

**REPORT OF PANEL APPOINTED TO REVIEW DENVER POLICE DEPARTMENT
POLICIES FOR COLLECTION AND RETENTION OF CRIMINAL INTELLIGENCE
INFORMATION**

June 28, 2002

Roger Cisneros, Jean E. Dubofsky, William G. Meyer

Earlier this year, several individuals and organizations complained that the Denver Police Department ("DPD") was maintaining criminal intelligence files targeting protesters who had not engaged in criminal activity. Police surveillance and the existence of the files, according to the complainants, chill individual rights of free speech and association. Police advocates maintain that the information collected is necessary if the police are to protect public safety.

Mayor Wellington Webb appointed the three of us ("the panel") to review the Denver Police Department policies for the collection of criminal intelligence information, to compare Denver's policies with those of other law enforcement organizations and to recommend a policy that the Denver police should follow. We have reviewed policies from around the country, met with an expert on such policies, received public input at a hearing, met with DPD leadership and representatives of the police unions, and reviewed all of the group and individual files in the DPD's computerized criminal intelligence system. The following includes a summary of our impressions and our recommendations, both with respect to a policy that we suggest the city adopt and what should be done with the information presently in the computerized system.

Beginning in 1954, the criminal intelligence bureau of the Denver Police Department maintained a rolodex with an estimated 90,000 to 100,000 contacts for both

criminal intelligence and for routine public security work. In 2000, the bureau replaced the rolodex with a sophisticated criminal intelligence software system from a company named Orion. When the police department purchased the system, it did not purchase training or assistance in the use of the system because the department's appropriation for the project had been halved. The detectives who transferred the information from the rolodex to the computer system, which had a powerful cross-indexing capacity, did not know how to utilize the system's capacity, let alone how to create subfiles. Consequently, the detectives put the intelligence bureau information into the computer without differentiating between categories of information. Our review of all of the files on the system reveals that the stored information includes the names of persons with concealed weapons permits, persons who have received honorariums from the police department, Project Exile individuals who have convictions involving use of a weapon, persons who are the subject of reports from schools in Denver, persons who have threatened a visiting dignitary or who are classified as "mental cases," as well as groups engaged in protest activities.

From our review, it appears that most of the information entered into the computer program has not been accessed by anyone other than the person who entered the information and the panel members who reviewed it. Most police "intelligence" is kept in an officer's head or in separate files that are kept in the police department's gang unit, its narcotics bureau or with the federal ATF-FBI terrorism task force. There is no requirement that the gang unit, the narcotics bureau or the terrorism task force place the material in their files on the ORION system. Because the material

placed in the computer is not detailed enough to be of particular use to anyone, it is not surprising that it has not been distributed either inside or outside the department.

At about the same time as the intelligence bureau began using the Orion software, the captain in charge of the bureau prepared rules governing the entry of information into the ORION system and the distribution of any information from the system. Bureau personnel, however, were not trained in the proper entry of information into the computer under the rules and appear to have been unaware that the rules existed. In effect, there were no rules because they were not disseminated to the officers who were collecting and entering the data.

Because the prior rules had not been subject to public comment, our commission held a public hearing on May 14, 2002, to address more comprehensive proposed rules governing the collection of police intelligence information. The proposed rules are based on federal regulations and allow the police to retain information about a group that is reasonably suspected of being involved in a definable criminal activity or enterprise. If the group is reasonably suspected of engaging in criminal activity, the intelligence file may include a list of the group's members. The proposed policy also allows the police to retain in criminal intelligence files information about individuals for whom there is a reasonable suspicion that the individuals are engaged in criminal conduct. The retained information must be in writing and must be specific, containing articulable facts to give a trained law enforcement officer a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. The information must reflect its source and the date that

it was received; the information must also reflect the reliability of the source, the identity of the person who determined to put the information into the computer, and the identity of the supervisor who approved entry of the information. Such information may be shared with other law enforcement agencies if those agencies have similar policies that set a boundary between legitimate law enforcement information and information that may impinge upon individuals' First Amendment rights.

In addition, the files may contain noncriminal identifying information about a group or an individual for whom there is a reasonable suspicion of criminal conduct. The noncriminal identifying information may include the names of associates of the criminal suspect, places that the suspect frequents, or groups to which the suspect belongs. Noncriminal identifying information must clearly specify that there is no suspicion that the identified person or group has engaged in criminal conduct. Rather, the information is retained to further criminal investigations that target an individual suspected of criminal activity. Because noncriminal identifying information may be linked in the computer, two individuals who each are suspected of criminal activity may be traced by finding that they both associate with the same persons or in the same place.

We reviewed all of the group and individual information presently retained in the DPD intelligence bureau file in light of the proposed rules. Although common sense tells us that some of the 208 groups listed have a criminal purpose, the information that we reviewed did not adequately justify the retention of the information about any of the groups in the department's criminal intelligence files. For some of the 3,277 individuals,

the information reflected an arrest record (information that can be obtained from other computerized systems), but not that there was a reasonable suspicion that the individual currently was engaging in criminal conduct.

Therefore, we recommend that all of the information about the 208 groups and 3,277 individuals be removed from the criminal intelligence file. For those groups for which there is a reasonable suspicion of current criminal activity, pertinent information -- with the addition of more detail -- may be reentered with sufficient articulable facts that justify the reasonable suspicion determination. Similarly, for those individuals for whom there is a reasonable suspicion of current criminal activity, the information may be reentered. All of the entities within the Denver Police Department which engage in intelligence work -- concerning gangs, narcotics, organized crime and terrorists, for example -- should forward the information that they have to the intelligence bureau. A detective, under the guidance of a supervisory officer, should review all of the intelligence information to see that it complies with the reasonable suspicion requirement before it is entered into the computer. Information contained in the criminal intelligence files should be regularly reviewed in order to assure that the information is current and useful and meets the requirement of the rule. Accurate, current information -- appropriately filed -- should make police work more effective.


The names of persons and organizations for which there is no reasonable suspicion of criminal activity should not be reentered in the criminal intelligence files. The names of persons with concealed weapons permits or the names of persons who are a group contact for a parade permit, for example, may be kept on the same

computer system in files that are separate from (and clearly identified as such) criminal intelligence files.

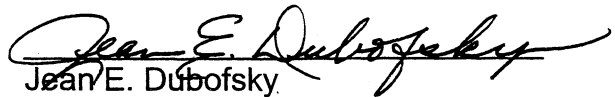
For the first year after this policy is in effect, on a quarterly basis, an individual with no connection to DPD, who is familiar with proper intelligence gathering, retention and dissemination processes, shall do an audit to determine if information has been collected, stored and disseminated in accordance with the reasonable suspicion requirement in the rules. The review shall be done on a semi-annual basis for the next two years, and annually thereafter.

Anyone who wishes to know if he/she -- or the group to which he/she belongs -- was the subject of an intelligence bureau investigation should call the police department, intelligence bureau at 720-913-6018 within 60 days to learn if either the individual's or the group's names were listed. If the names were listed, then the individual identified (or an officer, attorney for, or member of the group as reflected by the DPD files) may see the file with the names of others redacted to protect their privacy interests. The stored files should not be released to the general public in order to protect the privacy and associational rights of the individuals named. At the end of 60 days, the files will be destroyed. If an individual or a group remains the subject of reasonable suspicion of criminal conduct, then the names may be reentered in the criminal intelligence data base, along with details that form the basis of reasonable suspicion. As is true for all police investigation files, those files that are recreated will not be open for inspection by anyone without a legitimate police need to know.

We see no reason to punish anyone in the police department for retaining improper information in the intelligence bureau's criminal intelligence computer data base. There is no indication that any of the information was retained intentionally to harm someone or to inhibit the exercise of First Amendment-protected activities, and there is no indication that anyone has been harmed by the police department's collection of such information. The inclusion of all sorts of information in criminal intelligence files was a result of transferring information from a rolodex to a sophisticated computer program. The lack of assistance and training from the software company led to most of the problems. The proposed rule mandates frequent and on-going training for intelligence bureau detectives and supervisors on the proper collection, storage and dissemination of intelligence information. Training and independent oversight with respect to use of the computer software and to the practical application of suggested standards should restrict the collection of intelligence information that cannot be justified.



Roger Cisneros



Jean E. Dubofsky



William G. Meyer