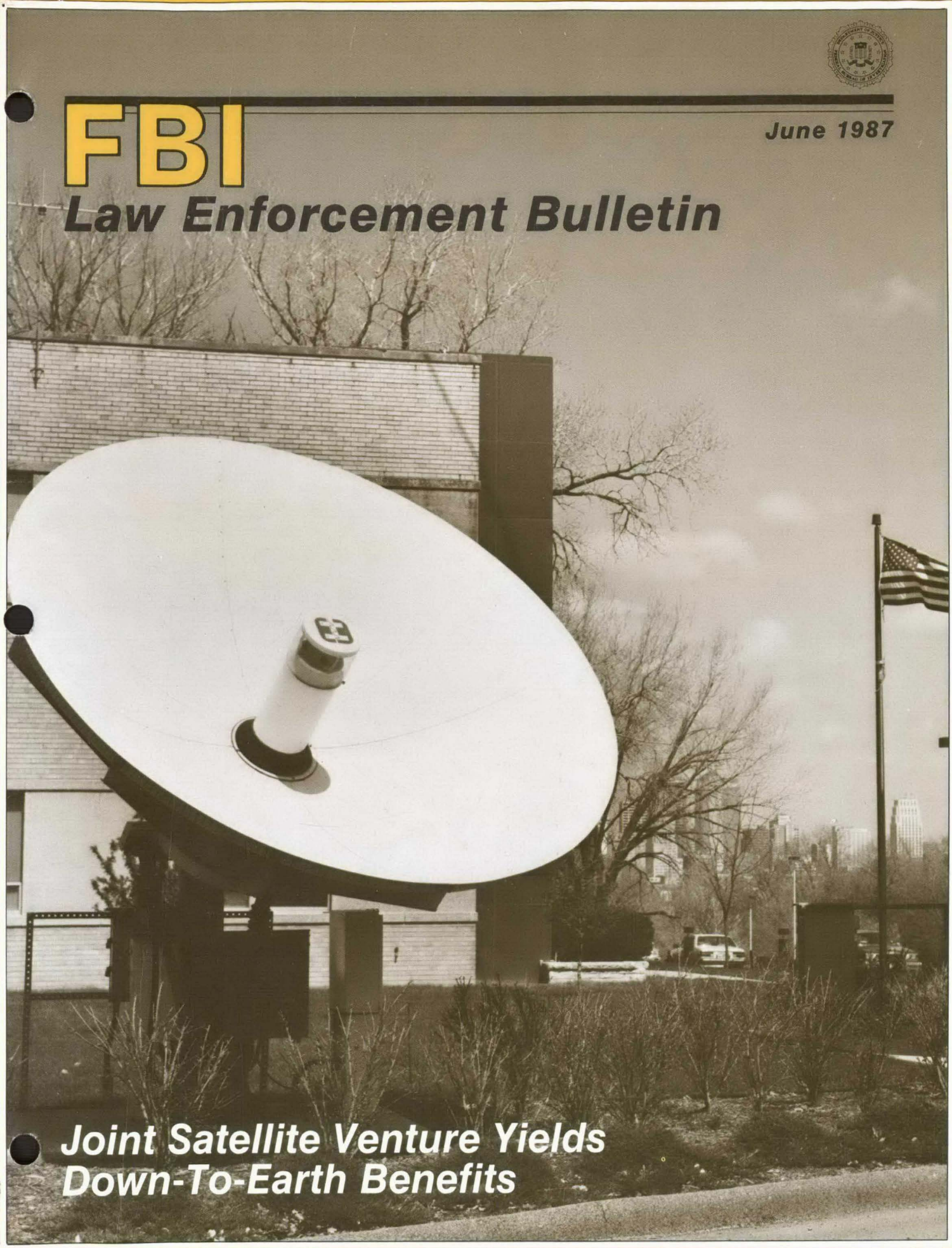
FBI
Law Enforcement Bulletin

June 1987



Joint Satellite Venture Yields Down-To-Earth Benefits

Contents

June 1987, Volume 56, Number 6

Training **1** **Joint Satellite Venture Yields Down-To-Earth Benefits**
Michael P. Kortan and Tony E. Triplett

Technology **6** **Polygraph Policy Model For Law Enforcement**
By Ronald M. Furgerson

20 **Book Review**

Legal Digest **21** **Minimization Requirements in Electronic Surveillance (Conclusion)**
By Robert A. Fiatal

31 **VICAP Alert**

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.)

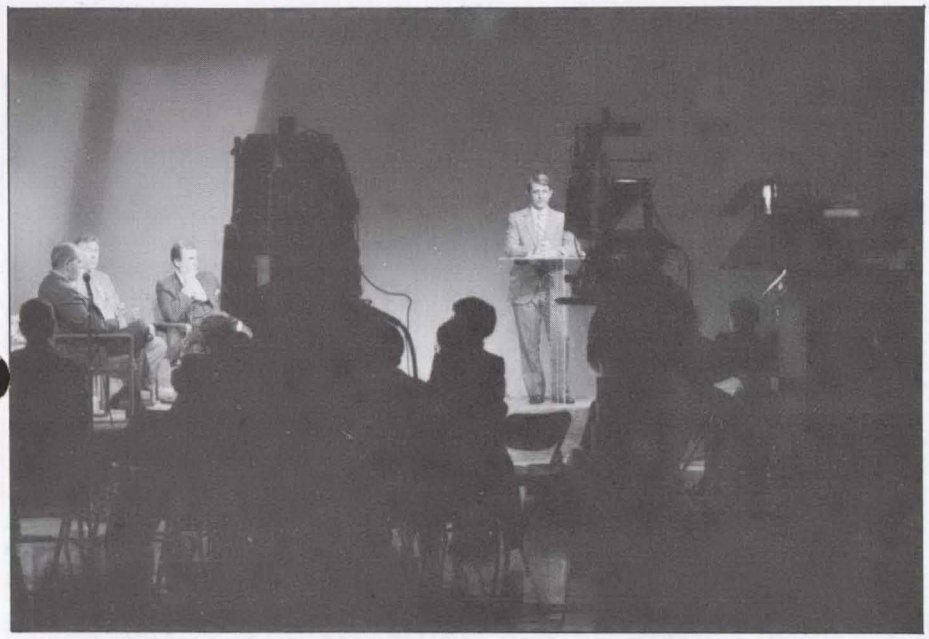
The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement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

ISSN 0014-5688

USPS 383-310

Joint Satellite Venture Yields Down-To-Earth Benefits

By
MICHAEL P. KORTAN
Special Agent
and
TONY E. TRIPLETT
Special Agent
Police Training Coordinator
Federal Bureau of Investigation
Kansas City, MO

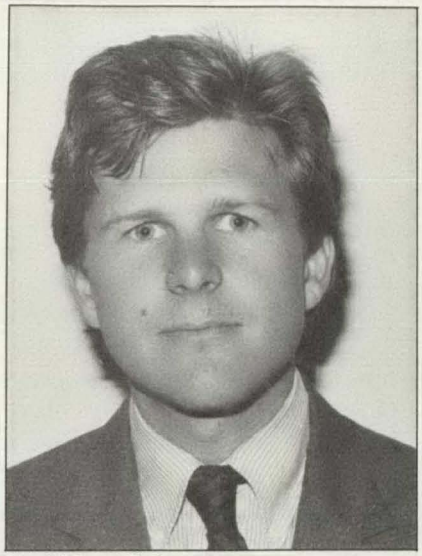


"Satellite teleconferencing has proved to be a cost-effective tool for providing valuable training information to a large law enforcement audience."

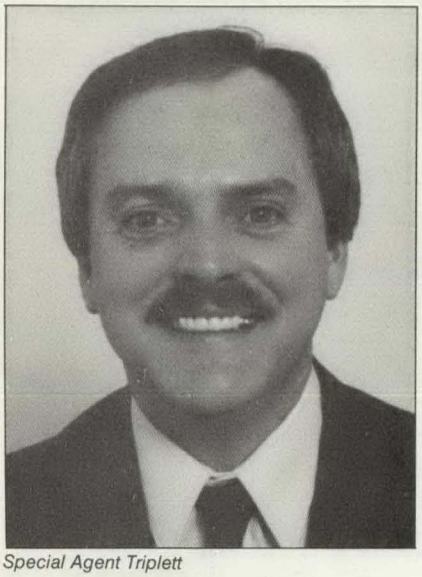
High technology and law enforcement training came together once again in Kansas City at the fifth national satellite teleconference sponsored by the Law Enforcement Satellite Training Network (LESTN). The March 25th program focused on criminal profiling and how it may be used by law enforcement agencies throughout the United States in the investigation of violent crime.

Acting FBI Director John E. Otto joined two Bureau behavioral science experts from the FBI Academy to examine profiling, personality assessment, and other behavioral strategies as investigative tools. The panel also discussed the FBI's Violent Criminal Apprehension Program (VICAP), a part of the National Center for the Analysis of Violent Crime based at the FBI Academy in Quantico, VA. In a case study, Capt. Gary Gene Terry of the Hillsborough County, FL, Sheriff's Department explained how profiling was used in combination with multiagency police investigation and forensic analysis to solve a series of 10 murders in the Tampa area in 1985.

LESTN is a cooperative venture of the FBI's Kansas City Office and the



Special Agent Kortan



Special Agent Triplett

Kansas City, MO, Police Department. The latest program was part of a series of telecasts designed to foster discussion on current issues of interest to law enforcement.

Since the inaugural teleconference in March 1986, LESTN has broadcast to an average of 100 receiving sites and 2,000 viewers. Wide-ranging topics, such as advanced hostage negotiations, drug abuse by police officers, homicide investigations, and drug awareness and education, have been featured.

The programs originate at a Kansas City television station and feature a moderator and a panel of experts on the particular issue being discussed. The format of each program consists of live and preproduced lecture from the experts, followed by call-in questions and answers between the panel and viewing participants across the country.

History of Satellite Network

The marriage of teleconferencing and law enforcement training was first proposed by the FBI's Kansas City training coordinator and two police officers assigned to the department's training academy. When tasked with the assignment to develop and produce training videos, the two officers merged the traditional seminar training session format with an institutional cable channel in Kansas City.

Regular inservice training for police officers and investigators is necessary to ensure up-to-date information is available on the myriad of complex legal, investigative, and administrative issues facing the law enforcement community. Yet, without readily available training at a reasonable cost, usually provided by Federal, State, and/or larger municipal agencies, many departments would be virtually without inservice training.

Seminars have long been used as an effective way to provide training information to law enforcement employees. An expert in a particular subject area lectures to an audience, and members of the audience respond with questions and comments. In recent years, however, the use of video tapes has proved to be a valuable supplement to—and often a substitute for—a speaker to provide information on a wide range of topics. Video tapes allow for greater flexibility in program presentations and dissemination of educational information to agencies where speakers are not readily available.

As a result, the videotaping of seminars, along with the feedback of questions and comments from the audience, has become popular. And with access to a cable channel and up-to-date technology, sought-after speakers on popular law enforcement topics can be made available to a wider audience on a regular and timely basis.

Prompted in part by cable franchise restrictions which would limit distribution of the program in outlying areas, the FBI Agent and the two officers decided that today's technology should be taken a step further—to the sky. With the help of a police department long known for opening law enforcement's door to experimentation and innovation, the idea to bring police training into the satellite age was born in Kansas City.

The FBI has been a continuous source of programming resources for local law enforcement training. However, to ensure the success of this untested project, more than a commitment of speakers and topics was necessary. It became evident that the Bureau's nationwide field structure would be the key to bringing together law enforcement agencies across the country into a single, simultaneous training session.

Production Obstacles

Initially, the technical and logistical aspects of satellite teleconferencing had to be addressed. The three law enforcement officers, armed with a basic understanding of teleconferencing requirements, examined the necessary elements, i.e., production facilities, an "uplink" which transmits the program from the studio to an "earth station," the earth station to send the program up to the satellite, and a transponder, or channel, on the satellite which acts as a mirror and "reflects" the program back to receiving sites. On the ground, two elements are necessary—a satellite receiving dish and a facility with television monitors and telephones to allow viewers to participate.

The first objective was to acquire a production facility. Although a studio was available at the police academy, its dated equipment could not meet the technological demands of a satellite production. At this point, American Cablevision of Kansas City was approached for the use of a facility. Not only was a studio offered at a modest cost, but so was a volunteer crew. And, the cable company's facility had an uplink to an available earth station at WDAF television in the metropolitan area.

The next step was to acquire satellite time and an uplink contract. Both services can be rented—with an advanced reservation and at a modest cost. Production dates and times for the inaugural March 6, 1986, program were set, and the necessary technical arrangements were made.

The major cost associated with satellite teleconferencing lies with the rental of receiving sites. With a hotel, or another type of meeting place capable of accommodating a large group and equipped to receive a satellite program, rental costs can range from $50 to $200 an hour. As a result, a typical 3-hour broadcast to 40 sites could become an expensive endeavor on a limited law enforcement training budget. To help defray this expense to police departments, American Cablevision's parent company, TIME, Inc., was approached. TIME owns cable franchises across the country, and the individual companies agreed to donate the sites as a community service.

Partnership Expands

The Kansas City FBI Office was the logical place to assist in identifying receiving sites. Each of the Bureau's 59 field offices has an Agent assigned as the coordinator for police training in the office's jurisdiction, and this coordinator is familiar with each police department's training officers and educational needs and interests. Because of these established relationships, the FBI representative was a logical choice to coordinate teleconference participation and develop liaison with local cable operators. More importantly, the Bureau coordinator could provide feedback on the quality of the production.

Once the production aspects were in place, the FBI's training facility at Quantico, VA, was contacted to enlist the participation of the Bureau's highly regarded education and training center to ensure programming resources. With a commitment from the FBI's training facility and the support of FBI field training coordinators in those cities with a TIME-owned cable franchise, the Law Enforcement Satellite Training Network was born.

Inaugural Program

Months of planning and discussion materialized on March 5, 1986, when over 1,000 police officers at 32 viewing sites nationwide participated in a live satellite teleconference on the subject of advanced hostage negotiations. The Kansas City chief of police and the Special Agent-in-Charge of the Kansas City Office watched as a combined effort of the two agencies began a new era in law enforcement training. Experts from both the FBI and police departments shared insight on a critical subject with law enforcement officers across the country.

While the response to the initial effort was overwhelmingly positive, the planners began immediately to look for ways to improve and streamline the production process for the next program. The first goal was to expand the number of receiving sites to include those cities not served by a TIME-owned cable company. For this, the Kansas City Area Hospital Television Association was approached about the feasibility of using hospitals around the country as receiving sites. As a result of a meeting in Pittsburgh, PA, with the national director of Hospital Television Networks, over 400 participating facilities donated their meeting rooms and satellite receiving capabilities. With the hospitals' offer of receiving sites came years of valuable experience in satellite teleconference production.

The second teleconference on June 25, 1986, tackled the growing problem of substance abuse by police officers. The program was transmitted through the new hybrid network of cable affiliates and hospitals and featured FBI experts and the personnel director of the Chicago Police Department in a discussion of the behavioral, medical, and legal questions surrounding the issue. Several police training academies and colleges also participated in the

"... satellite teleconferencing [has] found its place in law enforcement."

Acting FBI Director John Otto presented introductory remarks at the fifth national satellite teleconference. Also on the panel were, from left, SA Larry Welch (retired), SA Robert Ressler and SA John Douglas, behavioral science experts from the FBI Academy, and Capt. Gary Gene Terry of the Hillsborough County, FL, Sheriff's Department.

program, increasing the number of receiving sites to over 100 in 80 cities. At some locations, rented dishes and home units were used to receive the broadcast.

It became evident that satellite teleconferencing had found its place in law enforcement. The program on October 22d featured veteran homicide investigators and a Yale University pathologist who offered an overview of techniques critical to conducting successful homicide investigations. On December 3d, a panel of Drug Enforcement Administration narcotics experts, an assistant police chief, and a nationally noted medical researcher and founder of the Cocaine Helpline provided educational information to law enforcement officers on cocaine and "crack" from both the enforcement and demand sides. Feedback following each program was positive as viewer participation grew to an estimated 5,000 viewers at 150 sites for the December teleconference.

The format of each program—provided at no cost to the receiving agencies—allowed viewers at the receiving sites to ask the panelists questions, resulting in an increase in viewer participation and a further sharing of valuable information.

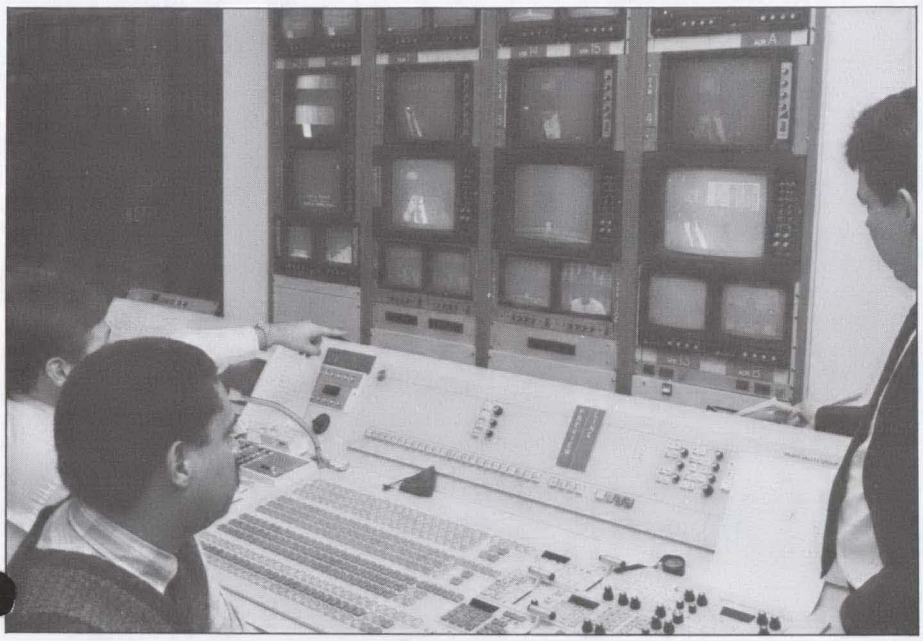
Future of Satellite Teleconferencing

As the cost of satellite receiving dishes continues to drop, many agencies can now afford to purchase their own. And when the volume of quality programming increases, dishes will no doubt be in even greater demand. Many agencies are anticipating increased use of the medium. For example, the New Jersey State Police Academy and the Alcoa, TN, Police Department have been authorized funding for receiving dishes, and the Kansas City FBI Office recently installed one.

The application of satellite technology to law enforcement needs is not limited to the area of training. The capability to encrypt the signal could allow agencies to transmit information on criminal suspects, as well as intelligence data.

The FBI is studying satellite teleconferencing for its own informational and educational needs, and the National Academy and other bureau training programs are likely recipients of such technology. Budget demands will no doubt continue to pressure Federal, State, and local agencies to seek alternative ways to maintain quality training programs.

As savings continue on both the production and receiving ends, the success and continued growth of the medium seems assured. Some predict a satellite channel dedicated entirely to law enforcement will be in place in a few years. As technology advances, it's



The program's producer directs technical adjustments in the television control room.

conceivable that individual agencies could originate a training program which would be made available to all members of the network.

Although the current cost of approximately $10,000 to produce a national satellite teleconference is modest, the Kansas City Police Department continues to explore funding alternatives to further reduce the department's financial burden. Government and foundation grants and corporate sponsorships are among some the potential alternatives under study.

Conclusion

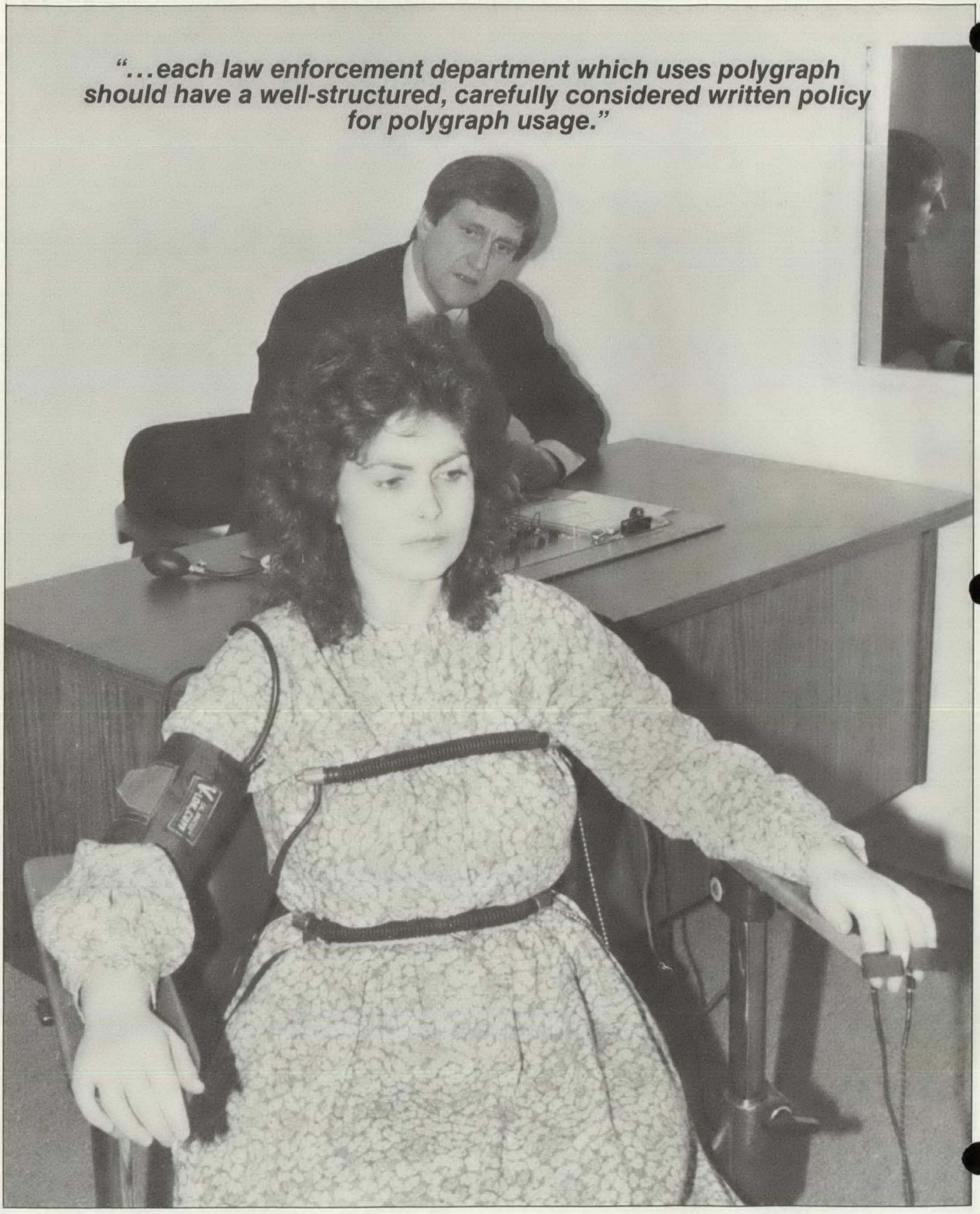
Quality training is essential to the success of every law enforcement agency. The formation of the Law Enforcement Satellite Training Network has proved to be a major step toward meeting the escalating challenge of providing that training.

Satellite teleconferencing has proved to be a cost-effective tool for providing valuable training information to a large law enforcement audience. Although used by business and trade associations for the past few years, teleconferencing is new to law enforcement and the result has been quality, up-to-date training on useful topics at a modest cost.

This joint effort of a major police department and the FBI has benefited from the strengths each agency could offer. The department, in its ongoing responsibility to prepare police officers for the street, is constantly evaluating and searching for ways to improve the level of police training. And the Bureau, with a historical commitment to using its unique national position to maintain the highest standard of law enforcement training, will ensure educational resources for years to come.

FBI

The next LESTN satellite teleconference is scheduled for July 1, 1987, and will examine terrorism. Any law enforcement agency interested in participating is urged to contact the nearest FBI office for further details.


"...each law enforcement department which uses polygraph should have a well-structured, carefully considered written policy for polygraph usage."

Polygraph Policy Model for Law Enforcement

By
RONALD M. FURGERSON
Special Agent/Assistant Section Chief
Document Section
Laboratory Division
Federal Bureau of Investigation
Washington, DC

The intense nationwide controversy surrounding polygraph has caused use of the technique, including use by law enforcement, to be subject to intense scrutiny. A number of State legislatures,[1] as well as the Congress of the United States, have passed or are considering bills which impact on and/or could prohibit certain polygraph testing in the private sector.[2] Sentiment for removal of polygraph testing from the arsenal of investigative techniques available to law enforcement has been expressed recently in the media.[3] Also, the interest in polygraph generated by continuing media attention has heightened the vulnerability of policy administrators and polygraph examiners,[4] and even municipalities,[5] to civil/personnel liability actions from citizens who believe their rights were violated, that they were examined using unprofessional methods and procedures, or that they suffered emotional damage.[6]

To preclude legitimate criticism of a polygraph program and to promote the professional and ethical application of the technique, each law enforcement department which uses polygraph should have a well-structured, carefully considered written policy for polygraph usage. That policy, when applied judiciously and uniformly, will do much to allay fears and charges of polygraph abuse and help prevent loss of the technique's availability by legislative action. It will also serve as a ready source of information for investigators and officials who might have questions concerning polygraph usage.

Incorporated into this article is a chart designed to assist law enforcement executives and managers in quickly identifying most, if not all, of the policy areas that should be addressed for various polygraph applications. If these policy areas, plus a few items which follow later in this article, are covered in a department's policy, and if supervisors and examiners adhere to the policies, use of polygraph will be reasonable, appropriate, and defensible.

The comments which follow describe certain aspects of the chart. Numbers appearing in the text correspond to the circled numbers on the chart. Remember that the chart sets out areas which should be addressed in departmental policy. However, suggested policies, examples, etc., contained herein are just that and should not be construed as necessarily the best or only policy which a department could or should adopt.[7] The best policy for a particular department will depend on many factors and conditions operating within the department.

GENERAL POLICY CONSIDERATIONS

Approval Authority

① Departmental policy should specify which individuals in the agency are authorized to approve particular types of polygraph examinations. It is recommended that approval authorities be designated by title rather than by name to preclude having to change the policy document when a new incumbent is appointed to the position.

The rank/position level which is appropriate for approval authority will vary from department to department, depending on such factors as department size, structure, and the confidence the chief policy-making authority of the department has in the officers to exercise sound judgment and discretion in the use of polygraph. Examples of the level of authority which might be appropriate for various investigative applications are set forth in the chart. Because polygraph effectiveness is a function of how and when the technique is used in the

Special Agent Furgerson

investigative process, it is critical that the approval authority be an experienced, mature investigator who has a proven record of investigative insight.

For particular routine polygraph applications, it may be preferable to authorize examinations by use of a standing order or as a matter of departmental policy. For example, if a department requires that all applicants be polygraphed, considerable administrative time will be saved by a standing order prescribing the conduct of the examinations and setting forth how and at what stage in an applicant's processing the examination is to be administered.

Approval Criteria

When authorizing an examination, the approval authority should:

1) Determine that investigation by other means has been as thorough as circumstances reasonably permit. Polygraph effectiveness and accuracy are greatest when relevant issues and the examinee's knowledge of the matter under investigation have been narrowly defined and well-defined.
2) Insure that the proposed examinee has been interviewed and that consistent with the circumstances of the case, the development of additional information by means of polygraph is essential and timely for further conduct of the investigation. Use of polygraph should *not* be a "last resort" effort to salvage a case. The decision as to when polygraph should be used in the investigative process must be based on individual case circumstances—weighing the exigencies of the situation against the improved capability of the technique to fully resolve issues resulting from greater investigative thoroughness.
3) Verify that there is reasonable cause to believe the person to be examined has knowledge of or was involved in the matter under investigation, or is withholding information relevant to the investigation. Dragnet-type screening of large numbers of suspects should be avoided.
4) Consideration should also be given to the following:
   —Age factor (a waiver must be obtained from a parent or guardian if a minor is examined);
   —Known physical or mental abnormalities;
   —Ensuring full security for an examinee in custody;
   —Ensuring pending prosecution is not jeopardized; and
   —Results of any prior polygraph examinations afforded the examinee.

Although he may not be the final "approval authority" for polygraph examinations, the examiner must make the ultimate determination concerning the suitability of an individual for polygraph testing. Persons who are not sufficiently sound physically or mentally should not be afforded a polygraph examination. Prior to testing, the person to be examined should have had adequate food and rest. The examinee should not, at the time of the examination, be under the adverse effects of alcohol, narcotics, drugs, stimulants, or sedatives. During the pretest interview, the examiner should determine whether the person to be examined is presently

"...the examiner must make the ultimate determination concerning the suitability of an individual for polygraph testing."

receiving or has in the past received medical or psychiatric treatment or consultation.

If the examinee exhibits symptoms of mental or physical fatigue, narcotics addiction or the influence of intoxicants, a mental disorder, etc., the polygraph examination should not be conducted if, in the examiner's opinion, the condition would inhibit the individual's ability to respond or otherwise cause the individual to be an unfit candidate for examination.

A mental disorder could cause the examinee to lose contact with reality or become violent during the test, and an examinee experiencing physical discomfort, disabilities, or defects may suffer abnormal physiological reactions to the test. If the examiner has any doubt concerning the ability of an examinee to safely undergo examination, an opinion/statement should be obtained from the examinee's physician before proceeding with the test.

Finally, polygraph examinations should be given only to individuals who freely and without threat or coercion consent in writing to be examined and who cooperate with and follow the examiner's instructions during the examination process.

Issues

② Matters discussed with examinees during the polygraph interview and questions asked during the actual testing must be scrupulously limited to the matter under investigation and items strictly pertaining to the actual conduct of the examination. The examiner must avoid any suggestion of impropriety or appearance that any part of the examination process is being used to elicit unrelated personal information or to satisfy the examiner's curiosity. Historically, the failure of examiners to exercise good judgment in the matters they discuss with examinees has been a primary source of criticism concerning polygraph.[8] It is important, therefore, that departmental policy identify those issues which are not to be addressed unless they are (in a particular case) directly relevant to the investigation. Religious beliefs or affiliations, beliefs and opinions regarding social matters (e.g., integration, abortion, unions, political preferences, etc.), and information concerning sexual opinions and practices are examples of areas which should be avoided.

Use of Polygraph Examination Results

③ Departmental policy should recognize that polygraph is not a perfect investigative process and that polygraph results, both examiner opinions following chart evaluation and (even) confessions and admissions obtained from examinees, are subject to error. Therefore, results should be considered in the context of a complete investigation. They should not be relied upon to the exclusion of other evidence or used as the sole means of resolving questions of verity. Absent prior stipulated agreement with a defendant and his counsel, polygraph examiner opinions as to truth or deception, based upon interpretation of polygraph charts, are not intended for use as evidence in criminal, civil, or administrative courts. Statements, admissions, confessions, etc., made by examinees during a polygraph examination are normally admissible.[9]

TYPE INVESTIGATION

There are basically five types of polygraph usage which are common in law enforcement and which should be addressed from a policy standpoint, namely, applicant testing, internal investigations, criminal/law enforcement investigations, examinations conducted as a service to other agencies, and examinations of convicted subjects. If polygraph is not permitted in certain situations by a department, departmental policy should state this specifically. This will preclude the possibility of having an examination administered inadvertently contrary to the "intentions" of management. If certain types of examinations are conducted only on rare occasions or as an exception to general procedures, the written policy should be specific as to the situations wherein use of polygraph could be approved.

APPLICANTS

It has been well-documented that polygraph is highly useful in the applicant investigation process, and many law enforcement agencies use it routinely for such purposes.[10] During a recent survey of National Academy students at the FBI Academy, about 50 percent indicated that their departments used polygraph during the applicant investigation process. Its use is predicated on its value in helping to insure the suitability of applicants for law enforcement work (history of criminal or other disqualifying behavior as defined by department policy) and for verifying the accuracy and completeness of information furnished on application forms or statements of personal history or during interviews.[11] It is also believed polygraph serves as a useful deterrent to those seeking to penetrate law enforcement departments for untoward purposes.

④ Departmental policy should be clear as to which classes of applicants are, or may be, required to submit to

"Managers should be aware of polygraph limitations and use good judgment in evaluating and making investigative and personnel decisions based on polygraph findings."

pre-employment polygraph examinations. Employment application literature and application forms should specify if a polygraph examination will be, or may be, required during application processing and that the purpose of the examination will be to verify the accuracy and thoroughness of information furnished. While this procedure is useful in alerting applicants to the use of polygraph, it also insures uniform application of the technique and acts as a deterrent against the submission of false/incomplete information by applicants. If successful completion of a polygraph is a necessary prerequisite for employment according to departmental policy, all literature concerning employment opportunities should indicate this fact.

Those departments which do not use polygraph as a routine procedure during applicant processing may elect to use it only in those instances when questions concerning the applicant's suitability for employment arise during the background investigation. Polygraph can be very valuable when problems of conflicting information develop and other investigative techniques are ineffective in resolving the matter. Departments using polygraph in this manner should include language in their polygraph policy and/or hiring policy which clearly provides for the use of polygraph on a case-by-case basis as required to resolve background investigation issues.

Once a department decides to use polygraph as part of its applicant processing, policy should be established to define clearly the purpose of the examination and the specific issues to be addressed during polygraph testing. Great care should be exercised in this area to ensure that polygraph is used wisely. Generally, it is preferable that polygraph be used only for those areas of interest which cannot be explored effectively by other means, e.g., thorough background investigation, appropriate records checks, and medical examinations and psychometric testing or psychiatric interviews.[12] This is consistent with the philosophy that polygraph should be a complement to, and not a substitute for, other investigative techniques, or in this case, for traditional personnel selection methods.

Questions concerning the applicant's basic honesty would be appropriate. As with polygraph examinations conducted for other purposes, questions used for applicant examinations must be reasonable and as unobtrusive as possible and should be such as would be appropriate in any personnel/applicant interview situation, or which could be asked on the department's personnel application form.

INTERNAL INVESTIGATIONS

Polygraph is often useful in investigations involving law enforcement agency personnel. The majority of these uses occur in situations set forth on the accompanying chart.

Personnel Security/Integrity Program

Polygraph is used by some departments to insure an employee's suitability for initial or continued assignment to selected special duties, e.g., vice, narcotics, intelligence, organized crime, etc.[13] It is essential that such examinations be administered under a consistent, uniform policy to demonstrate that fairness, not favoritism, is involved in these critical selections. The examination should be concerned only with the officer's freedom from "compromise" or some other type of coercive influence prior to and/or during the sensitive assignment.

Criminal Investigation Involving Departmental Officer or Employee (Voluntary)

If an officer or employee becomes involved as a subject or witness in a criminal investigation wherein prosecution is the objective, he or she should be treated the same as any other citizen, insofar as possible use of polygraph is concerned (given *only* if the employee freely volunteers to take the examination). This is necessary to protect the employee's constitutional rights and permit use of any statements or admissions made during the examination to be entered into evidence. In these situations, as in all other law enforcement applications, it is recommended that no adverse inference be drawn from a subject's refusal to submit to an examination. Adverse inferences *may* be drawn in administrative inquiries and internal investigations, but refusal to submit to examination in these situations *should not* constitute the sole basis for disciplinary action. (8)

Internal Investigation/Administrative Inquiry (Required)

Polygraph can be highly useful in investigations involving an employee's conduct where prosecution is not the ultimate objective. For reasons of fairness and to preclude allegations that polygraph is being used to coerce or intimidate an employee, or to otherwise single them out for "special treatment," departmental policy should specify those types of situations which could result in an employee being required to submit to a polygraph examination. It is best if the policy requires the existence of a substantial objective basis (not just a vague suspicion or intuition) to believe that the employee was involved in a serious violation of law or departmen-

tal regulation. The types of forbidden activities or situations which might result in a requirement for a polygraph examination should be specified in the policy. Examples of such situations are set forth in the sidebar. ⑥

Person Making Allegation

If a citizen or another departmental employee makes an allegation of misconduct against an employee, polygraph may be useful in determining if there is any substance to the allegation. Of course, if it is possible to establish the veracity of the allegation by other means, that course should be followed. But, as is often the case, when a serious allegation is made and other avenues for substantiating its truthfulness are not available, polygraph may be the only viable alternative.

While polygraph has potential application for testing both the accuser and the subject of the allegation, experience has demonstrated the advisability of testing the accuser first. Frequently, persons who are making spurious allegations out of revenge, jealousy, or for whatever motive will refuse to be tested or will admit during testing that the allegations were unfounded. When an accuser does consent to testing, the polygraph process is valuable in that it helps to narrow the issues and eliminate exaggerations and/or partial truths. Another reason for testing the accuser first is that it often permits resolution of the matter without having to unnecessarily subject a valued employee to an examination. It is unfortunate that there will be situations where examination of the employee will be the only viable means for the employee to demonstrate his innocence and clear his name. Yet, it is fortunate that there is a means.

It should be noted that just because a person making an allegation "fails" a polygraph examination, based upon the examiner's interpretation of the polygraph charts, the possibility still exists that there was an element of truth in the allegation. It is possible that an accuser, by either exaggerating the nature and extent of an employee's wrongdoing, or by lying about or denying personal involvement in the wrongdoing, may be found deceptive during the polygraph examination, while actually furnishing some truthful and accurate information about the employee's wrongdoing.

It is also possible that an accuser may honestly believe he is being factual in what he is reporting, and yet be totally mistaken. Because polygraph is only useful in determining the examinee's perception of the truth, and not actual or "ground truth" as polygraph researchers say, the accuser may clear the polygraph as "non-deceptive" with the result that the polygraph findings are misleading. Managers should be aware of polygraph limitations and use good judgment in evaluating and making investigative and personnel decisions based on polygraph findings. Because an element of uncertainty normally exists concerning polygraph chart interpretation and the exact nature of an examinee's psychophysiological responses to questions, it is always recommended that if at all possible, no decisions be made solely on the basis of an examiner's interpretation of polygraph charts.

Examiner Selection in Internal Investigations

⑤ For obvious reasons, it is important that examiners chosen to work internal investigation cases be selected with special care. There should never be a compromise concerning the quality of the examiner selected for these types of examinations. The examiner must have impeccable credentials as an examiner and be respected for his competence, integrity, and high ethical standards.

Objectivity and accuracy will be promoted and ethical considerations satisfied by use of an examiner who is not more than slightly acquainted with employees being tested. It is even preferable that examiners not know the accused employee or the person lodging the allegation.[14] To accomplish this, smaller departments may use an examiner from another department or agency,[15] or even to contract for the services of a commercial examiner.

To protect the confidentiality of internal investigations and prevent further embarrassment and extraneous psychological stress to an officer, consideration should be given to having the examination conducted at a site where the testing will not be apparent to fellow employees. Use of an offsite location, when needed, will prevent rumors and unnecessary damage to an employee's reputation.

LAW ENFORCEMENT APPLICATION

The primary use of polygraph in the law enforcement community is for investigations of criminal violations. All the general policy considerations discussed above apply to these applications, including policy on approval authority and criteria, limitations on issues to be addressed, and use of polygraph results and examiner conclusions.

⑦ One area deserving special comment is the use of polygraph to verify information furnished by citizens and informants, especially those whose reliability has yet to be established or is

"...department policy should also include provisions for establishing that polygraph examinations were taken freely and voluntarily."

suspect. Consideration should be given to establishing a policy that requires polygraph be considered prior to significant commitments of manpower or financial resources solely on the basis of unsubstantiated information furnished by citizens or informants. This can be especially useful in matters involving allegations against prominent individuals and public officials whose reputations could be unduly tarnished by the mere existence of an investigation. Frequently, the use of polygraph for such "verification" or "confirmation" purposes will disclose there is no basis for the allegations or that they were grossly exaggerated or distorted. In either case, valuable investigative time will have been saved and possible embarrassment to a citizen of the department will have been prevented.

An interesting application of polygraph is to aid in establishing "probable cause" where a warrant is sought and part or all of the basis for its issuance is predicated on information furnished by an informant or witness of unknown reliability.[16] Polygraph, in this situation, can add weight to the probable cause documentation.

In view of the inherently stressful nature of polygraph examinations, it is recommended that departmental policy prohibit the use of polygraph for the dragnet-type "screening" of large numbers of suspects in criminal investigations. Likewise, the use of polygraph as an expedient substitute for logical investigation by conventional methods should be forbidden. Limiting polygraph usage in this manner will do much to improve its effectiveness.[17]

POLYGRAPH ASSISTANCE TO OTHER AGENCIES

Occasionally, other departments, law enforcement and otherwise, may request polygraph assistance for one of their investigations or in connection with some type of personnel action. There is generally no reason why the support should not be given, provided the requested examination meets the standards for approval set forth in the policy of the department furnishing the support.

In those situations where polygraph support for particular applications, e.g., applicant processing, is furnished on a routine basis, an interdepartmental memorandum of understanding is appropriate. It should describe the terms of the agreement and the responsibilities of each department.

For polygraph support requests of a nonroutine nature, it is useful for the requesting agency to formalize requests in writing on a case-by-case basis. Requests should set forth the nature of the investigation/inquiry and briefly describe the investigation conducted to that point. The polygraph examiner can be briefed on specific details by an official of the requesting agency most familiar with the case. The formal request should also specify the issue(s) to be addressed, any special precautions or instructions to be observed, and the type of examination report desired. The exact questions to be asked and their wording should be left to the discretion of the polygraph examiner.

When another department requests polygraph support for the first time, or when new requesting officials make their initial requests for support, they should be furnished a copy of the instructions in force at the examining agency so there will be no misunderstanding regarding the policy followed when conducting an examination. It would also be wise for the examiner to brief officials from the requesting agency concerning polygraph theory, limitations and capabilities, and evaluation of polygraph results and examiner conclusions. A briefing is especially critical for noninvestigative agencies whose officials may have no basic understanding of the investigative process and the proper role of polygraph.

POST-CONVICTION EXAMINATIONS

(9) Following their convictions, but prior to sentencing, the examination of defendants may be very useful. Examination results may legitimately influence sentencing and be helpful in a number of post-conviction investigative activities. Examples of particularly good uses of polygraph in post-conviction circumstances are contained in the sidebar.

The use of polygraph following a trial, however, should normally be limited to legitimate, continuing investigative interests. Except under the most compelling circumstances, such as when ordered by a judge, post-conviction examinations *should not* address issues such as the veracity or guilt of the defendant concerning the basic trial issue. Polygraph's proper role is not to usurp the function of the trial process. When polygraph is used as part of a plea or pre-sentencing agreement, the terms of the agreement should be carefully documented and approved by the judge, defense attorney, prosecutor, and the defendant.

MISCELLANEOUS CONSIDERATIONS

Polygraph Consent Forms

In addition to whatever method is used for advising examinees of their constitutional rights, department policy should also include provisions for establishing that polygraph examinations were taken freely and voluntarily. This

can probably best be accomplished with a preprinted form developed in cooperation with the department's legal counsel. Consultation with legal counsel is important to insure that all legal requirements, including pertinent judicial precedents from recent court decisions, have been satisfied. As a minimum, a polygraph consent form should establish that the examinee realizes that the examination is to be taken freely and voluntarily, that it will be discontinued at any time at the request of the examinee, and that the examinee may refuse to answer any particular question during the examination.

In designing a polygraph consent form (or a consent to interview with polygraph form, which may be a more appropriate name), it is also useful to include wording which indicates that the examinee is consenting to an "interview with polygraph" or that the polygraph examination is an interview process which includes the use of a polygraph instrument. The purpose is to preclude misunderstanding concerning the nature of the examination process, which includes pretest and post-test interview/interrogation phases as well as the actual testing phase. The component phases of the polygraph process are described adequately elsewhere.[18] What is critical to understand is that following indications of "deceptive" responses during the conduct of the testing phase, it is normal and proper for the examiner to attempt to determine the nature of any problems the examinee had in responding to the test questions. If sensible and adequate reasons for the observed reactions are given by the examinee, additional tests may be conducted to verify that the examinee has indeed been candid. The test-interview-retest process continues until the examinee either tests nondeceptive or the examiner concludes that deception is the only apparent reason for the noted reactions to relevant questions. Under normal circumstances, there is no requirement that each retesting and/or interview phase be preceded by additional rights advisements. However, any deviation from normal circumstances, such as a significant delay between phases, should trigger consideration as to the advisability of reminding examinees of their constitutional rights.[19]

Monitoring/Recording Polygraph Examinations

While there is no absolute requirement that polygraph examinations must be monitored, experience has demonstrated that significant benefits may be derived from this practice. There are no appreciable drawbacks to such witnessing.

In attaching the polygraph components, examiners must make physical contact with examinees when placing components to their fingers, arms, and the breast area of their bodies. With female examinees, it is advisable to have a witness to this procedure to assure that the examiner's conduct was entirely proper.

When an examinee is believed to have been less than candid during polygraph testing, an attempt is normally made to elicit truth through questioning and persuasive reasoning. Confessions or incriminating admissions are often made by examinees as a result of this approach. These confessions and admissions are sometimes later retracted, changed, or denied. During the course of examinations, examinees also frequently make subtle, but significant, adjustments to previous statements made during the investigation. For these reasons, it is highly useful to have the case officer present to witness the polygraph interview.

Experience has also taught that witnesses, while of great value, should not be physically present in the polygraph room during the examination process. The examiner must establish rapport with the examinee in an emotionally charged atmosphere. This can normally be accomplished best in a one-on-one situation with no one else present in the room. Further, deceptive examinees are more likely to tell the truth when confronted with examination results if the case officer, before whom the examinee has previously maintained a facade of truthfulness and cooperation during previous interviews, is not present. Being alone with the impartial and objective examiner presents an optimum opportunity for the examinee to be candid regarding the issue with minimal damage to his self-esteem and pride.

Necessary witnessing of examinations can generally take place free of outside interference or distraction by use of one-way windows and sound reproducing (monitoring) equipment. Some situations, however, involve space limitations and physical conditions which mitigate in favor of closed-circuit television for witnessing.

While, given certain conditions, it may be possible for witnessing/monitoring to be accomplished legally without the knowledge of examinees, there is generally no compelling reason why that practice would be advisable. Experience has shown that advising examinees of the presence of witnesses on monitoring devices prior to the examination has not inhibited or impacted adversely on the examination process.

"...experience has demonstrated that significant benefits may be derived from [monitoring polygraph examinations].

Witness observes polygraph examination through one-way window.

The notification on witnessing/monitoring of examinations can be accomplished during execution of the advice of rights and polygraph consent process.

In establishing departmental policy, administrators should also consider whether polygraph examinations, or portions of the polygraph examination process, should be recorded. Occasionally, good judgment and/or circumstances, such as a court order, may dictate the advisability of or require recording. In most situations, however, the advantages which would accrue from recording (either audio or video or both) are available through routine witnessing/monitoring as recommended herein, and yet have none of the disadvantages which may be associated with recording. As with any other interview or interrogation situation, many things are said which would be misleading when viewed only in the context of information captured on a recording. Depending on examiner competence and the availability of witnesses who have received special instruction, recording of the testing phase of the examination process could be beneficial by providing a method whereby use of physical countermeasures by the examinee might be better detected.

Therefore, with regard to witnessing/monitoring, it is recommended that absent circumstances which make it impossible or impracticable, polygraph examinations be witnessed as a matter of policy, that such witnessing be accomplished by witnesses located outside the polygraph suite, and that all such witnessing be conducted with the prior knowledge of examinees. Policy should also specify that witnesses are to be limited to those with a legitimate interest in the investigation and/or those who will serve as government witnesses to the examination process. The recording of examinations may be advisable or required in some situations.

Examiner Competence

As examiner competence is of primary importance in the operation of a successful polygraph program, it is recommended that departments establish minimum (certification) standards for their examiners. The following are suggested:

—Graduation from a reputable polygraph school (The American Polygraph Association accredits polygraph schools which adhere to prescribed curricula and instructor requirements);

—Participation in periodic retraining seminars/courses at established intervals—preferably not to exceed 2 years; and

—Conducting a minimum number of examinations annually (The FBI requires its examiners to conduct a minimum of 48 per year to retain certification).

Quality Control

Experience has shown the value of quality control as an integral part of law enforcement polygraph usage. In such a program, polygraph charts and documentation are reviewed "in the blind" by another senior and well-qualified ex-

(continued p. 19)

tigation. They are not to be relied on to the exclusion or other evidence or used as the sole means of resolving questions of verity. Polygraph examiner opinions as to truth or deception based upon interpretation of polygraph charts are not intended for use as evidence in criminal, civil, or administrative courts. Statements, admissions, confessions, etc., made by examinees during a polygraph examination are admissible.

4 Employment application literature and forms should specify that accuracy and thoroughness of information furnished on the application are subject to verification by polygraph examination.

5 Selection of a polygraph examiner to conduct examinations of department employees must be handled with special care to insure objectivity. Consideration may be given to using an examiner from another department who does not know the examinee. Also, if the site of the department's polygraph suite is near the examinee's work space and the fact that the employee was being tested would be readily apparent to the employee's peers and fellow employees, thereby unduly increasing the psychological stress on the employee, good judgment may dictate conducting the examination away from the employee's own office/precinct.

6 The department must establish the existence of a substantial objective basis to suspect that the employee is involved in one or more of the following situations.

a. The intentional and unauthorized release of sensitive, protected information (including, for example, the disclosure of information which is prohibited by law or regulation) with the reasonable expectation that it would ultimately be disclosed to those from whom the information is protected and would seriously and adversely affect a departmental function;

b. Serious questions concerning an employee's relationship with or allegiance to an organized criminal element;

c. The illegal or improper exercise of influence, coercive or otherwise, by an individual or group on an employee, which could reasonably be expected to seriously affect or inhibit the employee in the impartial and effective performance of the employee's duties;

d. The intentional and unauthorized destruction, mutilation, alteration, misplacement, taking, falsification, or other impairment of previously existing documents or evidence in the department's possession or control;

e. Use or unauthorized dealing in controlled substances, as defined under the Comprehensive Drug Abuse and Controlled Substances Act of 1970, Title 21, United States Code, by department employees during the course of their employment; or

f. The furnishing of false statements or the failure to candidly disclose information concerning prior criminal activities requested during the course of his/her employment processing.

7 Use of polygraph should be considered prior to making significant commitments of manpower or financial resources solely on the basis of unsubstantiated information, particularly in sensitive investigations or when information which is to serve as case predication is not readily verifiable by other means.

8 The fact that a subject/suspect was requested to submit to a polygraph examination and refused to do so should not be recorded in any type of investigative report in a manner which could reasonably be construed as prejudicial to the individual.

9 Post-conviction continuing investigative interests include investigation to resolve issues that were not central to the issues adjudicated by the jury or court. Examples are:

a. Perjury during trial;

b. Defendant's compliance with plea bargaining arrangements/conditions;

c. Accuracy and completeness of information furnished by cooperating witness; and

d. Validity of extenuating and mitigating circumstances bearing on sentencing considerations.

1 Approval: When authorizing an examination the approving authority should determine that an investigation by other means has been as thorough as circumstances reasonably permit, recognizing that polygraph effectiveness and accuracy are greatest when relevant issues and the examinee's knowledge of the matter under investigation have been narrowly and well-defined. The proposed examinee should have been interviewed, and consistent with the circumstances of the case, the development of additional information by means of polygraph should be essential and timely for further conduct of the investigation or inquiry. There should be reasonable cause to believe that the person to be examined has knowledge of or was involved in the matter under inquiry or investigation, or is withholding information relevant to the inquiry of investigation. The following should be considered:

a. Determine if age is a factor. If a minor is to be examined, ensure a waiver is obtained from a parent or guardian.

b. Are there any known physical or mental abnormalities?

c. If the examinee is in custody, can full security and control be assured?

d. Will the use of polygraph jeopardize pending prosecution?

e. What were the results of any prior polygraph examinations afforded the examinee?

Although not the final "Approval Authority" for polygraph examinations, the polygraph examiner must make the ultimate determination concerning the suitability of an individual for polygraph testing. Due to the nature of polygraph examinations, the following guidelines are appropriate:

a. Persons who are not in sufficiently sound physical or mental condition will not be afforded a polygraph examination.

b. A person to be examined should have had adequate food and rest before the examination. Examinee should not, at the time of the examination, be under the effects of alcohol, narcotics, drugs, stimulants, or sedatives. During the pretest interview, the examiner will specifically inquire of the person to be examined whether he/she is presently receiving or has in the past received medical or psychiatric treatment or consultation.

c. Polygraph examinations will not be conducted if, in the opinion of the examiner, any of the following inhibit the individual's ability to respond or otherwise cause the individual to be an unfit candidate for examination:

1. It is apparent that the examinee is mentally or physically fatigued.
2. The examinee is unduly emotionally upset, intoxicated, or adversely under the influence of a sedative, stimulant, or tranquilizer.
3. The examinee is determined to be addicted to narcotics.
4. The examinee is known to have a mental disorder which causes the examinee to lose contact with reality or which would reasonably result in the examinee becoming violent during a test.
5. The examinee is experiencing physical discomfort of significant magnitude or appears to possess disabilities or defects which, in themselves, might cause abnormal physiological reactions.

d. If the examiner has any doubt concerning the ability of an examinee to safely undergo an examination, obtain an opinion/statement from the examinee's physician before proceeding with the test.

2 Issues: The following issues are not to be addressed unless directly relevant to the investigation or inquiry and then only in keeping with established departmental regulations/policy:

a. Religious beliefs or affiliations;

b. Beliefs and opinions regarding social matters;

c. Information concerning sexual opinions and practices.

3 Use of Examination Results: Polygraph examinations are aimed at developing information which was unavailable prior to the examination (e.g., confessions, admissions against interests, the identification of false/exaggerated informant information, false exculpatory statements, false claims by alleged "victims," and the development of additional investigative avenues). Results are to be considered in the context of a complete inves-

	TYPE INVESTIGATION	PREDICATION	APPROVAL AUTHORITY (1)	CONSEQUENCE OF FAILURE TO TAKE OR COOPERATE DURING EXAM	ISSUES (2)	USE OF POLYGRAPH EXAMINATION RESULTS (3)	SPECIAL REQUIREMENTS & CONSIDERATIONS
APPLICANTS	**APPLICANT** (pre-employment examination) (4)	**NEED TO:** • Insure suitability • Verify accuracy & completeness of info. on application • Resolve questions or conflicts arising during background investigation	Personnel Officer/ Administrative Officer/ Personnel Selection Board or Standing Order/Policy	**NO JOB** a condition of employment	• Freedom from coercive forces • History of criminal or other disqualifying behavior • Accuracy and completeness of info on application form	One factor to be considered in **SUITABILITY DETERMINATION**	Scope of any "lifestyle" questions should be scrupulously limited to those areas of legitimate interest as defined by department policy
INTERNAL INVESTIGATIONS	**PERSONNEL SECURITY/ INTEGRITY PROGRAM**	**NEED TO:** insure employee's suitability for initial or continued assignment to selected special duties, e.g., vice, narcotics, intelligence, o.c., etc., as defined by department policy	Personnel Officer/ Administrative Officer/ Personnel Selection Board or Standing Order/Policy	Denial of Participation in or removal from special duty or assignment	**ISSUES PERTAINING TO SUITABILITY OF EMPLOYEE** for assignment to particularly sensitive duties or freedom from "compromise" prior to or during assignment	One factor to be considered in **SUITABILITY DETERMINATION**	Exercise special care in selecting polygraph examiner (5)
	DEPARTMENTAL OFFICER/EMPLOYEE (Voluntary)	**INVESTIGATIVE NEED** Same justification as for use in any investigation	Chief of Police/ Director of Public Safety/ Director/Superintendent of State Police/ Highway Patrol/ State Bureau of Investigation	**NONE** The officer or employee should be treated the same as any other citizen whose submission to an examination is on a voluntary basis	Issues relevant to **BASIC INVESTIGATIVE THRUST**	**INVESTIGATIVE DIRECTION**	(5)
	DEPARTMENTAL OFFICER/EMPLOYEE (Required) Administrative Inquiries and Internal Investigations involving certain serious violations of law or policy	Substational objective **BASIS TO BELIEVE OFFICER/EMPLOYEE MAY BE WITHHOLDING INFORMATION** relevant to the matter being investigated (6)	Chief of Police/ Director of Public Safety/ Director of Internal Affairs Division/ Director/Superintendent of State Police/ Highway Patrol/ State Bureau of Investigation	**MAY DRAW ADVERSE INFERENCE** (but may not consititute sole basis for disciplinary action)	Issues relevant to **BASIC INQUIRY/INVESTIGATION**	**INVESTIGATIVE DIRECTION** One factor considered in **ADMINISTRATIVE/ DISCIPLINARY ACTION DETERMINATION**	(5)
	PERSON MAKING ALLEGATION against officer/employee	**INVESTIGATIVE NEED** Same justification as for other types of investigation	Chief of Police/ Director of Public Safety/ Director of Internal Affairs Division/ Director/Superintendent of State Police/ State Bureau of Investigation	**FACTOR TO BE CONSIDERED**	Issues relevant to **BASIC INVESTIGATIVE THRUST**	**INVESTIGATIVE DIRECTION** One factor considered in **ADMINISTRATIVE/ DISCIPLINARY ACTION DETERMINATION**	Select polygraph examiner with special care to insure objectivity, possibly an examiner from another department who does not know officer/employee against whom allegation is directed
LAW ENFORCEMENT	**LAW ENFORCEMENT MATTERS**	**INVESTIGATIVE/OPERATIONAL NEEDS** (7)	Division/District/Precinct Commanding Officer or Chief of Detectives	**NONE** (8)	Issues relevant to **BASIC INVESTIGATIVE THRUST**	**INVESTIGATIVE or OPERATIONAL DIRECTION**	Dragnet-type screening of large numbers of suspects or use as a substitute for logical investigation by more conventional means prohibited
OTHER AGENCIES	**ASSISTANCE TO OTHER AGENCIES/** Law Enforcement Departments	**LEGITIMATE INVESTIGATIVE NEED** when requested in accordance with conditions of interdepartmental agreements	Chief of Police/ Director of Public Safety/ or Standing Order/Policy	Depends upon circumstances and regulations of requesting agency	Issues relevant to **BASIC INVESTIGATIVE THRUST**	**REPORTED TO REQUESTING AGENCY** for appropriate use	Be alert to requests for examinations of questionable propriety or having political overtones or implications
POST CONVICTION	**POST CONVICTION/ PRE-SENTENCING** (continuing investigation)	Required in furtherence of continuing investigative interests (9)	Division/District/Precinct Commanding Officer	**MAY INFLUENCE PLEA AND SENTENCING** Arrangement	**LIMITED TO ISSUES WHICH PREDICATED EXAMINATION** Should not address issues adjudicated during judicial proceedings	May influence **SENTENCING AND POST CONVICTION INVESTIGATIVE DIRECTION**	If exam is conducted as part of a plea or pre-sentencing agreement, terms of the agreement should be carefully documented and approved by the judge, defense attorney and prosecutor
	POST CONVICTION/ PRE-SENTENCING (Veracity/Guilt of defendant concerning trial issue)	May be **ORDERED/REQUESTED BY TRIAL JUDGE OR DEFENSE ATTORNEY**	Chief of Police/ Director of Public Safety	**MAY INFLUENCE POST TRIAL JUDICIAL DETERMINATION**	Limited to **SPECIFIED ISSUES**	Possible factor in **POST TRIAL JUDICIAL DETERMINATIONS**	Polygraph should be used in this manner only under the most compelling of circumstances. Polygraph's proper role is not to usurp the function of the trial process

* Large numbers refer to notes on subsequent pages

"...examiner competence is of primary importance in the operation of a successful polygraph program...."

FBI quality control examiner reviews charts submitted by field examiner.

aminer to insure that they substantiate the conclusion of the testing examiner as to truth or deception. Departments too small to establish their own quality control program may be able to avail themselves of such a program through cooperation with another department. If it is impossible to obtain a quality control review locally, charts and documentation from particular important cases may be submitted to the FBI for review. They should be sent to: **Director, Federal Bureau of Investigation, Attn: FBI Laboratory, Washington, DC 20535.**

FBI

Footnotes

[1]Norman Ansley, *Quick Reference Guide to Polygraph Admissibility, Licensing Laws, and Limiting Laws,* 11th ed. (Severna Park, MD: American Polygraph Association, 1987).

[2]H.R. 1524, "Employee Polygraph Protection Act," 99th Cong., 2d Sess. (1986) and S. 1815, "Polygraph Protection Act of 1985," 99th Cong., 1st Sess. (1985). If enacted these bills would prohibit private sector employers from administering polygraph examinations to employees or prospective employees.

[3]Paul Berg, "Plea for More Restraints on Use of Polygraph," *The Washington Post,* January 13, 1987, Health Sect., p. 25.

[4]42 U.S.C. sec. 1983 reads: "Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory, subjects, or causes to be subjected, any citizen of the United States or other persons within the jurisdiction thereof to the deprivation of any rights, privileges or immunities secured by the Constitution and laws, shall be liable to the party injured on an action at law, suit in equity, or other proper proceeding for redress." For a discussion of constitutionally based civil litigation against law enforcement officers, see, Jeffrey Higginbotham, "Defending Law Enforcement Officers Against Personal Liability in Constitutional Tort Litigation," *FBI Law Enforcement Bulletin,* vol. 54, No. 4, April 1985, pp. 24–31, & No. 5, May 1985, pp. 25-31.

[5]A municipality may also be named as a defendant in an action under 42 U.S.C. sec. 1983 charging a constitutional violation only where the individual law enforcement officer's conduct was the result of a custom, policy, or practice of the municipality. For a discussion of municipal liability arising from constitutional tort litigation, see, Daniel L. Schofield, "Law Enforcement and Government Liability: An Analysis of Recent Section 1983 Litigation," *FBI Law Enforcement Bulletin,* vol. 50, No. 1, January 1981, pp. 26–31.

[6]According to a "News-Lines" article, *U.S. News And World Report,* p. 77, April 1, 1985, "Polygraph tests can cause emotional damage, the Minnesota Court of Appeals declared in affirming a lower court's $60,000 award against a bank. After deposits were missed, two tellers were asked to take lie detector tests. One began having nightmares in which the polygraph turned into an electric chair. She also was unable to work with money. Psychiatrists testified that the test had led to post-traumatic-stress syndrome...."

[7]For a comprehensive and instructive example of a polygraph program policy statement and implementing instructions, see, Department of Defense (DOD) Polygraph Program Directive, Number 5210.48, December 24, 1984, which established basic DOD policy for polygraph usage, and DOD Polygraph Program Regulation Number 5210.48-R, January 1985. The regulation, which implemented the polygraph policy, specifies the circumstances under which the polygraph may or shall be used, prescribes procedures for conducting examinations, and establishes standards for the selection, training, and supervision of DOD polygraph examiners. The directive and regulation were published in *Polygraph Law Reporter,* vol. 8, No. 1, March 1985, and No. 2, June 1985, respectively, Norman Ansley ed., (Severna Park, MD.: American Polygraph Association). For another treatment of this subject area, see, Richard O. Arthur, "Recommended Law-Enforcement Polygraph Rules & Regulations," *The Journal of Polygraph Science,* vol. 21, No. 3, November–December 1986. The *Journal* is published by and available through the National Training Center of Lie Detection, Inc., 200 West 57th Street, New York, NY 10019.

[8]See, e.g., Stephen Budiansky, "Lie Detectors," *The Atlantic,* vol. 254, No. 4, October 1984, p. 40.

[9]James K. Murphy, "The Polygraph Technique—Past and Present," *FBI Law Enforcement Bulletin,* vol. 49, No. 6, June 1980, p. 4. Also, see, *Polygraph Law Reporter,* Norman Ansley ed., (Severna Park, MD.: American Polygraph Association) for abstracts of Federal and State cases wherein issues related to admissibility of polygraph, or other forms of truth verification, are addressed.

[10]Billy Dickson, "Pre-Employment Polygraph Screening of Police Applicants," *FBI Law Enforcement Bulletin,* vol. 55, No. 4, April 1986, pp. 7–9.

[11]*The Accuracy and Utility of Polygraph Testing* (Washington, DC: Department of Defense, 1984), pp. 9–10. Also see, generally, David E. Nagle, "The Polygraph in Employment: Applications and Legal Considerations," *Polygraph,* vol. 14, No. 1, March 1985, pp. 1–33.

[12]Frank S. Horvath, "The Police Candidate Polygraph Examination: Considerations for the Police Administrator," *Police,* June 1972, pp. 33–38.

[13]The value of requiring polygraphs for officers assigned to law enforcement intelligence units is pointed out in *Basic Elements of Intelligence: A Manual of Theory, Structure and Procedures for*

[13]The value of requiring polygraphs for officers assigned to law enforcement intelligence units is pointed out in *Basic Elements of Intelligence: A Manual of Theory, Structure and Procedures for use by Law Enforcement Agencies Against Organized Crime,* E. Drexel Godfrey, Jr., Ph.D., and Don R. Harris, Ph.D., (Technical Assistance Division, Office of Criminal Justice Assistance, Law Enforcement Assistance Administration, U.S. Department of Justice, p. 97, 1971).

[14]Richard O. Arthur, "Should a Law-Enforcement Polygraphist Examine His Fellow Officers?—NO!" *The Journal of Polygraph Science,* vol. 9, No. 3, November–December 1974, pp. 3–4; cf., James C. Young, "Should a Law-Enforcement Polygraphist Examine His Fellow Officers?—YES!" *The Journal of Polygraph Science,* vol. 9, No. 3, November–December 1974, pp. 1–2.

[15]Melvin Kilbo, "Interagency Agreement," *FBI Law Enforcement Bulletin,* vol. 55, No. 5, May 1986, pp. 14–15.

[16]*Herlong* v. *State,* 236 Ga. 326, 223 S.E.2d 672 (1976). In this murder prosecution, it was ruled that the court did not err in admitting evidence that a witness had been given a lie detector test and that warrants were obtained for the defendant immediately thereafter; such testimony was admissible to explain the conduct of police officers.

[17]Supra note 15.

[18]*Scientific Validity of Polygraph Testing: A Research Review and Evaluation—A Technical Memorandum* (Washington, DC: U.S. Congress, Office of Technology Assessment, OTA-TM-H-15, November 1983), pp. 11–25. Also see, Stanley Abrams, *A Polygraph Handbook for Attorneys* (Lexington, MA: Lexington Books, 1977), pp. 69–97.

[19]While this additional advisement of rights may not be necessary, it may be useful in subsequent legal proceedings in showing that given the totality of the circumstances, there was a knowing and intelligent waiver as required under *Miranda* v. *Arizona,* 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed. 2d 694 (1966). See *Vassar* v. *Solem,* 763 F.2d 975 (8th Cir. 1985) for the court's discussion on the voluntariness of confessions obtained following the testing phase of polygraph examinations. See also, *United States* v. *Eagle Elk,* 711 F.2d 80, 83 (8th Cir. 1983) *cert. denied,*—U.S.—, 104 S. Ct.1015, 79 L.Ed.2d 245 (1984). This court held that the defendant had, prior to his polygraph examination, knowingly and intelligently waived his right to have counsel present at a post-polygraph interrogation.

Book Review

The Heist: How A Gang Stole $8,000,000 at Kennedy Airport and Lived to Regret It. Ernest Volkman and John Cummings, Franklin Watts, 1986 ($16.95).

In 1978, seven robbers escaped with $8 million in cash, foreign currency, gold, and jewels from the Lufthansa Air Cargo Terminal at New York's Kennedy Airport. None of this money or the valuables has been recovered. However, according to these authors, at least 13 people connected with the crime have been murdered or are missing and presumed dead.

The lack of convictions and recoveries belies the strong efforts put forward by numerous law enforcement agencies in connection with this case. This book is a fascinating case study in major case administration and the challenges that are presented by multi-jurisdictional efforts.

The robbery took place inside Kennedy Airport, a territory principally policed by the Port Authority of New York and New Jersey. Within minutes of discovering the robbery, the Port Authority police notified other interested law enforcement agencies. Agents and detectives from seven different Federal, State, and local law enforcement agencies responded to the crime scene. The working out of roles and cooperation between them as chronicled in this text is as fascinating as the crime itself. Additionally, the law enforcement investigators had to contend with the conflicting demands between the State and Federal prosecutors.

Ultimately, a task force was formed. Each agency would share the fruits of its investigation with the others to prevent duplication. However, there were to be two exceptions to the sharing of information. An agency would keep the names of its informants a secret from the other agencies and would follow up the initial leads received from its informants without telling the others.

As the investigation evolved over a number of years, the two principal organizations involved—at least according to the chronicle of these authors—were the New York City Police Department and the Federal Bureau of Investigation. The authors do both organizations justice in characterizing their respective strengths. In dealing with the various obstacles that the investigators found, whether they were their relations with the prosecutors or the misunderstandings that arose from their dealings with the media, the authors seem always to convey these developments from the point of view of the investigators.

The authors end on a very positive note, pointing out the improved working partnership that has grown up between the New York City Police Department and the FBI. They praise a number of joint task forces that have been formed, especially units working on bank robberies and terrorism. The authors cite reports from both organizations praising the task forces highly.

Ernest Volkman and John Cummings, the authors, have both worked for "Newsday"—the Long Island, NY, newspaper. Volkman is a former national correspondent for "Newsday" and is now a freelance writer. He has authored two previous books, "A Legacy of Hate"and "Warriors of the Night." Cummings is a staff reporter of "Newsday" and has written estensively on organized crime and related matters. This is his first book. Since the robbery in 1978, both of these men have authored numerous news accounts of the robbery as developments have unfolded.

—SA Thomas J. Baker, M.P.A.

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.

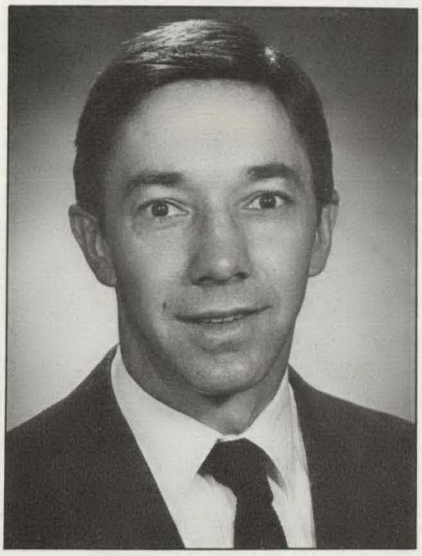
Part two will examine the factors in the *Scott* test, the interception of conversations involving unrelated criminal activity, and the consequences of a judicial finding of inadequate minimization. Finally, it will suggest procedures to best assure compliance with minimization requirements.

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.

VICAP ALERT

"UNABOM"

Description

NAME:	Unknown
RACE:	Caucasian
AGE:	Approx. 25–30 years old
HEIGHT:	5'10"
WEIGHT:	165 lbs
HAIR:	Reddish-blonde, possibly sun bleached
FACIAL HAIR:	Mustache
CLOTHING:	Last seen wearing a gray sweat shirt with hood, blue denim jeans, aviator-type sunglasses with gray lenses.

Background

Since 1978, an unknown bomber has been linked to 12 incidents across the United States, injuring 21 people and killing 1. The explosions have taken place in six States. Several of the devices were contained in packages that were delivered to university professors, an airline company executive, an airline manufacturing company, and two computer sales and service firms.

The most powerful device to date was placed at an employees' entrance of a computer rental store in Sacramento, CA, which resulted in the death of the owner who had attempted to move the concealed device. On four occasions, explosive devices were placed on campuses of major universities.

Modus Operandi

Targets

The targets appear to have common links—university departments, professors, and individuals involved with computers, airlines, and aircraft productions. So far, professors and students working in the fields of psychology, engineering, and computer science have been targeted.

Device Construction

The bombs have been disguised as a novel, a manuscript, a notebook, an electrical testing device, and parcels either mailed or addressed as if prepared for mailing. Among the items used to construct these devices have been wrapping paper, match heads, nails, screws, towels, fishing line, glue, string, switches (some handmade), barometer, metal, pipes, gun powder, and batteries.

Planning and construction of these devices take a considerable amount of time. Pieces of metal and electrical circuitry and switches appear to be homemade. Such work requires special skills in soldering and metal work. Letters delivered in conjunction with two of the bombs were intelligently written and neatly typed. Fictitious return addresses and correct delivery addresses have also been used.

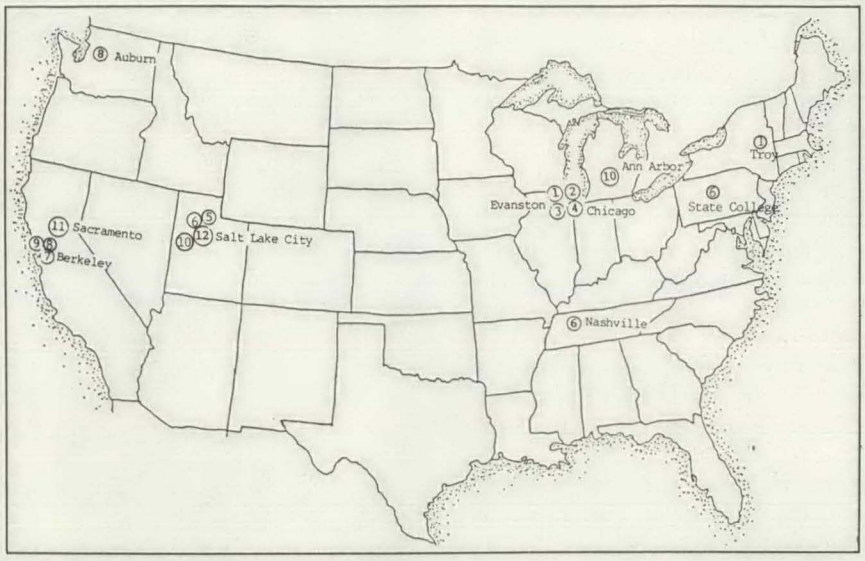
Bomber's Travels

During the period of 1978 through 1980, the bomber is believed to have operated from the Chicago, IL, area. In 1981, the bomber appeared in the Salt Lake City, UT, area. In 1982, the

VICAP

NCAVC

VIOLENT CRIMINAL APPREHENSION PROGRAM



bomber next appeared in the Berkeley, CA, area. Then for 3 years, the bomber remained inactive. In May 1985, he mailed a bomb from Oakland, CA, to an aircraft manufacturing firm in Washington State and placed a bomb in Berkeley, CA. Six months later, a package bomb was mailed from Salt Lake City, UT, to Ann Arbor, MI, and in December, a bomb was placed in Sacramento, CA. In early 1987, he placed a device in Salt Lake City, UT.

Alert to Chiefs and Sheriffs

A task force made up of the U.S. Postal Service, FBI, and Bureau of Alcohol, Tobacco and Firearms, in addition to various local law enforcement agencies, is working together to identify the bomber. Th FBI's National Center for the Analysis of Violent Crime has prepared and updated an extensive criminal personality profile of the individual responsible for these motiveless bombings.

The U.S. Postal Service has offered a reward of $50,000 for information leading to the arrest and conviction of the person(s) responsible for these bombings.

This information should be brought to the attention of all homicide officers, bomb technicians, and arson investigators. If solved or unsolved cases in your department resemble the MO's or fit the same time frame or locations (see map), contact the UNABOM LAW ENFORCEMENT TASK FORCE, Salt Lake City, UT, at (801) 359-1917. Collect calls will be accepted if reference is made to the "UNABOM" investigation.

UNABOM CASES

1) University of Illinois, Chicago, IL, 5/25/78 (a package found in the university parking lot with a return address of a Northwestern University professor in Evanston,IL, was sent to a professor at Rensselaer Polytechnic Institute in Troy, NY)
2) Northwestern University, Evanston, IL, 5/25/78
3) American Airlines Flight #444, Chicago, IL, 11/15/79 (en route to Washington, DC)
4) Lake Forest, IL, 6/10/80 (a United Airlines official received explosive device in mail)
5) University of Utah, Salt Lake City, UT, 10/3/81
6) Vanderbilt University, Nashville, TN, 4/25/82 (package mailed from Brigham Young University to a professor at Pennsylvania State University was forwarded to addressee's new location)
7) University of California, Berkeley, CA, 7/2/82
8) Boeing Company, Auburn, WA, 5/8/85 (package containing an explosive device mailed from Oakland, CA)
9) University of California, Berkeley, CA, 5/15/85
10) Ann Arbor, MI, 11/12/85 (package containing an explosive device mailed from Salt Lake City area to a professor)
11) Rentech Computer Rentals, Sacramento, CA, 12/11/85
12) CAMM's Inc., Salt Lake City, UT, 2/20/87 (a computer sales and service firm)

Unusual Pattern

The accidental whorl is the only pattern which may possess more than two deltas. Although three deltas appear in this impression, the pattern is given the classification of plain whorl, inner tracing, and is referenced to an accidental whorl, inner tracing. Due to the extreme edge positioning of the uppermost delta, it is probable that this delta will not appear in the majority of subsequent printings.

Change of Address

Not an order form

FBI
Law Enforcement Bulletin

Complete this form and return to:

Director
Federal Bureau of
Investigation
Washington, DC 20535

Name

Title

Address

City State Zip

U.S. Department of Justice
Federal Bureau of Investigation

Second Class Mail
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Washington, D.C. 20535

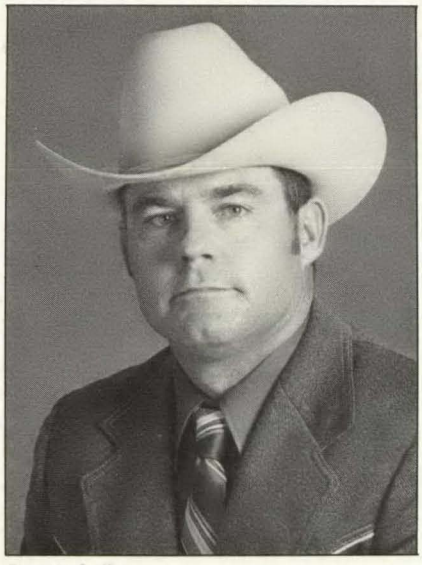
Official Business
Penalty for Private Use $300
Address Correction Requested

The Bulletin Notes

Texas Rangers Stanley Keith Guffey and Johnnie Earl Aycock came under hostile fire while working a joint FBI/Texas Department of Public Safety investigation of the kidnapping of a 2-year-old girl and her nanny in Horseshoe Bay, TX.

On January 22, 1987, Rangers Guffey and Aycock engaged the suspect in a shootout; Ranger Guffey fell mortally wounded, while Ranger Aycock fatally wounded the suspect. The 2-year-old girl was recovered unharmed, while the nanny had been murdered.

The Bulletin joins the Texas Rangers in saluting the bravery and heroism of Stanley Keith Guffey and Johnnie Earl Aycock in effecting the safe release of the 2-year-old girl. As Col. James B. Adams, director of the Texas Department of Public Safety, said, "He (Guffey) did what was right, but it cost him his life. It is an example of raw courage and heroism at its best."



Ranger Guffey

Ranger Aycock