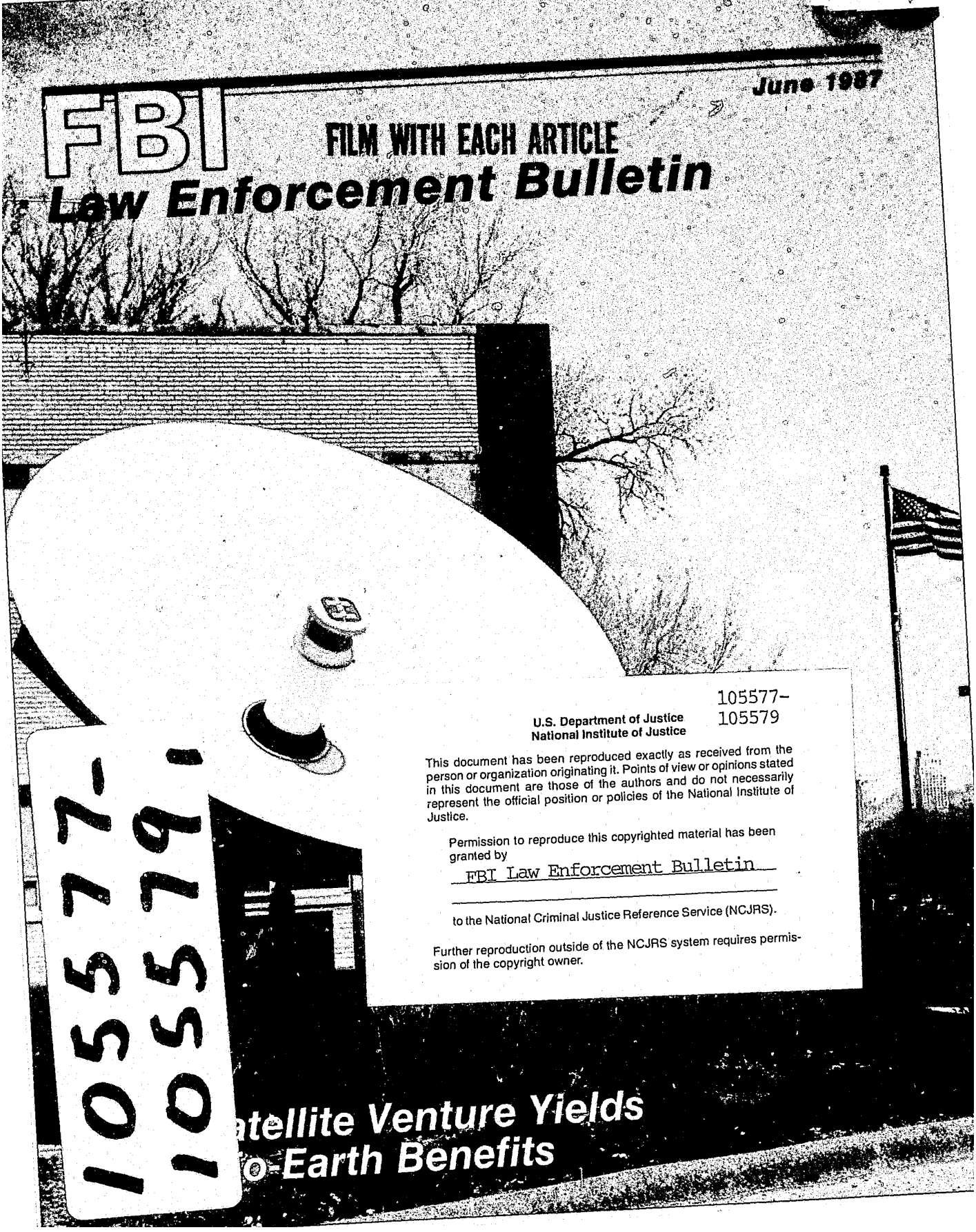
June 1987

FBI Law Enforcement Bulletin

FILM WITH EACH ARTICLE



atellite Venture Yields
o-Earth Benefits

Contents

June 1987, Volume 56, Number 6

FILM WITH EACH ARTICLE

105577

FBI
Law Enforcement Bulletin

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

John E. Otto, Acting Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Congressional and Public Affairs

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—Kevin J. Mulholland
Production Manager—Mark A. Zettler
Reprints—

The Cover:
The merger of satellite teleconferencing and educational resources represents a new era in law enforcement training. (See article p. 1.)

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.

ISSN 0014-5688

USPS 383-310

Minimization Requirements in Electronic Surveillance

(Conclusion)

"... to be lawful, minimization efforts must be reasonable as measured by the facts and circumstances of each case, as they exist at the time of interception."

By
ROBERT A. FIATAL, J.D.
Special Agent
FBI Academy
Legal Counsel Division
Federal Bureau of Investigation
Quantico, VA

Law enforcement officers of other than Federal jurisdiction who are interested in any legal issue discussed in this article should consult their legal adviser. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

Part one of this article traced the constitutional origins of "minimization" and defined this term as making reasonable efforts to avoid seizing nonpertinent conversations which have no evidentiary or investigative value in a court-authorized electronic surveillance. It then examined the Supreme Court's decision in *United States v. Scott,*[31] which prescribed the test reviewing courts are to apply when assessing minimization efforts by law enforcement personnel.

Part two will examine the factors in the *Scott* test, the interception of conversations involving unrelated criminal activity, and the consequences of a judicial finding of inadequate minimization. Finally, it will suggest procedures to best assure compliance with minimization requirements.

MINIMIZATION FACTORS

In *Scott,* the Supreme Court determined that to be lawful, minimization efforts must be reasonable as measured by the facts and circumstances of each case, as they exist at the time of interception. Before considering the factors used in this determination, it is important to remember that these circumstances may change during the course of the electronic eavesdropping order. A communication which may have been pertinent, and therefore, not subject to minimization efforts at the time of its interception may no longer be pertinent at the time a reviewing court determines if proper minimization procedures have been followed. Likewise, what was deemed an innocent conversation at the time of interception and was nonetheless listened to and recorded by monitoring officers may later become pertinent. In either instance, sufficient minimization efforts will be adjudged in accordance with the facts *as they existed at the moment of interception,* and not as they may have subsequently developed.

The Supreme Court in *Scott* and numerous lower Federal and State courts when applying the *Scott* rationale have identified a number of common factors in determining if minimization efforts were lawful. To assist the law enforcement officer tasked with monitoring a bug or wiretap in satisfying minimization requirements, each of these factors will be addressed in turn:

1) Nature and scope of the criminal activity being investigated;
2) Use of ambiguous, guarded, coded, or foreign language;
3) Location and use of the phone or facility;

Special Agent Fiatal

4) Expectation of contents of the intercepted conversation;
5) Extent of judicial supervision of the electronic surveillance;
6) Absence of interception of privileged communications; and
7) Good faith of the monitoring officers.

Nature and Scope of the Criminal Activity Being Investigated

As recognized by the Supreme Court in *Scott,* the nature or type, as well as the size, of the criminal activity being investigated by use of the electronic surveillance is an integral factor when assessing proper minimization. If the crime being investigated is an offense which is not ongoing or involves a limited number of participants, stringent minimization efforts are generally required by the courts.[32]

For example, if it is known that only one person or a small number of persons are involved in a single or small number of criminal episodes, interception should accordingly be limited. In such situations, once monitoring officers determine that persons being overheard are not those specifically named in the eavesdropping order, they must normally stop listening to and recording the conversations unless, of course, it is apparent that those intercepted are carrying on a conversation criminal in nature. If in such circumstances the named conspirators are known to rarely devote their conversations to purely innocent topics, interception of all conversations between those conspirators, except those that are obviously innocent, will generally be tolerated.[33]

If the investigation involves a widespread conspiracy which includes as yet additional unknown conspirators,[34] minimization efforts need not be as great as when the investigation involves a small conspiracy with a limited number of conspirators. As the Supreme Court stated in *Scott*:

> "[W]hen the investigation is focusing on what is thought to be a widespread conspiracy more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise. And it is possible that many more of the conversations will be permissibly interceptable because they will involve one or more of the co-conspirators."[35]

Similarly, courts have also adopted a more lenient attitude toward minimization if the investigation involves criminal activity which is complex in nature, such as a multiple series of illegal financial transactions.[36] In these instances, monitoring personnel may justifiably listen to conversations until they reasonably determine that those overheard are not involved in and not discussing matters relevant to the investigated conspiracy.

Officers may normally conduct more intrusive overhears with less emphasis on stringent minimization in investigations involving widespread or complex conspiracies when the purpose of the eavesdropping order is not only to obtain incriminating evidence but also to define the dimensions, or reach, of the conspiracy by identifying the conspirators and their whereabouts. This is frequently the purpose of wiretaps or bugs in investigations of conspiracies involving narcotics distribution,[37] as in *Scott.* In such investigations, electronic surveillance is used both to obtain incriminating evidence

"...courts have recognized the procedure of spot-monitoring to assure that the supposedly innocent communication does not later become pertinent."

and to identify the chain of dealers, suppliers, sources, and money launderers in the investigated narcotics distribution network. Seldom are such criminal operations narrow in breadth or scope.

Electronic eavesdropping in large-scale gambling investigations is also frequently instituted as much as to determine the identities and locations of the financiers of illegal bookmaking operations as to gain incriminating information.[38] When the purpose of the bug or wiretap is to at least partially determine the contours of a criminal conspiracy, monitoring officers will be justified in expanding their listening efforts, particularly at the beginning of the prescribed interception period. As the electronic surveillance progresses and the conspirators are identified, however, minimization efforts should be accordingly intensified. Officers should then be increasingly cautious when monitoring in order to avoid interception of conversations involving those not previously identified as conspirators, unless they are discussing criminal activities.

Use of Ambiguous, Guarded, Coded, or Foreign Language

More extensive interception will also be justified when those intercepted use guarded, coded, or ambiguous language in their conversations.[39] When conspirators are known to mask their communications with such terms and language, monitoring officers may intercept otherwise seemingly innocent conversations. Courts have recognized that criminals frequently intentionally mask their conversations through the use of codes, jargon, and colloquial terms. This is especially true of those criminals involved in the illicit distribution of narcotics where drugs, locations, prices, amounts, and participants are given predetermined nicknames and codes in order to thwart detection by electronic surveillance. For example, a Maryland court, in assessing the propriety of minimization efforts, recognized that the targeted conspirators frequently used the terms "candy" and "dresses" to allude to narcotics in their intercepted communications. That court stated that "[W]here coded conversations are utilized to obfuscate the true meaning of the dialogue, perfection in minimization is virtually impossible."[40] Similarly, the Supreme Court in *Scott* noted that intercepted calls which may be categorized as nonpertinent nonetheless may "apparently involve[] guarded or coded language,"[41] and therefore, would be reasonably intercepted.

Monitoring officers are confronted with a similar problem when those intercepted converse in a foreign language. If it is expected that the targets of the electronic surveillance will use a language other than English, appropriate efforts should be made to assign personnel capable of translating that expected language to monitoring responsibilities. In this way, minimization may be conducted at the moment of interception. There will undoubtedly be instances, however, when translators are not reasonably available to monitor the bug or wiretap, or when those intercepted unexpectedly converse in a foreign tongue. In such narrowly drawn situations, total interception of the foreign language communication is the commonly accepted procedure.[42] This presupposes, however, immediate and diligent efforts to locate and assign translator-officers to conduct further monitoring. When it is necessary and justifiable to record such foreign language conversations in their entirety, interpreters who subsequently conduct a first-time review of the recordings must then effectively minimize their listening efforts. The interpreters must make reasonable efforts to avoid listening to innocent conversations. They can evidence their efforts by making yet another recording of only those portions of the conversations they actually overhear.

It may also be reasonable to listen to and record conversations which are seemingly ambiguous in nature, and therefore, incapable of being catalogued as nonpertinent. This situation is compounded when the ambiguous communications are extremely short in duration and end before any determination of pertinency can be made. As the Supreme Court recognized in *Scott*, in such "circumstances agents can hardly be expected to know that the calls are not pertinent prior to their termination."[43]

Location and Use of the Phone or Facility

Another significant factor in measuring the propriety of minimization efforts is the location or use of the phone which is tapped or the place or facility which is bugged. As the Court recognized in *Scott,* if the phone or facility which is subject to electronic surveillance is located in the residence of a criminal co-conspirator and is used principally to discuss illegal activity or to further the aims of the criminal conspiracy, less extensive minimization will be expected.[44]

For example, in *United States* v. *Suquet,*[45] the telephone which was tapped was located in the residence of a person who was thought to be the head of a major drug ring. The Federal

"...periodic reports of the progress of the bug or wiretap, to include minimization efforts and results, should be made to the authorizing official."

district court determined that under such circumstances, "extensive monitoring may be both permissible and necessary."[46] The court also stated that "this is especially true at the outset of the investigation when the Government lacks the information it needs to identify the relevant cast of characters"[47] in the criminal conspiracy. In such situations, when the purpose of the surveillance is to determine the scope of the investigated conspiracy, nearly all conversations may be intercepted at the initiation of the surveillance, unless of course they are patently innocent.

On the other hand, if a public telephone is tapped or a place which is frequented by the general public is bugged, minimization will be crucial. Innocent individuals will likely use the phone or facility, thereby necessitating stringent minimization efforts.[48] Physical surveillance of such a public phone or place should be instituted, where feasible, and monitoring conducted only when an investigative target is seen at least in the area of the phone or facility.[49] When physical surveillance of such a targeted facility or phone is impossible, due to its physical location or countersurveillance efforts,[50] extreme care should be taken to recognize familiar voices, names, and telephone numbers when monitoring, in order to effectively minimize interceptions of innocent conversations.

In this regard, minimization is obviously more complex when monitoring a bug, where a microphonic device is placed in a targeted room or area where criminal conversations are to take place, than when monitoring a wiretap. There may conceivably be many individuals present at the same time in the bugged location, with several conversations concerning several different topics occurring at once. Compounding the difficulty of this likely situation is the recognition that these conversations may instantaneously shift from being seemingly innocuous in character to criminal in nature. It is totally unlike wiretap interceptions, where the calls most often can be assessed individually. In such instances, the purpose of the surveillance order, the expected use of the bugged area, the presence of conspirators in the bugged facilities, and their use of jargon or ambiguous language are of particular importance in determining what is proper minimization. When such factors are present, interception may be more intrusive when monitoring bugs than when monitoring wiretaps,[51] as there is generally greater difficulty in determining what conservations are nonpertinent.

Further minimization difficulties may arise in microphone surveillance when a bug with a normal range of interception is placed in a room where conversations criminal in nature are to take place, yet this unenhanced microphone is capable of picking up conversations from adjoining rooms. In such situations, monitoring officers should take reasonable efforts to limit their interceptions to criminally related conversations which originate from the room which is specifically mentioned in the authorizing court order.[52]

Frequently, the microphonic devices used transmit the intercepted conversations over publicly accessible radio frequencies to the monitoring officers. Even when the monitors refrain from listening to and recording nonpertinent conversations, the conversations themselves nonetheless continue to be broadcast, where they can conceivably be overheard by members of the general public. In such circumstances, the U.S. Court of Appeals for the Sixth Circuit has found the possibility of such intrusion by the public to be inconsequential in determining if proper minimization has been satisfied.[53] The court of appeals recognized that the chance of such unwarranted interceptions would be slight, as it would require the use of a compatible receiver in the same vicinity as the transmitter tuned to the same frequency. Even if this occurred, the interceptor would likely have no idea who was being intercepted.

Expectation of Contents of the Intercepted Conversation

The monitoring officer's reasonable expectation of the character of the conversation to be intercepted is also highly relevant in assessing proper minimization efforts. If two criminal conspirators are overheard, there obviously is a much greater likelihood that they will discuss matters criminal in nature than if friends or family of the conspirators are overheard, which would demand more intensive minimization. Even friends and family, however, may be known to be pawns of the conspirators and act as messengers of or fronts for the transmission of criminally pertinent information.

Such expectations are dependent upon the information available to the monitoring officer at the time of interception. This information normally becomes more abundant as the electronic surveillance progresses. As this information develops, categories of conversations which will not likely produce pertinent information also develop over the course of the bug or the wiretap. When a conversation is assessed to fit one of these predetermined categories of innocence, its interception should be avoided.

In order to develop these categories, greater leeway in minimization will normally be allowed at the beginning of the electronic surveillance period, especially when the purpose of the surveillance is not only to gather incriminating evidence but also to determine the breadth and scope of the investigated conspiracy. As the Supreme Court in *Scott* stated, "During the early stages of surveillance the agents may be forced to intercept all calls to establish categories of nonpertinent calls which will not be intercepted thereafter. Interception of those same types of calls might be unreasonable later on, however, once the nonpertinent categories have been established and it is clear that [the] particular conversation is of that type."[54] This does not suggest, however, that the interception of patently innocent conversations will be tolerated, no matter when they may occur.

Once categories of innocence are developed, as consistent patterns of innocent parties, times, and telephone numbers are established, interception of nonrelevant conversations will generally no longer be justified. Even after these categories have been developed, it is still necessary to intercept some portion of each call to determine if it falls into one of the nonpertinent categories and to assure that nontargeted individuals are not being used by conspirators to convey criminal information or to mask the conspirators' subsequent use of a targeted telephone. In this regard, courts generally allow monitoring officers to intercept up to the first few minutes of a call to determine the parties to and the subject of the conversation,[55] particularly if the speakers are known to use guarded language. If nonpertinency is determined in less time, of course, interception should be immediately terminated.

Presuming there is sufficient time to develop patterns of innocence,[56] there may be insufficient time to assess if the intercepted conversation fits any such category. It may be impossible to determine the relevancy of a short or ambiguous conversation. The Supreme Court in *Scott* acknowledged that "in these circumstances it may not be unreasonable to intercept almost every short conversation because the determination of relevancy cannot be made before the call is completed."[57]

Once the monitoring officer has determined the conversation to be nonpertinent and has ceased listening to and recording it, courts have recognized the procedure of spot-monitoring to assure that the supposedly innocent communication does not later become pertinent.[58] Spot-monitoring allows the monitoring officer, after ceasing to intercept a conversation, to periodically and routinely reinstitute interception for short periods of time. This is done to determine if the subject of the conversation or the identity of the speakers has changed. These periodic interceptions should, of course, be recorded and noted on interception logs. If the communication remains nonpertinent, interception should cease immediately. Such practice effectively balances the privacy interests of those being intercepted with the recognition that they may preface their criminal conversations with small talk in order to avoid electronic detection. The length and frequency of these spot-checks are best determined by the facts and circumstances of the investigation.[59]

Extent of Judicial Supervision of the Electronic Surveillance

In determining if proper minimization efforts have been effectuated, reviewing courts will pay great deference to the contemporaneous oversight of minimization efforts by the judicial officer who authorizes the electronic surveillance. It is, therefore, advantageous to submit both planned minimization procedure and proposed written instructions concerning this procedure to the authorizing judge for review and approval prior to interception.[60]

Additionally, periodic reports of the progress of the bug or wiretap, to include minimization efforts and results, should be made to the authorizing official.[61] Title III provides that "the court may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception."[62] Such reports not only allow the court to determine the need for continued interceptions but also to determine if proper minimization efforts are being taken.

To produce reports that accurately reflect minimization efforts, monitoring officers should compile detailed logs of their interception activity, to include summaries of the intercepted conversations. These logs also provide a convenient record of minimization efforts for later evaluation by reviewing courts.

Supervising officers and prosecuting attorneys should also periodically visit the monitoring facilities, as well as listen to recordings of intercepted conversations, in order to assure that proper minimization is being performed. Based upon the logs and their observations, these supervisors can then include in their progress reports to the authorizing judicial official not only the contents of incriminating communications but also the number of irrelevant

"...the nature or type, as well as the size, of the criminal activity being investigated by use of the electronic surveillance is an integral factor when assessing proper minimization."

conversations overheard, the reason for their seizure, minimization practices, and what, if any, steps have been taken to improve these minimization procedures.

Finally, the authorizing judge might consider visiting the monitoring facilities, unless security considerations dictate otherwise. There, the issuing authority can view firsthand monitoring practices to ascertain if proper minimization standards are being met.[63]

Absence of Interception of Privileged Communications

Certain confidential communications are considered at law to be privileged in nature to foster relationships considered essential to the functioning of an ordered society. These include confidential conversations between husband and wife, doctor and patient, priest and penitent, and attorney and client. Title III provides that "No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."[64]

Accordingly, authorizing judges will frequently include in electronic eavesdropping orders provisions prohibiting the interception of privileged communications. Even in the absence of such a provision in the authorized order, efforts to avoid interception of privileged communications are frequently considered a factor in assessing if proper minimization efforts have been made.[65] Therefore, care should be taken to neither listen to nor record conversations determined to fall into one of the aforementioned categories of privileged communications.

The identities and phone numbers of targeted conspirators' spouses, attorneys, and doctors should be ascertained and disseminated to monitoring officers, so the monitors may anticipate privileged communications and minimize accordingly. Additionally, when the phone or office of a privileged professional, such as an attorney, is tapped or bugged, monitoring officers should exercise significant care in minimization efforts, honoring privileged communications and intercepting only pertinent conversations.

If, however, the conversations between two parties in a potentially privileged relationship involve crimes they have committed in concert, are presently committing, or are planning to commit, they are no longer privileged.[66] Such conversations should therefore be intercepted. This situation will be particularly applicable where an attorney, doctor, clergyman, or spouse is a targeted conspirator in the criminal activity being investigated. For example, in *United States* v. *Harrelson*,[67] monitoring agents intercepted communications between Jamiel Chagra and his wife, Elizabeth Chagra, and his brother, Joseph Chagra, who was an attorney, concerning the murder of U.S. District Court Judge John Wood. The U.S. Court of Appeals for the Fifth Circuit found that those conversations were not privileged, as they were made to further the criminal conspiracy being investigated, and were therefore properly intercepted.

In *United States* v. *Hyde*,[68] the U.S. Court of Appeals for the Fifth Circuit also recognized the propriety of initially monitoring an ostensibly privileged conversation a short period of time to ascertain that the participants were not involved in the investigated criminal conspiracy. The court of appeals stated, "It would be unreasonable to expect agents to ignore completely any call to an attorney or doctor; doctors and lawyers have been known to commit crimes."[69] Such practice would only be acceptable, however, in the early stages of the execution of an eavesdropping order, before the conspirators are identified.

Spot-monitoring can be used to assure privileged communications do not lose their privileged character and to safeguard against instances where surveillance-conscious conspirators assume the identities of doctors, lawyers, or priests to mask criminal conversations, or use a spouse as an unwitting answering service.

If the target of electronic surveillance efforts is the subject of pending criminal charges, extreme care should be exercised to avoid interception of that subject's conversations with his attorney concerning the pending charges. Such communications are protected not only by their privileged nature but also by the subject's right to counsel as guaranteed by the sixth amendment to the U.S. Constitution.[70] Interception of legal advice, to include discussion of defense plans and strategies, concerning pending charges should be strictly avoided, as it may deprive the subject of his constitutional right to effective assistance of counsel and result in dismissal of those charges.[71]

Good Faith of the Monitoring Officers

Interestingly, the Supreme Court in *Scott* specifically stated that the failure of monitoring officers to exercise good faith, or to be honest and sincere, in their minimization efforts is inconsequential, as long as the minimization requirement has been objectively satisfied. The focus of the minimization inquiry is "on the agents' actions not their motives" in conducting the electronic surveillance.[72]

Regardless, monitoring officers should perform their tasks with a good faith belief in their validity. A good faith effort to minimize properly assures respect for the minimization process and compliance with minimization criteria. It also adds credibility to the officers' claims of what information was known to them at the time of the interception.

Despite its pronouncement in *Scott,* the Supreme Court acknowledged that if minimization is found to be unsatisfactory, the monitoring officers' good faith, or subjective intent, may be relevant in determining the propriety of the application of the exclusionary rule.[73] Additionally, at least one Federal district court and several State supreme courts have determined the subjective intent of the monitoring officers to play a small, if not dispositive, role in minimization inquiries.[74]

All of the above discussed factors will be considered by reviewing courts in assessing if reasonable efforts have been made to minimize the interception of communications irrelevant to the investigation. The more factors present, the more likely minimization will be determined proper. There may be instances, however, when conversations which are totally unrelated to the matter under investigation may be purposely and lawfully overheard when they concern extraneous criminal activity.

INTERCEPTION OF COMMUNICATIONS INVOLVING UNRELATED CRIMINAL ACTIVITY

Monitors who have been instructed to minimize their interception of conversations which are not pertinent to the criminal activity being investigated sometimes unexpectedly overhear information concerning other unrelated crimes which are not specifically identified in the electronic eavesdropping order. As long as the monitoring officers were justifiably intercepting the conversations at the time they encountered the unrelated criminal information, they are justified in continuing their interception. An analogy can be drawn to the "plain view" seizure of physical evidence, as 1) the monitors were validly listening at the time they overheard the unrelated information, 2) they immediately recognized the overheard conversation as evidence of criminal activity, and 3) their discovery was inadvertent.[75] For example, if officers, while monitoring a wiretap or bug for the purpose of obtaining information concerning a narcotics distribution network, happen to overhear information concerning illegal gambling activity or stolen property interspersed with drug-related information, they may justifiably intercept it.[76]

One U.S. court of appeals has addressed a similar situation where the person who was using the phone which was tapped engaged in criminal conversations with others who were nearby while he dialed the phone or waited on hold. The Fourth Circuit Court of Appeals found the interception of such background conversations to be permissible, being in "plain view" while the agents were justifiably monitoring.[77]

CONSEQUENCES OF IMPROPER MINIMIZATION

As minimization efforts in *Scott* were determined to be reasonable, the Supreme Court was not presented with the opportunity to decide the appropriate remedy for improper minimization.[78] The Court only commented that in such a situation, the good faith of the monitoring officers may be relevant in determining the propriety of the application of the exclusionary rule.[79]

Lower Federal and State courts which have had the need to determine the consequences for excessive monitoring are divided as to the appropriate remedy. Some courts have required complete and total suppression of all intercepted conversations whenever minimization standards are violated.[80] Most courts, however, have suppressed only those communications which have been inappropriately intercepted.[81] Those which are properly overheard and seized are admitted. This presumes that those conversations were lawfully listened to and recorded at the time of their interception and should not have otherwise been minimized. If the conversation was one which fits a developed pattern of innocence or nonpertinence and was nonetheless monitored, it was unlawfully intercepted and should be suppressed, even if it proves to be relevant. As one Federal district court stated:

> "If the government continues to intercept, for example, a person not named in the authorizing order after his or her identity has been established and a pattern of innocent conversation takes place, it would be of no moment that eventually that individual was heard discussing incriminating matter; the conversation would still be subject to suppression because it would have been 'unlawful' for the monitors to be overhearing the conversation in the first instance."[82]

Many courts have questioned the sufficiency of these remedies in deterring law enforcement officers from listening to and recording nonpertinent conversations, which may lead to nominal efforts to effectuate proper minimization. Therefore, if minimization efforts are totally disregarded, evidencing bad faith on the part of the monitoring officers, total suppression of all intercepted conversations will routinely be

"...monitoring officers should compile detailed logs of their interception activity, to include summaries of the intercepted conversations."

warranted.[83] When minimization procedures are blatantly ignored, the electronic surveillance turns into a general search with constitutional implications.

RECOMMENDATIONS FOR PROPER MINIMIZATION

As improper minimization can lead to adverse consequences, namely, the exclusion of incriminating conversations in a subsequent criminal proceeding, proper minimization efforts are crucial. The importance of judicially acceptable minimization is particularly emphasized when one considers the amount of time, money, and man hours normally expended to successfully use the extraordinary investigative technique of electronic surveillance. Several suggestions are, therefore, offered to assure the monitoring officer minimizes his interception of conversations in a reasonable manner considering the circumstances that exist at the time of interception.

Know Court-mandated Limitations and Purpose and Scope of Electronic Surveillance

First, all monitors should read both the application for the electronic surveillance and the order authorizing the bug or wiretap. In this way, one becomes familiar with court-mandated limitations on eavesdropping, to include limitations on the *hours one may monitor, who one may intercept,* and the *types of conversations one may overhear.*[84] Similarly, the monitoring officer is able to ascertain the *purpose of the surveillance,* which is particularly important when the wiretap or bug is used not only to gain incriminating evidence but also to define the breadth of and participants in a criminal conspiracy. If monitors are unaware of the scope of the electronic surveillance and the court-ordered limitations upon their interception efforts, they would necessarily rely exclusively upon their own discretion when minimizing. This would likely lead to a general search which would violate both statutory and constitutional standards.

Copies of these documents should be provided to all monitoring officers prior to the initiation of interceptions. Additional copies should also be kept at the listening post, where the monitoring activity takes place. They will provide the basis for extrinsic minimization by identifying mandated hours of monitoring, if any, and also the initial facts and circumstances which provide the framework for intrinsic minimization. In establishing this framework, monitoring personnel should review the application and order for pertinent data on the factors identified in the *Scott* case—nature and scope of the criminal activity, any code or foreign language issues, the location and use of the phone or facility, any known expectations of contents, and any known privileged communications. These factors should also be addressed in the written instructions described below.

Provide Written Instructions and Guidance from the Prosecutor to Monitoring Personnel

Second, written instructions on minimization should be prepared[85] in advance of the surveillance and provided to the authorizing judicial official for his review and approval. These instructions should then be distributed to all monitoring officers, in conjunction with a presentation on minimization concerns by the prosecuting attorney charged with supervising the wiretap or bug. Again, copies of these instructions should be maintained at the listening site.

These instructions should emphasize that monitors should only listen when they are recording properly intercepted conversations, as any other procedure may evidence improper minimization efforts.[86] Precise instructions on what to intercept and not intercept are obviously difficult to formulate, but as much information as possible should be included in the instructions to assist the monitor in anticipating the contents of conversations. They should identify and describe *anticipated speakers, places, persons, locations, and phone numbers* associated with the matter under investigation. They should also state the *authorized purpose of the wiretap or bug,* as it may not only be to obtain incriminating statements but also to ascertain the identities and locations of the conspirators, the whereabouts and sources of contraband and evidence, and the locations of other premises and telephones used to discuss and conduct criminal activities. If the purpose encompasses these varying concerns, all or nearly all calls or conversations made at the beginning of the eavesdropping period may be intercepted, until innocent persons and patterns are ascertained.

Update Instructions as New Information is Developed

Third, as *additional conspirators* and *their locations,* as well as any *other information* relevant to the investigation, are determined throughout the course of the bug or wiretap, instructions should be updated accordingly. Similarly, as *innocent patterns of communications* emerge, *nonpertinent times, people,* and *telephone numbers* should be disseminated to monitoring officers so they might better be able to anticipate and determine what conversations should not be overheard.

Identify and Post Possible Participants to Privileged Communications

Fourth, monitors should also be cautioned to avoid interception of privileged communications. The identities of a targeted subject's *spouse, attorney, priest,* or *doctor* should be posted at the listening site as they are determined, in order to facilitate the anticipation of conversations which may be privileged in nature. This presumes, of course, that such parties are not involved in the investigated criminal conspiracy, in which case the conversations will unlikely be privileged.

Spot-monitor Privileged and/or Nonpertinent Conversations

Fifth, officers should also be cognizant of the accepted practice of spot-monitoring privileged and/or nonpertinent conversations to overcome any tactics criminals might use to frustrate electronic surveillance, such as prefacing their calls or conversations with small talk or assuming the identities of privileged professionals.

Maintain Detailed Logs of Interceptions

Sixth, monitors should also maintain detailed logs of their interception endeavors, to include the *times* calls and conversations were listened to and recorded, *who if anybody was identified,* and a *summary of the content* of the intercepted communication, unless it was ambiguous in nature. Such logs are of particular assistance to supervising officers and attorneys when drafting periodic progress reports of the electronic surveillance, as they provide a convenient record of minimization efforts. They also may assist the monitoring officer in explaining why he intercepted a particular conversation in any judicial determination of minimization compliance at subsequent suppression hearings.

Continuing Supervisory Review and Control

Finally, *supervising officers and prosecutors* should routinely and periodically assure the electronic surveillance order is being properly executed. They *should not only review logs of interception activity but also tapes of intercepted communications.* If a problem is noted, they should advise monitoring officers of unsatisfactory interception, whether it be a matter of too little or too much minimization.

CONCLUSION

Monitoring officers should realize that effective minimization requires the officer to balance the government's legitimate interest in detecting, investigating, and prosecuting criminal activity with constitutional safeguards. Minimization does not require the termination of interception of all portions of all nonrelevant conversations, as that would be humanly impossible. Minimization requires a reasonable effort on the part of the monitoring officer to minimize the interception of innocent calls and conversations as much as is possible under the then existing circumstances. By understanding this concept and following the suggested recommendations for proper minimization, monitoring officers should maximize the objective reasonableness of their efforts. FBI

Footnotes

[31]436 U.S. 128 (1978).

[32]*See, e.g., State* v. *Tucker,* 662 P.2d 345 (Or. Ct. App. 1983) (stringent minimization required where only two conspirators were known to be involved in a narrowly focused investigation).

[33]*See United States* v. *Suquet,* 547 F.Supp. 1034 (N.D. Ill. 1982).

[34]The Supreme Court has determined that it is necessary to specifically name in the eavesdropping application only those for whom there exists probable cause to believe they are committing the investigated offenses. When the purpose of the interception is to also identify those individuals not yet known, they may be referred to appropriately as "others yet unknown" in the application. *United States* v. *Kahn,* 415 U.S. 143 (1974).

[35]*Supra* note 27, at 140.

[36]*See, e.g. United States* v. *DePalma,* 461 F.Supp. 800 (S.D.N.Y. 1978).

[37]*See, e.g., United States* v. *Van Horn,* 789 F.2d 1492 (11th Cir. 1986); *United States* v. *Hyde,* 574 F.2d 856 (5th Cir. 1978); *United States* v. *Lilla, supra* note 27; *United States* v. *Suquet, supra* note 33; *Commonwealth* v. *Doty, supra* note 24; *State* v. *Andrews,* 480 A.2d 889 (N.H. Sup. Ct. 1984); *State* v. *Whitmore,* 340 N.W.2d 134 (Neb. Sup. Ct. 1983); *Salzman* v. *State,* 430 A.2d 847 (Md. Ct. Spec. App. 1981); *Poore* v. *State,* 384 A.2d 103 (Md. Ct. Spec. App. 1978).

[38]*See, e.g., United States* v. *Clerkley,* 556 F.2d 709 (4th Cir. 1977); *State* v. *Catania, supra* note 25.

[39]*See, e.g., United States* v. *Turner, supra* note 22; *United States* v. *Suquet, supra* note 33; *United States* v. *DePalma, supra* note 35; *State* v. *Andrews, supra* note 37; *Salzman* v. *State, supra* note 37.

[40]*Poore* v. *State, supra* note 37, at 117.

[41]*Supra* note 27, at 140.

[42]*See United States* v. *Cale,* 508 F.Supp. 1038 (S.D.N.Y. 1981) (title III order allowed total interception of foreign language until translator became available); *Gonzalez* v. *State,* 333 S.E.2d 132 (Ga. Ct. App. 1985) (objectively reasonable to record interceptions in their entirety when Spanish-speaking officer not present); *State* v. *Olea,* 678 P.2d 465 (Ariz. Ct. App. 1983) (recording of one call in entirety due to the then unavailability of Spanish-speaking officer acceptable). The Electronic Communications Privacy Act of 1986, which amends title III, also allows for delayed minimization of intercepted communications conducted in a code or foreign language, if an expert in that foreign language or code is not reasonably available during the interception period. 18 U.S.C. 2518(5).

[43]*Supra* note 27, at 140.

[44]*Supra* note 27, at 140. *See also, United States* v. *Rodriguez,* 606 F.Supp. 1363 (D. Mass. 1985); *Commonwealth* v. *Doty, supra* note 24; *Sulzman* v. *State, supra* note 37.

[45]*Supra* note 33.

[46]*Id.* at 1037.

[47]*Id.* at 1037.

[48]*See United States* v. *Scott, supra* note 27, at 140. *See also, United States* v. *Dorfman,* 542 F.Supp. 345 (N.D. Ill. 1982) (wiretap on phone of legitimate business with over 100 employees).

[49]*See, e.g., State* v. *Whitmore, supra* note 37 (public phone monitored only when physical surveillance indicated it was being used by a conspirator).

[50]*See, e.g., United States* v. *Van Horn, supra* note 37 (business which was subject of eavesdropping was surrounded by open area and noncooperative businesses, and conspirators were extremely surveillance conscious).

[51]*See, e.g., United States* v. *Clerkley, supra* note 38 (bug in gambling investigation used to determine extent of conspiracy where coded language commonly used).

[52]*See United States* v. *Terry,* 702 F.2d 299 (2d Cir. 1983) (monitoring DEA agents took reasonable efforts to limit interception to narcotics-related conversations originating in living room where bug was placed).

[53]*United States* v. *Feldman,* 606 F.2d 673 (6th Cir. 1979).

[54]*Supra* note 27, at 141. *See also, United States* v. *Hyde, supra* note 37; *United States* v. *Dorfman, supra* note 48; *State* v. *Catania, supra* note 25.

[55]See, e.g., *United States* v. *Lilla*, *supra* note 27. *See also, United States* v. *DePalma*, *supra* note 36 (approval of 3-minute initial interception); *Commonwealth* v. *Doty*, *supra* note 24 (approval of 3-minute initial interception).

[56]*See State* v. *Andrews*, *supra* note 37.

[57]*Supra* note 27, at 141.

[58]See, e.g., *United States* v. *DePalma*, *supra* note 36; *State* v. *Monsrud*, 337 N.W.2d 652 (Sup. Ct. Minn. 1983); *State* v. *Catania*, *supra* note 25; *Poore* v. *State*, *supra* note 37.

[59]See, e.g., *Commonwealth* v. *Doty*, *supra* note 24 (ceasing interception for 2 minutes and then spot-checking for 1 minute valid in investigation of widespread narcotics conspiracy); *United States* v. *DePalma*, *supra* note 36 (waited 3 minutes, spot-checked for 1 minute); *Sulzman* v. *State*, *supra* note 37 (spot-monitoring in 30-second alternating intervals).

[60]See, e.g., *Commonwealth* v. *Doty*, *supra* note 24.

[61]See, e.g., *United States* v. *Hyde*, *supra* note 37 (two reports in 30 days); *United States* v. *Clerkley*, *supra* note 38 (reports every 5 days); *United States* v. *Rodriguez*, *supra* note 44 (reports every 5 days); *United States* v. *Cortese*, 568 F.Supp. 119 (M.D. Pa. 1983) (reports every 5 days); *United States* v. *Suquet*, *supra* note 33 (reports every 5 days); *State* v. *Olea*, *supra* note 42 (reports every other day); *People* v. *Gable*, 647 P.2d 246 (Colo. Ct. App. 1982) (weekly reports); *Sulzman* v. *State*, *supra* note 37 (reports every 4 days); *Poore* v. *State*, *supra* note 37 (weekly reports).

[62]18 U.S.C. 2518(6).

[63]*See Commonwealth* v. *Leta*, 500 A.2d 85 (Pa. Super. Ct. 1985); *State* v. *Olea*, *supra* note 42.

[64]18 U.S.C. 2517(4).

[65]*See United States* v. *Hyde*, *supra* note 37; *United States* v. *Lilla*, *supra* note 26; *United States* v. *DePalma*, *supra* note 36; *Poore* v. *State*, *supra* note 37.

[66]*See United States* v. *Kahn*, *supra* note 34 (conversations between husband and wife in furtherance of crime are not privileged); *United States* v. *Dyer*, 722 F.2d 174 (5th Cir. 1983) (attorney-client privilege does not exist where communication was intended to further continuing or future criminal activity); *United States* v. *Shakur*, 560 F.Supp. 318 (S.D.N.Y. 1983) (communications by attorney to client which are designed to assist the client in the commission of a crime are not privileged).

[67]754 F.2d 1153 (5th Cir. 1985).

[68]574 F.2d 856 (5th Cir. 1978).

[69]*Id.* at 870.

[70]U.S. Const. amend. VI provides:

"In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense."

[71]*See Weatherford* v. *Bursey*, 429 U.S. 545 (1977) (sixth amendment right to counsel violated when prosecution learns of defense plans or strategy or obtains incriminating evidence as result of interference with attorney-client relationship).

[72]*Supra* note 27, at 139.

[73]*Id.* at 139, note 13.

[74]See *United States* v. *Suquet*, *supra* note 33 (minimization determination cannot be based entirely on absence of good faith, as such a foctor only plays a small role in such an inquiry); *State* v. *Thompson*, *supra* note 6 (unnecessary to determine if absence of good faith is relevant as minimization was totally unacceptable); *State* v. *Monsrud*, *supra* note 58 (absence of good faith may require suppression of all interceptions if minimization violated); *State* v. *Catania*, *supra* note 25 (subjective good faith absolutely necessary for proper minimization); *People* v. *Floyd*, *supra* note 21 (minimization imposes duty on officers to make good faith effort to reduce interception of nonpertinent conversations to smallest possible number). Commentators have also stressed the importance of good faith efforts to comply with minimization, suggesting that the absence of good faith may lead to a total disregard of minimization, likely resulting in an amendment to title III requiring good faith. Fishman, Clifford S., *Wiretapping and Eavesdropping*, at 231 (1978).

[75]*See Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971) (plain view seizure of evidence justified where 1) seizing officers are validly present at the time they see the plain view evidence, 2) the evidence is immediately recognizable as evidence of criminal activity, and 3) the discovery is inadvertent).

[76]*See State* v. *Whitmore*, *supra* note 37 (interception of gambling calls in narcotics wiretap permissible as gambling calls were either short in duration or also frequently contained drug-related information).

[77]*United States* v. *Couser*, 732 F.2d 1207 (4th Cir. 1984).

[78]It is not the purpose of this article to discuss the standing an individual must possess to contest minimization procedures. *See United States* v. *Dorfman*, *supra* note 48; *United States* v. *Suquet*, *supra* note 33.

[79]*Supra* note 27, at 139 note 13.

[80]*See United States* v. *Focarile*, 340 F.Supp. 1033 (D. Md. 1972); *State* v. *Catania*, *supra* note 25 (pursuant to N.J. statute total suppression required when minimization violated).

[81]*See United States* v. *Cox*, 462 F.2d 1293 (8th Cir. 1972); *United States* v. *Sisca*, 361 F.Supp. 735 (S.D.N.Y. 1973); *State* v. *Monsrud*, *supra* note 58.

[82]*United States* v. *Dorfman*, *supra* note 48, at 395.

[83]*See United States* v. *Santora*, 600 F.2d 1317 (9th Cir. 1979); *United States* v. *Suquet*, *supra* note 33; *United States* v. *Webster*, 473 F.Supp. 586 (D. Md. 1979); *State* v. *Thompson*, *supra* note 6; *People* v. *Brenes*, 364 N.E.2d 1322 (N.Y. Ct. App. 1977); *State* v. *Tucker*, *supra* note 32. One of the leading commentators in the area of electronic surveillance has also expressed concern that a partial suppression rule is an ineffective deterrent to improper minimization efforts, and that if the eavesdropping becomes in effect a general search, total suppression is warranted, despite the monitoring officers' intentions. Carr, James G., *The Law of Electronic Surveillance*, at 267 (1978).

[84]*See, e.g., United States* v. *Rodriguez*, *supra* note 44; *United States* v. *Suquet*, *supra* note 33.

[85]For an excellent example of monitoring instructions, see Fishman, Clifford S., *Wiretapping and Eavesdropping*, at 232–240 (1978).

[86]*See, e.g., State* v. *Monsrud*, *supra* note 58 (improper minimization where monitors listened to all and only recorded pertinent conversations).

Law Enforcement Officers Killed 1986

The number of law enforcement officers killed in the line of duty decreased in 1986 from the previous year's total. Preliminary 1986 national figures show that 66 officers were slain feloniously, as compared to the 78 who lost their lives in 1985.

Thirty-four of the victims were city police, 23 were county officers, 5 were employed by State law enforcement agencies, and 4 were Federal officers. Of the 66 killings, 59 have been cleared by law enforcement agencies.

Last year, firearms were the weapons used in 62 of the slayings—handguns (51), rifles (8), and shotguns (3). The remaining 4 victims were intentionally struck by vehicles.

When slain, 26 officers were attempting to apprehend or arrest suspects. Ten of the 26 were attempting to thwart robberies or were in pursuit of robbery suspects, 7 were involved in drug-related situations, 1 was responding to a burglary, and 8 were attempting arrests for other crimes.

Ten victims were killed while enforcing traffic laws, 10 while investigating suspicious persons or circumstances, 6 upon answering disturbance calls, and 6 were ambushed. Five officers were murdered while handling or transporting prisoners, and three while dealing with mentally deranged individuals.

Geographically, 31 officers were killed in the Southern States, 13 in the Western States, 11 in the Midwestern States, 7 in the Northeastern States, and 4 in Puerto Rico.