SECURITY & PRIVACY
ISSUE BRIEF
No. 2 March 1981

PRIVACY AND INTELLIGENCE INFORMATION

SEARCH GROUP Inc.
The National Consortium for Justice Information and Statistics

SEARCH ISSUE BRIEFS

SEARCH, the National Consortium for Justice Information and Statistics, provides support to state and local agencies in all aspects of information system planning, design, implementation and management. SEARCH has particularly strong experience in the area of security and privacy of criminal justice information. This program is designed to support the successful implementation of security and privacy principles by clarifying national security and privacy issues and requirements. This is being accomplished through a grant from the Bureau of Justice Statistics, U.S. Department of Justice, which provides resources to guide and assist states in how to respond to federal and state privacy requirements.

In order to maximize the use of information contained in its data base, SEARCH plans to prepare quarterly issue briefs which will review and discuss topics of current interest to privacy specialists.

This paper constitutes *Issue Brief No. 2, Privacy and Intelligence Information.* It reviews major issues involved in the development of policy governing police intelligence information management and two operational policy models.

Project Staff

Gary R. Cooper, Deputy Director, SEARCH
Paul L. Woodard, Attorney, SEARCH

Project Monitor

Carol Kaplan, Director, Privacy and Security Staff
Bureau of Justice Statistics

Report of work performed under Grant Number 80-BJ-CX-0007, awarded to SEARCH Group, Inc., of Sacramento, California, by the Bureau of Justice Statistics, U.S. Department of Justice.

Points of view or opinions stated in this document do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SEARCH GROUP Inc.
The National Consortium for Justice Information and Statistics
925 SECRET RIVER DRIVE SACRAMENTO, CALIFORNIA 95831 (916) 392-2550
DR. ROBERT J. BRADLEY, Chairman STEVE E. KOLODNEY, Executive Director

INTRODUCTION

In the last decade, much progress has been made in the area of privacy of criminal history records. SEARCH surveys indicate that virtually every state has passed legislation which deals with some aspect of security of those records and the privacy rights of record subjects, and many states have established comprehensive controls dealing with the security and privacy of criminal history records.

However, few states have dealt specifically, let alone comprehensively, with the collection and use of intelligence information. This inactivity reflects a widespread reluctance to deal in specific statutory terms with the management and regulation of this highly sensitive information. Intelligence and investigative information generally has been excluded from the coverage of security and privacy legislation and Freedom of Information legislation. Instead, its management has been left to professional law enforcement officials who presumably are more familiar with investigative techniques and, therefore, the special needs of law enforcement agencies for investigative and intelligence data.

This approach is not likely to be acceptable to the public during the coming decade. The Watergate scandal and other publicized examples of abusive and intrusive information gathering practices by Federal intelligence agencies have led Congress to consider legislation to control the record practices of the Federal intelligence community. In addition, publicity surrounding covert police intelligence and surveillance activities against dissident groups has heightened public awareness of the potential threat to individual privacy associated with this kind of police activity. It seems likely that there will be increasing pressure in the states for regulations to balance legitimate law enforcement investigative and intelligence needs against the individual's interest in personal privacy, particularly in the sensitive areas of First Amendment rights, such as political, religious or social activities, associations and beliefs.

This paper summarizes some of the main issues involved in the formulation of policy concerning police intelligence information management, and discusses two recent documents that are relevant to these issues: (1) the revised Criminal Intelligence Systems Operating Policies issued by the Office of Justice Assistance, Research and Statistics (formerly the Law Enforcement Assistance Administration), and (2) an ordinance enacted by the City of Seattle establishing policies governing the Seattle Police Department's investigative and intelligence activities.

ISSUES

In brief, the main issues that must be addressed in a policy on intelligence information management are:

Collection

Questions that must be resolved in connection with collection concern the types of information that may be collected, the circumstances that permit the collection of information about a particular individual, and police techniques that may be used in collecting the data. Perhaps the most important questions are those concerning the collection of information about political, religious or other constitutionally

protected activities, since these are the activities where patterns of abuse have occurred most often. A related question is whether and for what purposes information may be collected about private sexual activities or tendencies. From the standpoint of privacy protection, rigid controls seem necessary to insure that police intelligence activities do not impinge on constitutionally protected rights. However, the controls must not be so rigid as to unduly hamper the police in dealing with criminal and terrorist activities which may attempt to hide behind the mantle of political, religious or community groups.

Another major issue involves the circumstances which may permit the collection of intelligence data about particular persons. Must the data collection have a nexus to criminal activity and how direct must the connection be? Must there be actual or suspected criminal acts already consummated or about to be consummated, or may information be collected on criminal activities that may or may not occur in the future? Must the individual about whom the information is collected be directly involved in the criminal activity or is it sufficient that the information be relevant to criminal activity by other persons, such as relatives or business or social associates?

The greatest privacy protection would be ensured by a policy requiring the individual to be directly involved in completed or imminent criminal activity. However, from the standpoint of effective police operations, such a strict policy might unduly hamper investigations of organized criminal groups which include large numbers of participants in complex and diverse criminal activities over a broad geographical area and which continue over a long period of time.

Other questions concern the use of particular police investigative techniques. For example, should there be limits on the use of paid informants or infiltrators? If infiltrators are used, should there be limits on the types of groups or organizations they may attempt to infiltrate and on the extent of their activities within these groups?

Security

For obvious reasons, intelligence and investigative information is extremely sensitive and deserves strict protection. Much of the information is unverified and may contain allegations or references to associations that can be extremely damaging to innocent persons. Most of the information will never be used or tested in court and many persons whose names are in intelligence files will never be arrested. Thus, it is critical to the privacy interests of these individuals that the security of intelligence information be protected against unauthorized access.

Most police agencies appreciate the sensitivity of intelligence data and evidence suggests that they guard it carefully. However, the advent of computers and other automated data handling equipment raises new issues about the security of intelligence data. May such data be safely stored in computers? What access controls are necessary to protect against unauthorized penetration? Should remote terminal access be permitted? May raw intelligence information be transmitted over computer links or must computerized systems be limited to name index-pointer systems?

Access

Since much intelligence data is unverified and perhaps unreliable, the issue of access is critical from the standpoint of personal privacy. Within a police agency, which officers may have access to intelligence data and for what purposes? May intelligence data be disseminated outside the agency that collected it and, if so, for what purposes and under what safeguards? May intelligence data be disseminated to non-law enforcement agencies or individuals, such as credit agencies, employers or private investigators?

Retention

Retention is one of the most controversial issues involved in the management of intelligence information. May intelligence data be stored indefinitely or must it be reviewed periodically and purged if no longer relevant or reliable? From the privacy protection viewpoint, periodic review and purge should be required, since much intelligence data is unverified and the passage of time makes the data even less valuable. However, from the viewpoint of the police, frequent review and revalidation is expensive and time consuming, often prohibitively so. Clearly, some periodic review and purge of intelligence files is desirable; the problem is to devise an approach that ensures some degree of relevancy and validity of retained information.

Sanctions

In order for any intelligence information management policy to be effective and to earn public confidence, there must be some means of enforcing adherence to the policy. Among the available methods are civil or criminal penalties against police personnel who violate the policy or civil causes of action for damages against the police department or the parent governmental entity. Questions arising under this approach include whether police personnel should be subject to penalties for good faith unintentional violations in the course of their duties and whether the governmental entity should be subject to liability for violations by employees acting outside the scope of their duties.

Other enforcement approaches include independent outside audit of police intelligence files to insure that violations have not occurred. While outside audit is unquestionably an effective enforcement approach, it raises serious issues concerning the integrity of intelligence files, the compromise of the identity of informants or infiltrators and the willingness of other police agencies to exchange information with an agency subject to outside audit, especially if the audit is by non-law enforcement personnel.

Finally, enforcement methods may include traditional personnel disciplinary sanctions, such as discharge, demotion, suspension or transfer.

THE OJARS POLICY GUIDELINES

The OJARS Policy Guidelines were issued by LEAA in 1978 and subsequently amended and reissued in 1980 by OJARS (the agency that resulted from a congressional reorganization of LEAA). The purpose of the guidelines is to ensure that all criminal intelligence systems supported under the Omnibus Crime Control and Safe Streets Act are operated in conformance with the privacy and constitutional rights of individuals. The guidelines apply to both discretionary grants by OJARS and to formula grants to the states which are subgranted to state and local governments.

While the guidelines are not intended to be comprehensive, they do set important limits on the collection and dissemination of intelligence information by covered law enforcement agencies and require the agencies to adopt more comprehensive policies in some areas.

Collection

The general rule set by the guidelines is that intelligence information about a particular individual may be collected and maintained only if it is "reasonably suspected" that the individual is involved in criminal activity and that the information

is relevant to that criminal activity. Thus, it would not be permissible to collect information about business associates, relatives or friends of persons suspected of criminal activity unless there were reason to suspect that these persons were themselves involved in the criminal activity. If the information relates to political, religious or social views, associations or activities, the rule is more stringent. Such information may be collected and maintained only if it "directly relates to an investigation of criminal activities and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct." Thus, there must be a criminal investigation in progress and there must be reasonable "grounds," rather than mere suspicion, that the subject of the information is involved in criminal activities directly related to the investigation.

Dissemination

The guidelines provide that intelligence data may be disseminated only to law enforcement officials, inside or outside of the agency collecting the information, "where there is a need to know/right to know the data in the performance of a law enforcement activity." The commentary to the original guidelines declined to offer a specific definition of "need to know/right to know," but stated that the term is generally understood in the law enforcement community to require that a criminal justice official requesting access to an intelligence file must establish that he is conducting an investigation pursuant to his official duties and that he needs the information in connection with the investigation. The guidelines require each covered agency to establish written standards defining need to know/right to know more specifically.

If intelligence data is disseminated outside the collecting agency, the recipient law enforcement officials must agree to follow procedures regarding data entry, maintenance, security and dissemination that are consistent with the guidelines.

Security

Agencies maintaining intelligence data are required to establish administrative, physical and technical safeguards to protect the data against damage or unauthorized access. These safeguards are to include an audit trail of disseminations outside of the agency.

Review

The guidelines require each covered agency to establish procedures to assure that all information which is retained has continuing relevance and importance. The procedures must provide for "periodic review" of data and destruction of any information which is "misleading, obsolete or otherwise unreliable." The original guidelines required agencies to review intelligence files at least every two years and to indicate the reason for retaining any information longer than two years. However, the amended 1980 guidelines deleted the two-year requirement on the grounds that it might be too burdensome and expensive for some agencies. The guidelines now permit periodic review on time schedules developed by individual agencies, but require that any information retained longer than two years must be reviewed and revalidated before it can be utilized or disseminated.

Automated Equipment

The guidelines provide that OJARS must approve system designs for the use of automated equipment for the storage and dissemination of intelligence information. They also prohibit direct remote terminal access to intelligence data stored in computers.

Sanctions

The guidelines do not provide sanctions, but require each agency to adopt sanctions to control unauthorized access, utilization and disclosure of intelligence information. However, accountability to OJARS is assured by a "funding guideline" which stipulates that intelligence systems will be funded only if control and supervision of information collection and dissemination will be retained by the head of a government agency or by an individual with general policymaking authority who has been expressly delegated control and supervision by the head of the agency. This supervising authority must certify in writing that he takes full responsibility and will be accountable for compliance with the guidelines.

THE SEATTLE POLICE INTELLIGENCE ORDINANCE

Seattle City Ordinance No. 108333, passed on July 2, 1979 and effective January 1, 1980, is perhaps the first legislative attempt to deal comprehensively with all aspects of police intelligence and investigative operations. As such, it should be of interest to other jurisdictions considering the adoption of legislation on this subject.

Because the ordinance deals with all aspects of police work, it is lengthy and complex. Although no attempt will be made in this issue brief to describe the ordinance in detail, its general approach will be described and a summary of its major provisions set out.

Approach

The approach of the ordinance is to deal with all aspects of the work of the Seattle Police Department related to criminal investigations and the collection and utilization of investigative and intelligence information. However, the main direction of the ordinance is to provide protections of individual privacy in areas where patterns of abuse historically have occurred. Thus, special protections are included for constitutionally protected activities, including political, religious and social activities and private sexual activities; and special attention is given to certain police techniques that have historically been overly intrusive in these areas, including the use of infiltrators, paid informants and the collection of information for the protection of visiting dignitaries.

The ordinance seeks to provide these protections through four mechanisms:

(1) Internal controls,
(2) Audit trails,
(3) An independent auditor,
(4) Civil liability.

Since the intent is to provide needed protections in specially sensitive areas, the ordinance carves out exceptions to the main provisions of the bill in areas of police work where patterns of abuse historically have not been experienced. Thus, a major exception exempts criminal investigations where criminal charges have been filed and the rules of discovery and other protections inherent in the criminal process are available for the protection of individuals. The bill also exempts confidential communications, materials open to public inspection, administrative records and "incidental references" to otherwise restricted information. This latter exemption excludes incidental references to sensitive information obtained during the course of normal police work, where the objective of the police activity was not to obtain the sensitive data. For example, passing references to sex or political beliefs or activities contained in incident

reports would not be covered by the ordinance.

The effect of the exclusions is to carve out the great majority of work essential to the daily operation of the police department, thus relieving the administrative burden on the department in areas where abuse is not likely and concentrating on the narrow scope of police techniques where abuse has most often occurred.

Restricted Information

"Restricted information" is defined by the ordinance as information about political, religious, social or community associations, activities, beliefs or opinions. The definition covers most activities protected by the constitution, including civil rights activities, community activities, and organizations or demonstrations for the furtherance of such activities or beliefs. This type of information is the main area of concern of the ordinance. The controls, prohibitions and procedures set out in the ordinance are designed primarily to prevent police abuses in the political/religious/social area.

Collection

Restricted information may be collected only upon the issuance of a written authorization obtained from a lieutenant or higher ranking officer. Authorizations may be granted only when there is a reasonable suspicion that the subject of the information is involved in criminal activity or is a victim or witness of criminal activity, and the information sought is relevant to the criminal activity or the arrest of the subject of the information. Authorizations are good for 90 days and may be renewed if grounds, such as new information, can be shown.

The authorization must be issued in writing and must set out detailed reasons for its issuance, including a description of the information to be sought and a statement of the facts and circumstances creating a reasonable suspicion of criminal involvement of the subject of the information. This authorization procedure is designed to create a detailed paper audit trail to facilitate control and examination of the collection of information in this sensitive area.

Dissemination

The ordinance provides that restricted information may not be transmitted to another criminal justice or governmental agency unless the agency has a need for the information that would be sufficient to obtain an authorization. Dissemination logs must be kept of each such dissemination.

Informants

The ordinance contains limits on the use of informants or infiltrators to gather restricted information about political, religious, social, civil rights or community organizations. The use of these police techniques to gather information in other areas, such as organized criminal groups, is not limited by the ordinance.

Where restricted information is to be gathered by an infiltrator, the Chief of the Seattle Police Department must approve an authorization stating the need for the use of the infiltrator, the matters about which information is to be collected and protective measures to insure minimum intrusion and to avoid unreasonable infringement of the rights of the organization to be infiltrated.

The ordinance also limits the use of paid informants to collect restricted information about political/religious groups. In such cases, the techniques of the informant and his participation in criminal activities are subject to specific limitations. If the informant is not paid or if the information to be collected is not restricted, the limitations do not apply.

Protection of Dignitaries

Since police agencies historically have used the pretense of dignitary protection to collect information on dissident political groups, the ordinance contains specific controls applicable to this technique. A separate authorization procedure is established and files including restricted information collected for this purpose are required to be kept separate from other investigative files. Strict time limits for collection and purging of the information are set, access logs are required to be kept and limits are set on the dissemination of such information outside of the Seattle Police Department.

Sexual Information

Sexual information is the second major category of information principally covered by the ordinance. It includes any information about a person's sexual practices or orientation. Private sexual information may be collected only when there is a specific connection to criminal activity involving sexual matters (such as rape, prostitution, pandering, procuring or pornography), and the information appears reasonably relevant to the investigation of such criminal activity or the arrest of the subject of the information. Such information may be disseminated outside of the Seattle Police Department only if the recipient criminal justice or governmental agency has a need for the information that would justify its collection under the ordinance.

No authorization is required for the collection of private sexual information in connection with the investigation of sex-related crimes, and no authorization may be issued to permit the collection of such information for any other purpose.

Auditing

Perhaps the most innovative procedure in the ordinance is the use of an independent outside auditor to assure compliance by the police department. The auditor is appointed by the Mayor and confirmed by the City Council for a three-year term. He is granted access to all Police Department files, except for certain internal personnel and confidential files and files relating to investigations of organized crime or government corruption that are certified by the Court Prosecuting Attorney for exemption from the auditor's review. This exception is included to permit the prosecuting attorney to withhold from the auditor certain especially sensitive case files, provided that the prosecuting attorney certifies that he will discharge the powers and responsibilities of the auditor with respect to such files to assure that the terms of the ordinance are met.

The auditor is required to review police department files at unscheduled intervals (but at least once every 180 days) to assure that the ordinance is satisfied. He is required to make summary reports of his findings to the Mayor and other city officials, including descriptions of any substantial violations of the ordinance discovered during the audit. He is also required to provide written notice to any person about whom restricted information has been collected if he has a reasonable belief that the information was collected in violation of the ordinance and would create civil liability under the ordinance.

Thus, the principal enforcement mechanism is independent audit and notice to individuals whose rights may have been violated, coupled with civil causes of action for damages.

Liability

The ordinance creates a civil cause of action against the City of Seattle for injuries proximately caused by willful violations of the ordinance by police department personnel in the scope and course of their duties. Liquidated damages are provided for in the amount of $500 for individuals and $1,000 for organizations.

The cause of action is against the city only and personal liability is expressly denied for any act or omission by a city employee made in good faith in the scope and course of official duties. However, city employees are subject to disciplinary sanctions, such as reprimand, suspension, transfer or discharge.

CONCLUSION

Although there has been little activity in recent years in the area of the regulation of investigative and intelligence information, this issue brief demonstrates that some attention has been given to the subject and at least one comprehensive legislative package has been produced. The Seattle ordinance is an excellent example of the kind of approach that might be taken to regulation of the full range of police investigative and intelligence activities. Although it remains to be seen how well some of the innovations will work and whether or not the ordinance will hamper legitimate police activities, the Seattle approach is courageous.

Whether other jurisdictions adopt this comprehensive approach or the more limited approach of the OJARS regulations, it seems clear that increased public attention recently focused on police intelligence activities will cause greatly increased legislative and regulatory activity in this important area of criminal justice information law and policy.

END