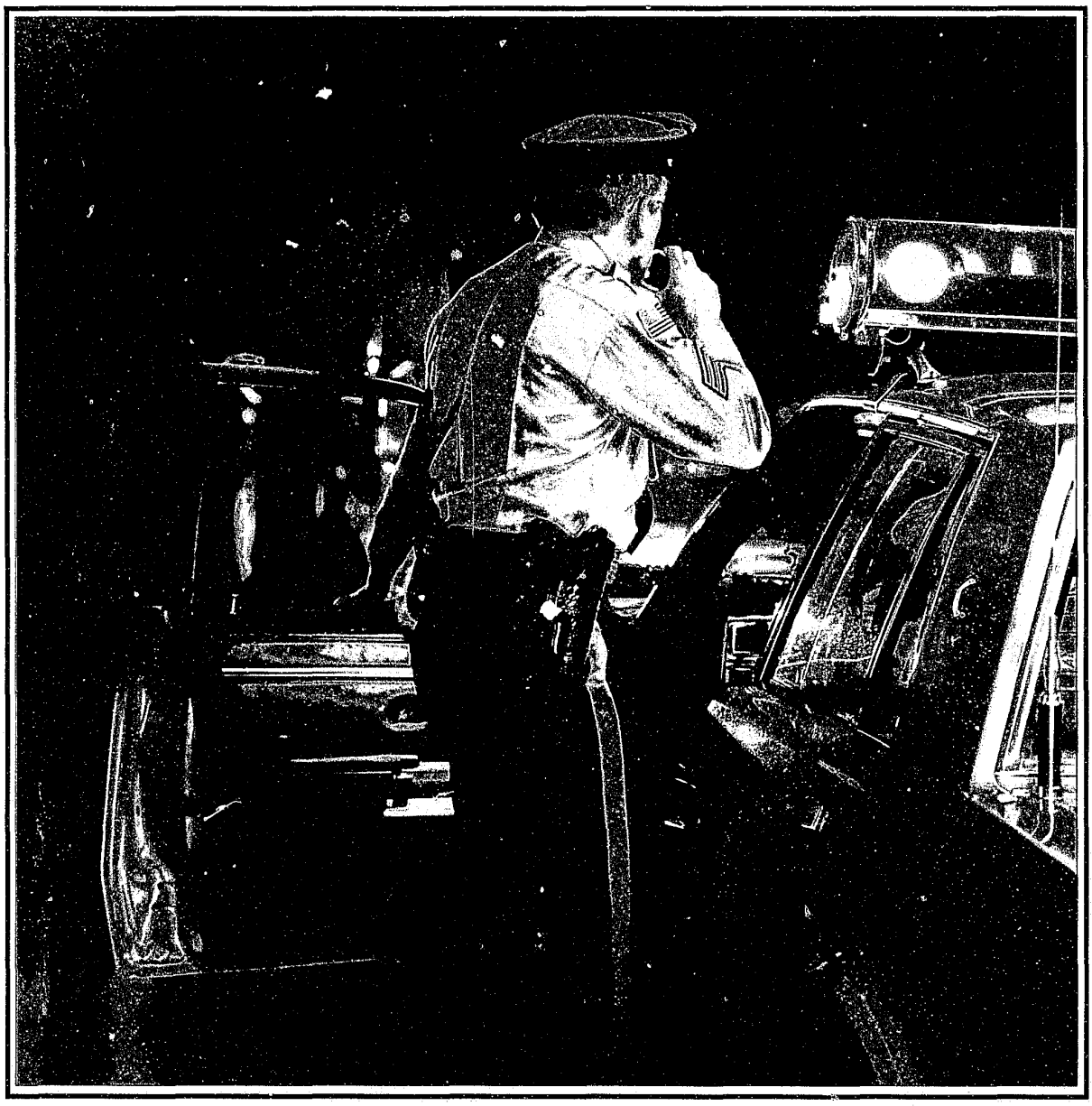
U.S. Department of Justice
Federal Bureau of Investigation

AUGUST 1995

FBI Law Enforcement BULLETIN



Communication Security

August 1995
Volume 64
Number 8

United States
Department of Justice
Federal Bureau of
Investigation
Washington, DC 20535

Louis J. Freeh
Director

Contributors' opinions and statements should not be considered as an endorsement for any policy, program, or service by the FBI.

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget.

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Avenue, N.W., Washington, D.C. 20535. Second-Class postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to *FBI Law Enforcement Bulletin*, Federal Bureau of Investigation, FBI Academy, Quantico, VA 22135.

Editor
Stephen D. Gladis, Ph.D.
Managing Editor
Kathryn E. Sulewski
Art Director
John E. Ott
Associate Editors
Andrew DiRosa
Julie R. Linkins
Kimberly J. Waggoner
Assistant Art Director
Brian K. Parnell
Staff Assistant
Stephanie L. Lowe

Internet Address:
fbileb@justice.usdoj.gov

Cover photo
© Sigarms

FBI Law Enforcement B·U·L·L·E·T·I·N

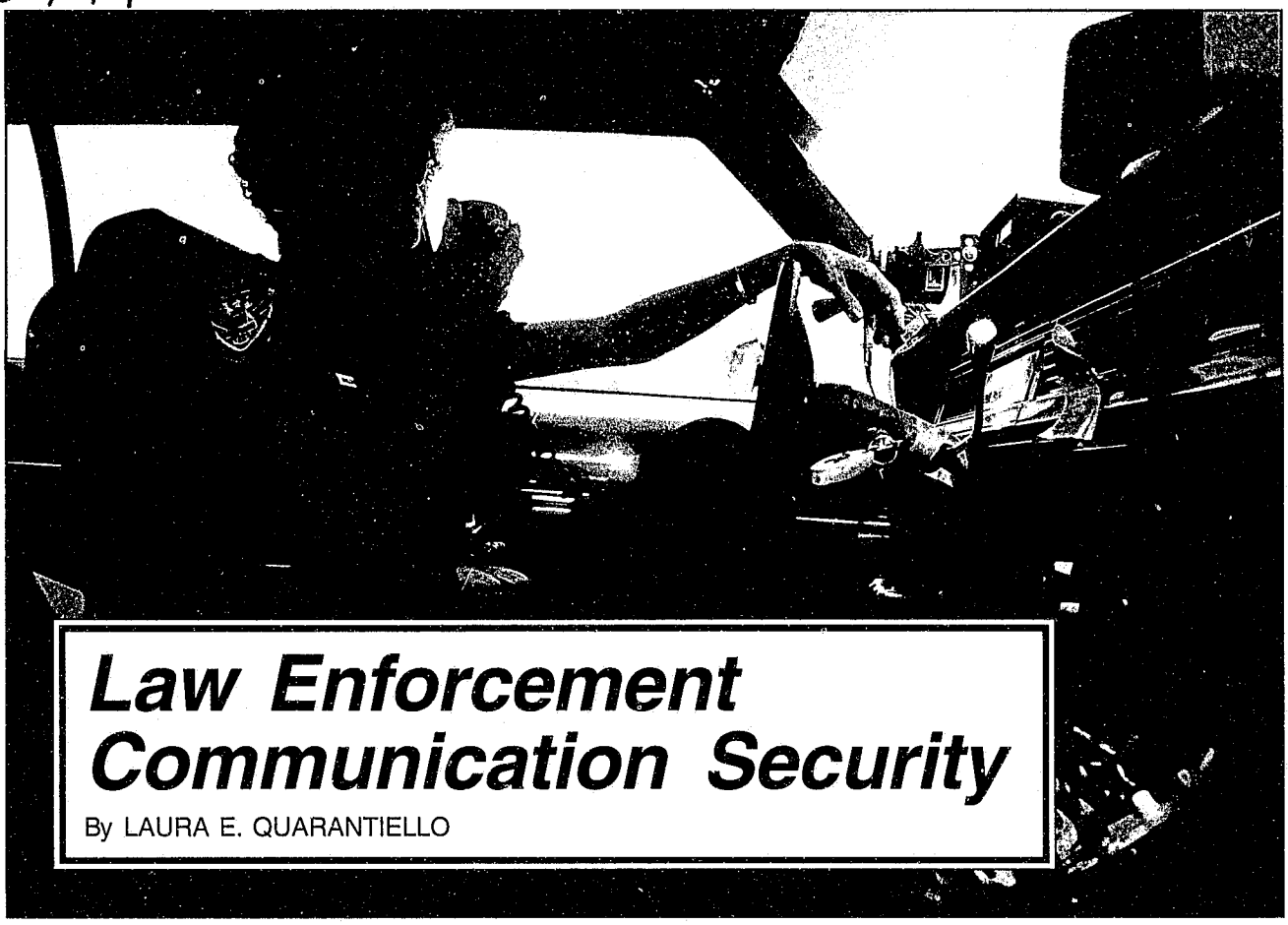
Features

156777
156778
156779
156780
156781

Departments

ISSN 0014-5688 USPS 383-310

156779



Law Enforcement Communication Security

By LAURA E. QUARANTIELLO

On every shift, law enforcement officers don equipment designed to protect them from harm during their tour of duty on the streets. Like a knight's armor, each piece of equipment forms a link of protection that, when complete, affords officers the best possible safety from the dangers they will face.

Under their uniforms they may wear tight-fitting protective vests; on their equipment belts, they carry service weapons and handcuffs. Trained to use these tools, officers hit the streets confident in the protective value of their gear. But the weakest link in the department-issued armor may turn out to be the most innocuous piece of equipment that officers use—the two-way radio.

THE LIFELINE

In the early days of urban policing, a blow on a whistle or the rap of a nightstick on a manhole cover was sufficient to summon assistance or transmit information. Officers basically worked alone, with very little need during their shifts to communicate with others in the department.

Today's police officers, however, work beats in a far different world. Their jobs and safety depend in large part on information exchange—a dispatcher giving details of a call for service or coordination among officers during a search for a suspect. This constant need for information can be fulfilled primarily through a voice link. Thus, the radio serves as an officer's lifeline.

Unfortunately, the radio wave that carries an officer's voice to a dispatcher's headset also radiates out into free air. Anyone with a scanner and a little time can tune in easily to the communications of local, State, and Federal law enforcement agencies. Every conversation can be overheard.

WHO IS LISTENING?

Officers using radios often fail to realize that not everyone who hears them is true blue. Though

officers intend police communication for internal, department use only, the radio frequencies used to broadcast them can be tuned in by anyone. A quick trip to the local electronics store will prove that the general public easily can acquire the equipment to intercept police transmissions.

Civilians who monitor police radio communication are, for the most part, hobbyists. They have an interest in the job itself and in keeping track of what happens in their city. The scanner simply provides entertainment. In fact, many hobbyists have become assets to police by calling in tips based on their knowledge of current police activities.

Hobbyists and their scanners do not concern law enforcement. What does concern the police is the increasing number of criminals who use scanners.

A scanner properly programmed with law enforcement frequencies can furnish criminals with a steady stream of information about police activities, including advance notice of everything from routine patrols to drug raids and warrant services. This legal eavesdropping compromises officer safety.

MYTHS AND ILLUSIONS

Officers who believe that their radio conversations cannot be intercepted by others outside of the department live with a delusion. Dependence on the radio link has bred complacency and generated several myths about radio security.

Officers often believe that with so many frequencies in use by their department, the chances must be small that a criminal will be listening to the right one at the right time. In fact, the chances are very good. With today's scanners capable of continuously searching hundreds of channels in seconds, even departments that use many different frequencies are not immune.

Officers believe that using codes and abbreviations prevents civilians from knowing what officers are talking about most of the time, right? Wrong. Commercial outlets routinely make police codes available. With a little listening and some common sense, most abbreviations can be deciphered. While number codes and abbreviations allow for clarity and brevity over the radio, they in no way ensure transmission security.

The biggest myth among police departments might be that 800 MHz (megahertz) radio systems make it impossible for police communication to be overheard. Manufacturers tout 800 MHz trunked systems as scanner-proof, and news agencies have reported that the advent of these systems destroys the ability of outsiders to listen. Nothing could be further from the truth. Trunked radio systems provide a bit of a challenge to monitor, but they also supply many pluses to listeners. With these systems, tactical and car-to-car communications, as well as the transmissions of detectives, now are broadcast over repeaters (devices that amplify and resend radio signals), which extend broadcast range. Even undercover details can be heard clearly.

Officers hold another common misbelief that most conversations over the radio are routine and disclose nothing that a criminal could use to put them in danger. It does not take a full-scale discussion to compromise officer safety. Just a few words, a seemingly minor detail, or a dropped name can be enough. An officer once innocently asked another, "207 David, 356 Adam. I am on the south side. Where are you?" "Second and Grand," responded the officer, continuing, "I am headed to Madison for a special detail."

"Dependence on the radio link has bred complacency and generated several myths about radio security."

Ms. Quarantiello, a writer in San Marcos, California, has published several articles on law enforcement radio communication.

Two things are wrong with this 5-second exchange. First, a criminal familiar with local police call signs would recognize that 207 David is the radio call of a detective unit. Second, the detective revealed his destination. The criminals listening in at the drug house on Madison would be packing by now, or loading their weapons.

PRECAUTIONS

Budget cuts and the high cost of equipping police officers often preclude the purchase and use of sophisticated scramblers and other forms of voice protection. In the end, the least expensive and most effective means of employing communication security lies in officers' watching their words. For this reason, officers should take the following precautions when transmitting over the radio.

Stick to the Necessities

The radio is not a telephone and should not be used for casual conversations. Officers should not convey personal or sensitive information over the radio.

Avoid Details That Can Be Communicated Later

Unless the information is urgent to current operations, it can wait. Officers should remember that everything they say can be heard, and they should always question whether they must communicate by radio immediately or if they can talk to the person later.

Use Typed Messages or Face-to-Face Meetings

Mobile Data Terminals (MDTs) provide some security by reducing conversations to typed messages relayed from computer to computer. Though MDT communication can be recorded and stored by the department, outsiders so far cannot decode the transmissions. If at all in doubt, officers should meet in person to exchange information.

> ***"...the least expensive and most effective means of employing communication security lies in officers' watching their words."***

Avoid Officer Names

Officers often approach conversations on tactical or car-to-car frequencies casually and use personal names instead of call signs. A wise criminal will learn to associate names with voices and then with call signs, which can endanger officers later when the criminal identifies special operations by the officers involved.

Avoid Unique Call Signs

Distinctive call signs alert criminals to the type of operations being conducted by the department. Departments should try to avoid special number or letter combinations that might tip off listeners to officers' whereabouts or activities.

Do Not Disclose Locations During Undercover Operations

Although officers might find it cumbersome to refer to "the location north of the main drag" or to use other verbal disguises, such tactics will help keep eavesdropping criminals off guard. All movements should be outlined in preliminary briefings and mapped out prior to the operation so as to reduce the need for radio exchanges.

Do Not Coordinate Special Operations Over the Air

The details of drug raids, warrant services, and other operations always should be coordinated during briefings. Once on the road to the location, radio chatter should be kept to an absolute minimum. All too often, listeners have heard sensitive details, such as the physical positioning of officers during tactical operations, that could place officers' lives in danger.

Use Low-Power Communications

If at all possible, officers should use simplex, low-power communications during undercover details and when transmitting from car to car. Sometimes called "talkaround," these channels do not use the system's repeater and, therefore, are harder to hear.

Use Out-of-Band Frequencies

Listeners know the police radio service bands and scan them diligently, so even communication on a supposedly unknown channel can be found if the channel falls within the range of police wavelengths. Departments should try low-power communications on bands away from the norm. Federal Communications Commission rules[1] allow police agencies to operate low-power radios on almost any public safety frequency, provided the transmissions cause no harmful interference.

Avoid Using Cellular Phones for Sensitive Conversations

Officers often attempt to avoid the radio by using cellular mobile telephones. These phones operate in the 869-894 MHz band, and their transmissions can be picked up by most moderately priced scanners. Recent legislation[2] makes the manufacture and importation of cellular-capable scanners illegal, but owning such a scanner remains legal.

Officers should make all phone calls from wire-connected telephones. If that is not possible, officers should avoid parking in one spot while using a cellular phone. Driving around takes advantage of frequent handoffs of the call from cell site to cell site, thereby causing listeners to lose the signal.

Do Not Rely on 800 MHz or Anti-scanner Tones for Protection

As mentioned previously, new 800 MHz trunked radio systems do not provide secure transmissions. In fact, they can be overheard easily. Some companies market their systems with anti-scanner tones intended to delay scanning radios and cause them to miss communications. However, users can defeat these tones by making internal modifications to the scanner.

CONCLUSION

The two-way radio has become so much a part of the daily routine that, unlike a weapon, officers largely ignore its potential for harm. Criminals, unfortunately, have realized the benefit of listening to police communications and often use the information gained to avoid discovery and arrest.

Officers' lives might be jeopardized when criminals intercept transmissions and learn of police movements and activities. Therefore, they always should guard what they say over unprotected radio frequencies, remembering that officer safety begins with a good coat of armor. ✦

Endnotes

[1] FCC Rules and Regulations 90.19(g)(3) allows law enforcement agencies to use any Part B public safety frequency between 40 and 952 MHz for surveillance and stakeouts, provided the power output does not exceed 2 watts. Prior approval is required for use of any Part B public safety non-police frequency, such as those designated for fire or highway maintenance.

[2] The Telephone Disclosure and Dispute Resolution Act of 1992 made it illegal (as of April 26, 1994) to manufacture in the United States, and/or export to the United States, scanning receivers or frequency converters that are designed or can be readily altered to receive cellular telephone frequencies.