Security and Privacy Considerations Relating to Organized Crime Intelligence Files

Edward J. DeFranco, Ph.D
Assistant Deputy Director
New York State Identification and Intelligence System (NYSIIS)

Presented at the

Fourth Organized Crime Law Enforcement
Training Conference
United States Department of Justice
Law Enforcement Assistance Administration

Center of Adult Education, University of Maryland
College Park, Maryland

January 4-8, 1971

Contemporary American life presents criminal justice with a monumental challenge. On the one hand, crime rates and losses of life and property through criminal actions are reaching crisis proportions - the risk of becoming a victim of crime increased by 100% between 1960 and 1969. In those nine years, the column of crime rose 48 percent while the population of the United States rose only 13 percent. Thus crime exceeded population growth 11.5 to 1.

Not only are the numbers of crimes being committed rising but the criminals are increasingly utilizing advanced techniques in transportation and communication, making traditional modes of law enforcement, investigation and detection more difficult. There is strong speculation, for example, that organized crime is now utilizing data processing in its activities to increase the efficiency of its operations.

The major responsibility of law enforcement is to prevent criminal conduct from so undermining the citizen's right to personal security, free movement and use of property - to, in a word, prevent social choas from overcoming democratic society - puts on it sharp pressure to modernize and take advantage of new scientific and technological developments to permit society to deal effectively with the crime problem and thus preserve our constitutionally granted liberties and freedoms.

Encouragement to do so has come from a variety of sources including the President's Commission of Law Enforcement and the Administration of Justice and the U. S. Supreme Court as well in several landmark decisions.

Thus, our rising crime rate, the continued growth and sophistication of organized crime, and the need to strengthen lawful law enforcement in response to both press for the development and utilization of new scientific techniques for law enforcement agencies.

We must balance this requirement, however, with the constitutional and traditional American guarantees of civil liberties and civil rights. There have been several scientific measures which, although at first the subject of strong objection, have stood the test of time and have become acceptable as meeting the test of consistency with constitutional rights. Some examples include fingerprinting, chemical analysis and radar.

The New York State Identification and Intelligence System (NYSIIS) has strived consistently to maintain this balance between need and rational response in all of its programs. As a national leader in the application of new scientific technology to the problems of criminal justice it has often found itself in a position of setting national and, indeed, international standards.

The task has not been an easy one. Growing from an initial staff of five people in 1965, NYSIIS is now a large, well established system employing in excess of 700 people with a budget of 7.5 Million. The major responsibility of NYSIIS is to facilitate information sharing between and among criminal justice agencies through the employment of modern technology. The ultimate objective of NYSIIS is to assist in the improvement of criminal justice and thereby reduce crime by: (1) developing and establishing a computer-based information sharing system; (2) implementing improved operational techniques - such as an automatic license plate scanning (ALPS) system, fingerprint processing and recognition systems, a fraudulent check system and an organized crime intelligence system; (3) developing a broad program of research in the area of criminal justice.

I would like to discuss with you this morning the progress NYSIIS* has made thus far in building civil liberties concepts and safeguards and to have you consider the applications these may have in your own areas of interest. Incidentially, these suggestions apply whether the system you contemplate is to be manual or computerized.

NYSIIS began with a positive commitment to the protection and advancement of civil liberties within its system. It actively sought and received comments and suggestions from a variety of sources as to the steps that should be taken to assure the building of an acceptable system. A dialogue was established with civil libertarian groups, legal groups, prominent private citizens and participants in the system to achieve the best thinking and research on the problem. For example, an Advisory Committee of user agencies was formed to recommend the kinds of data that ought to be included as well as excluded from the system.

Initially a security consultant and subsequently a privacy consultant were employed to analyze these respective areas and privide appropriate recommendations. The privacy consultant - Professor Alan F. Westin - conducted an analysis of the NYSIIS system and made extensive recommendations. Subsequently, in his monumental work, "Privacy and Freedom," often quoted by the Supreme Court in right-to-privacy cases, Professor Westin wrote: "At the state level, the New York State Identification and Intelligence System, a computerized base of information about criminal records,

---

*Note: NYSIIS is an identification and intelligence system, reflecting the significant difference in the source of entries into these two separate and distinct functions, many of the security and privacy measures differ for each. For example, although a subject has access to his identification record to correct any errors, this is not true of his intelligence file. References to the intelligence system are noted accordingly; references to both systems are referred to as the "total system" or "NYSIIS."

has pursued an exemplary policy of discussing such issues with bar associations, civil liberties groups, and academic experts and building excellent standards into its data-acquisition and dissemination procedures."

Basic to the NYSIIS Organized Crime Intelligence program are the following three distinct aspects:

1. Whether to acquire certain personal or sensitive information at all, either as offered by a participating agency or generated by NYSIIS itself.

2. Whether to collate information bit A with information bit B to create a new piece of information A-B by the linkage and relationship that NYSIIS has brought into being by collation.

3. Whether to release information properly acquired or collated to some or all NYSIIS participants.

Obviously, the process of decision by NYSIIS in the area of privacy is governed by a careful weighing of the social interests in protecting individual and group privacy against the need of government to have and use information to improve its performance of the criminal justice function. The criteria here are social policy judgments.

On the other hand, NYSIIS decisions in the area of security are affected by cost and efficiency factors--how much money can be spent on security installations, personnel, and procedures, and how much do security procedures impair the speed and effectiveness with which NYSIIS can perform its required tasks. Here, the criteria are managerial considerations.

In this sense, NYSIIS can be thought of as protecting privacy through two distinct policies: by respecting and enforcing the confidentiality that existing statutes or common law attach to certain classes of information, and by refusing to acquire, collate, or release personal or sensitive information that could be legally used because of NYSIIS's own determination that such a policy of exclusion is in the best social interest.

Sharing confidential criminal records between separate criminal justice governmental agencies has been going on for decades. It is nothing new. In addition to sharing required by statute, as submission of fingerprints for major crimes to a central repository, interchange of information scans the whole spectrum of the criminal justice process including interchange of information between federal, state and local agencies. Indeed, the practice will soon become accelerated under the pressure of vast new federal programs. All of the sharing is for the benefit of society and a program of criminal justice simply cannot exist without it.

Fortunately, while there is a high degree of error risk inherent in manual interchange, the computer can more than adequately correct this. We do recognize, of course, that the computer, by introducing orders-of-magnitude change into the situation is bringing about significant qualitative changes. These too can be adequately provided for. There is one aspect of this change that is positive: the computer is focusing light on a situation of long standing, where the facts may undoubtedly be much worse than realized by most. Through a system of rules, safeguards, penalties and remedies, computer files can be protected far better than manual systems and one large installation under the most stringent of rules may be better protected than many installations with lesser controls.

The potential threat of an information system and the potential benefits depend more on the organization using the system than anything inherent in the computer itself. Recognizing this, the legislature in creating NYSIIS designed it as a service agency only without powers, duties or facilities to arrest, prosecute, confine or supervise.

This provision assures the functioning of NYSIIS in an atmosphere of collecting, correlating and disseminating intelligence data in a purely objective fashion without the risk of jeopardizing privacy by the requirement to make cases and to engage in competition with other operating angecies.

Following are some of the specific measures NYSIIS has taken to protect the privacy of individuals about whom organized crime data is collected:

1. Users of the system are limited and specified by statute

2. Classes of information included in the system are specified by statute.

3. Unauthorized disclosure by an employee is forbidden by statute.

4. Employees and system participants are closely disciplined.

5. An information classification system, reflecting the data content of information, has been adopted with appropriate security measures applied depending upon level of sensitivity.

6. Extensive personnel training and monitoring systems have been adopted including an extensive security check prior to employment.

7. A NYSIIS Organized Crime Security Advisory Committee consisting of representative local and state criminal justice agencies contributing to the intelligence module has been formed. It meets periodically to offer consultation to the Director and his staff in developing policies and procedures.

8. A NYSIIS Security Review Board has been created to monitor all security measures adopted and to recommend changes and/or additions to the Director.

9. Extensive Technical and Systems Safeguards have been incorporated into the NYSIIS system including computer programming controls, information receipt functions, access controls, monitoring and auditing capabilities, storage and transmission security.

10. A basic concept is control by the donor who determines what information is submitted and what agencies are to be given access.

11. Processing of data is carefully planned and executed (see Exhibit 1).

12. Security and privacy response flow is carefully planned and executed (see Exhibit 2).

These are just some of the security and privacy measures NYSIIS has adopted in its efforts to develop an effective as well as a civil liberties minded intelligence system.*

Developments are fast moving and the NYSIIS system, as a whole, as well as others like it are proving to be indispensable in a civil liberties environment. For example, the potential impact of NYSIIS has been highlighted by recent United States Supreme Court decisions emphasizing the requirement for prompt arraignment of arrestees and placing constraints upon traditional police practices relating to search and seizure and confessions. The Supreme Court in Miranda v. Arizona, 384, U.S. 436, specifically called for more careful police investigation and expanded utilization of science and technology. NYSIIS has supported more rapid arraignment by the development of a facsimile transmission network to expedite the forwarding of fingerprints for the arresting agencies throughout the state to NYSIIS, and the return of information concerning prior criminal records or absence thereof. Bail decisions are more discriminatingly made when based on broad knowledge of a suspect and some high degree of certainty as to whether he is wanted

*The privacy benefits to be derived from this process have already been dramatically demonstrated. There has been a significant reduction in intelligence errors; data has been made more complete; and long term improvements in operational methods and security measures of state and local intelligence files will result.

elsewhere. Likewise, more effective criminal investigation is made possible through the application of new operational techniques developed by NYSIIS research. Our criminalistic efforts will assist in providing scientifically developed "real" evidence to support the criminal justice process.

The impact of the NYSIIS system, therefore, is to substantially improve the protection of civil liberties and civil rights by providing critical information where and when it is needed. It is important to recognize that NYSIIS is not collecting any new data but merely providing better utilization of data which has been collected for decades. The computer, by introducing orders of magnitude into the economics of the situation, is bringing about qualitative changes. It will strengthen the civil liberties of the offender by providing criminal justice decision makers with better, more reliable, and increasingly accurate information and, through multi-variable research methods, will broaden the civil liberties of the average citizen by providing trend analyses and other crime analytical techniques to strengthen the criminal justice system in combating crime.

As I have noted, a basic premise of the NYSIIS system is to achieve a balance of interest between the need of government to obtain information about offenders and its responsibility under the Constitution to provide for a "Tranquil Society." The basic question then becomes: Is the information collected, stored and disseminated <u>reasonably</u> related to advancing the general welfare, health or safety of society? A unified information system has definite economic, efficiency, and spatial advantages but these are not the primary considerations--qualitative inputs of data take precedence. The maintenance of a free society is more important than any argument for efficiency. Fundamental to the NYSIIS approach has been the humanistic question in determining inclusion of types of data.

In criminal justice, the problem becomes especially acute since the police role involves surveillance and detection which are direct assaults on privacy. But their motives are to protect the rights of all citizens to walk the streets safely and not to deliberately invade the private actions of the average citizen. It's the proper functioning of this activity which is generally accepted by the society and the courts as not constituting an unreasonable act of privacy invasion. Criminal acts require secrecy in planning and execution; protection of society often necessitates invasion of the privacy of criminals. The test is <u>reasonableness</u>.

This criterion is the very foundation of the NYSIIS approach and is applied to every step in the criminal justice process in order to arrive at decisions as to whether to collect, store, and disseminate items of information. For example, it is reasonable to extend the amount of data collected about an individual who has been convicted of a crime because his rights of privacy have been greatly diminished. Also, as he progresses out of the system and begins to repay his debt to society, he begins to regain his right to privacy and information collected, stored and disseminated in adjusted accordingly.

It is significant to note that confidential data concerning criminal activity has long been collected on a regular basis by criminal justice agencies, so its existence in the hands of the government is not an issue. There is widespread recognition for the need to improve the criminal justice system to make it more effective in dealing with the ever increasing crime rate. There is also a strong requirement for research in the problems of crime and crime control, described as the "greatest need" by the President's Commission on Law Enforcement and Administration of Justice. The computer will provide for both requirements.

While recognizing the need to protect privacy, it is obvious that an unreasonable obsession with confidentiality can defeat the very purpose of establishing a criminal justice computer facility.

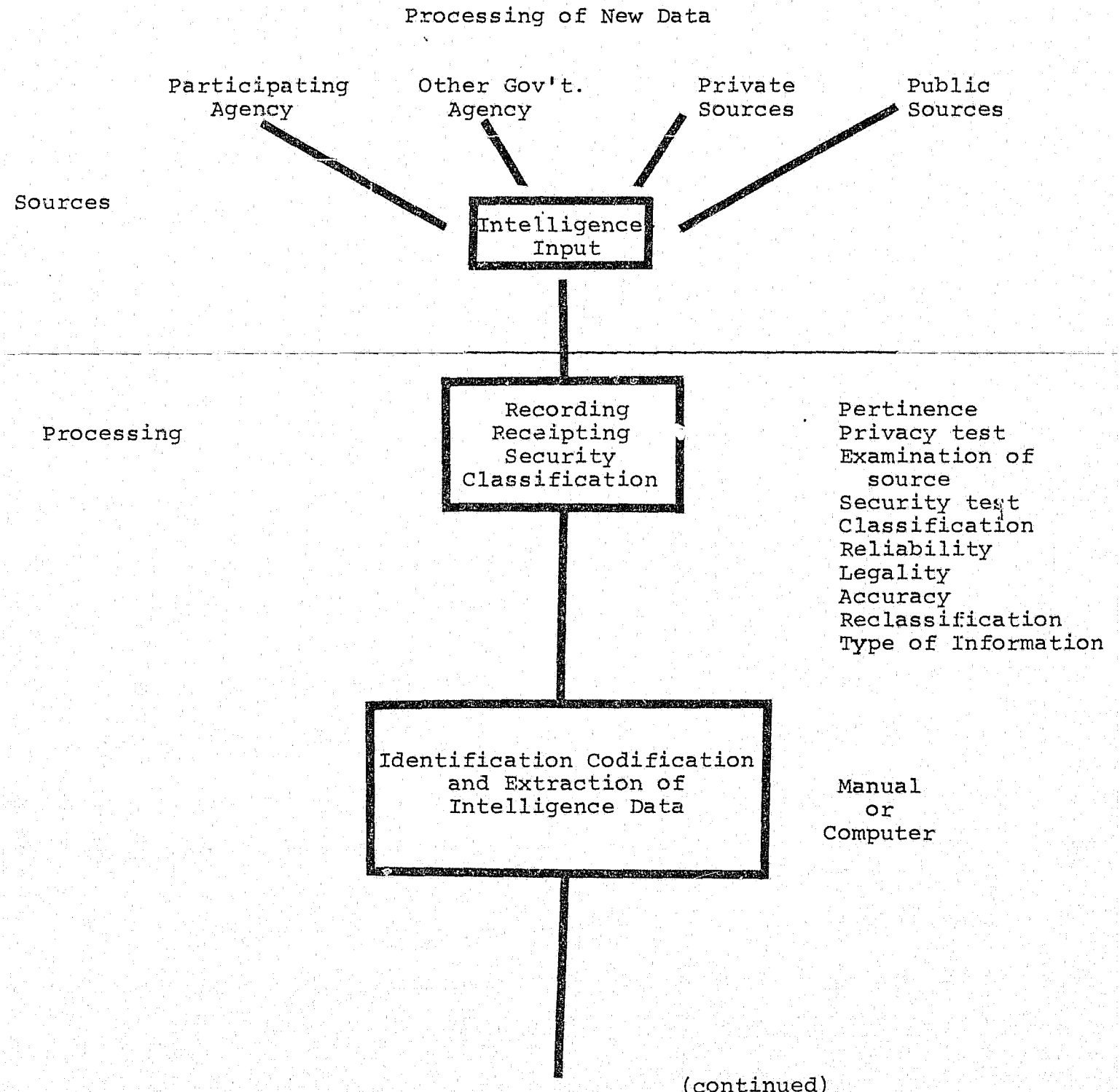
The core of the problem is the lack of clear law and guidance in the area of privacy which has now been made more complicated by the computer era. There is no clear cut definition of personal information as a precious commodity in American law as there exists in the law of property. Also lacking is a general system for dealing with the flow of information which government agencies control (aside from income tax and census data). Finally, there is an absence in American law of institutional procedures to protect against improper collection of information, storage of inadequate or false data, and intra-governmental use of such information for reaching decisions about individuals outside or inside the organization.

The NYSIIS system has had to develop within this atmosphere and so in many ways served as a prototype for other state systems now in the planning stages. The measures described herein are not, of course, the final word. NYSIIS management conducts continuous evaluation in an effort to provide the most secure and privacy protected system. It is important to realize that storing data in computers rather than on pieces of paper in metal filing cabinets permits far more technological protection. Bits of information in a computer memory bank can be locked to permit entry by only one or several individuals with the appropriate "password." Also, inquiries of manual systems are seldom recorded; a computer can be programmed to record the date, time and nature of an inquiry together with the name or identifier of inquiring persons thus leaving an "audit trail" for management to use as a control device.

In conclusion, I have offered some basic philosophy and procedural techniques which I consider a matter of prime importance for any evolving intelligence system to consider.

These are not by any means all the answers. They represent a beginning and I would hope that through the mechanism of meetings such as this and others to follow that the intelligence community will begin to give questions of security and privacy the attention they deserve.

EXHIBIT 1



(continued)

(Exhibit 1 continued)

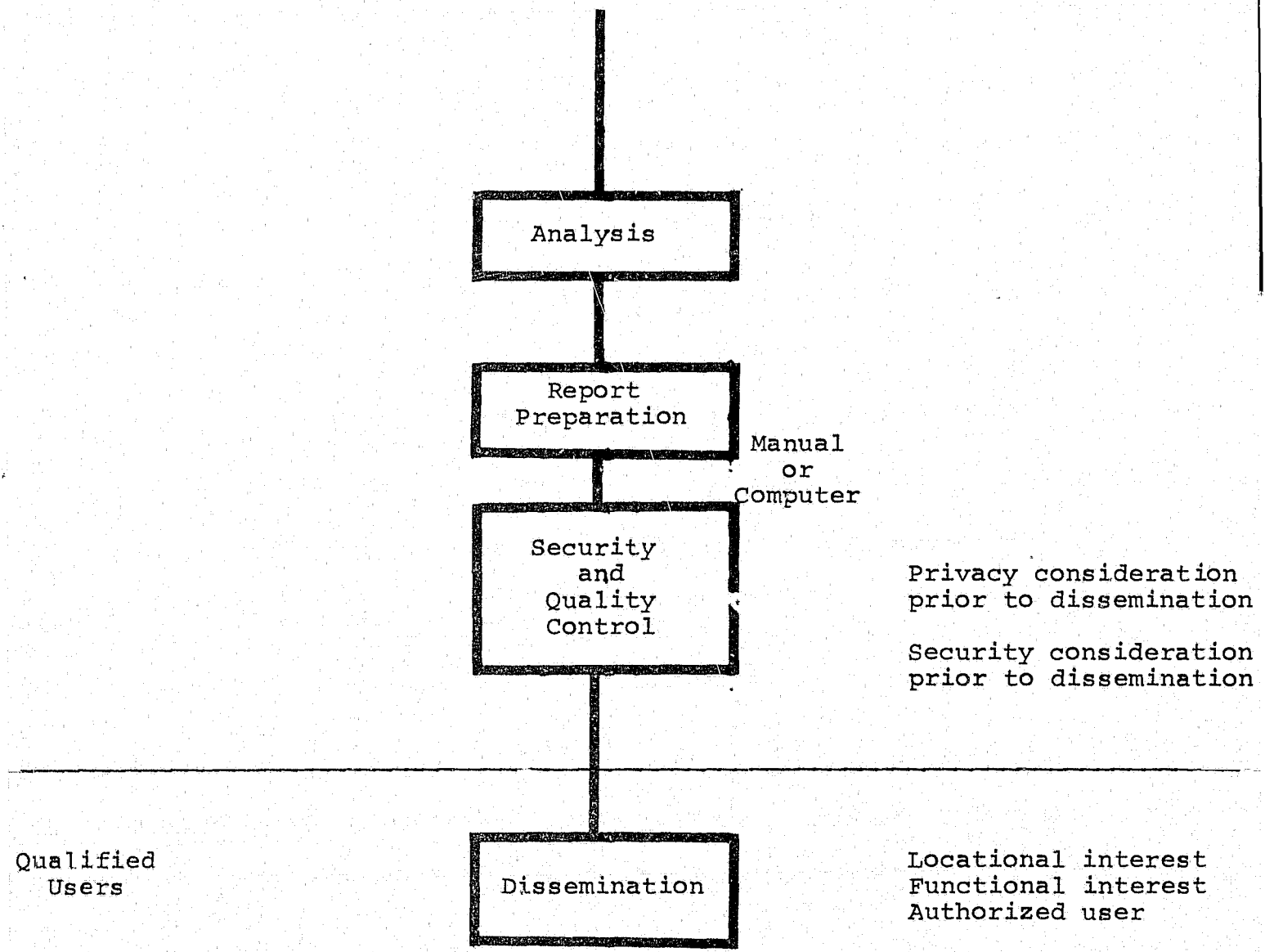
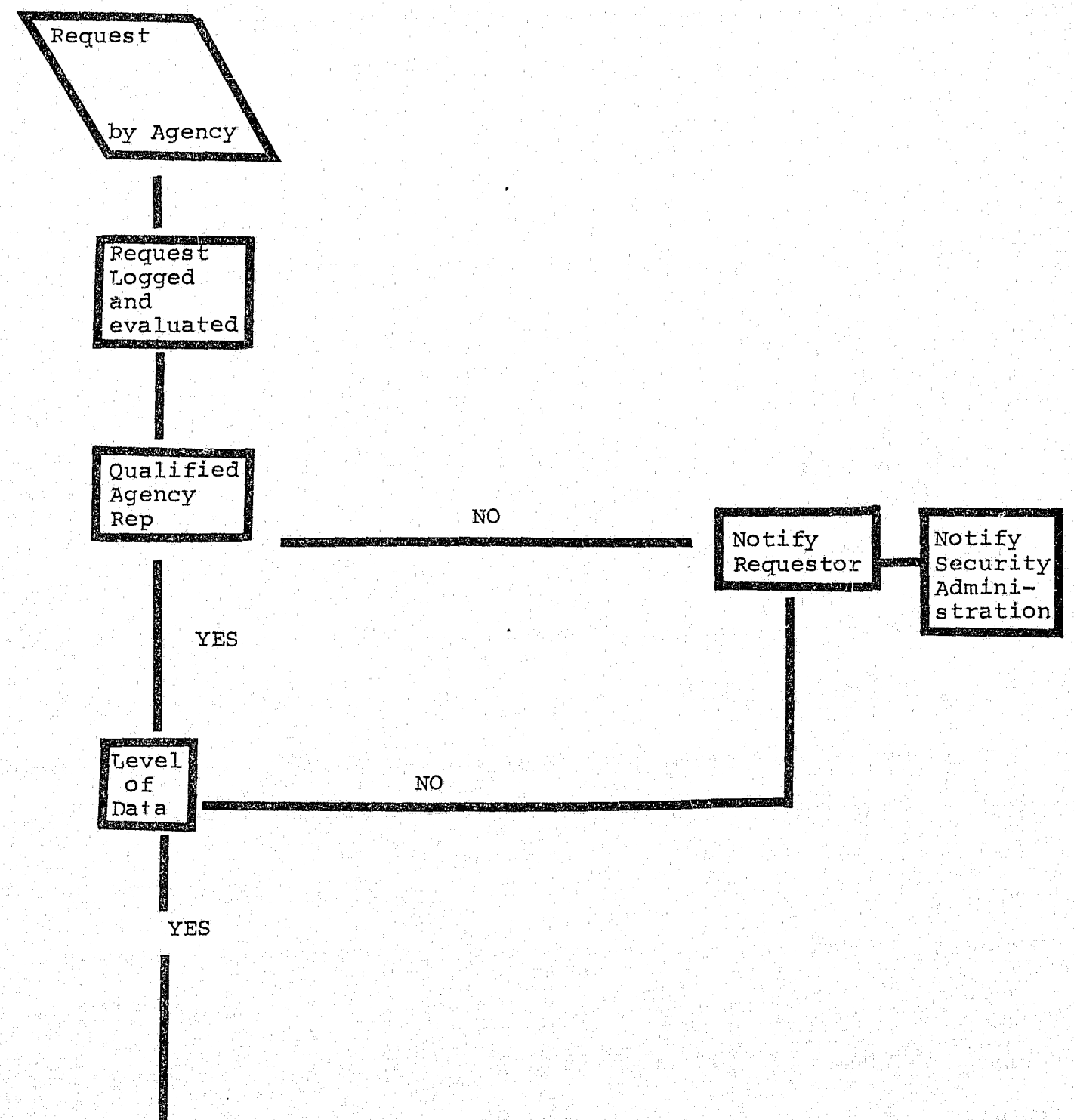


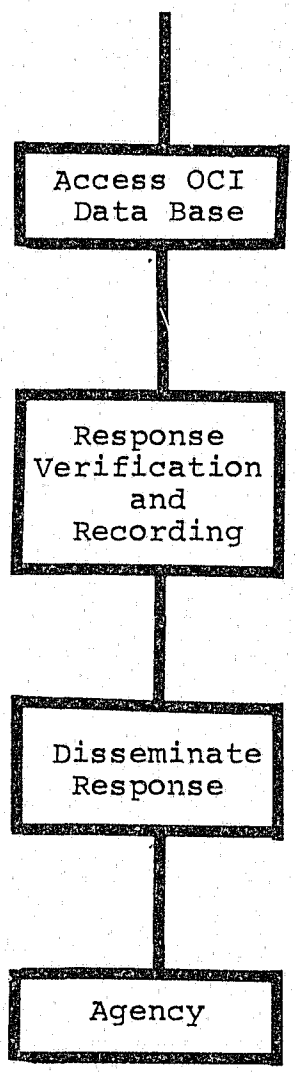
EXHIBIT 2

Security and Privacy Inquiry and Response Flow



(continued)

(Exhibit 2 continued)



NOTES:

I PERTINENCE

1. Is it pertinent with regards to O.C.?
2. Is it needed immediately, if so, by whom?
3. Of possible present or future value, if so by whom?
4. Is it relevant to the point of interest?

II PRIVACY TEST

1 Are there violations of privacy?
2. Does the data unnecessarily prejudice individual? (Political in nature?, Dealing with beliefs or sexual proclivities and activities?)

III EXAMINATION OF SOURCE

1. Is information received from a public unclassified source? (Newspapers, etc.)
2. Is the information received from State, Federal or private agency (source) subject to classification?

IV SECURITY TEST

1. Will disclosure of document damage reputation of NYSIIS or contributing agency?
2. Will disclosure damage reputation or cause embarrassment to any agency?
3. Will it disclose source or hinder intelligence effort?
4. Will disclosure hinder State law enforcement agencies in their prosecutions?
5. Will disclosure of document aid organized crime?

6. Can this information be misused or misinterpreted to hinder or weaken State agencies in their ability to combat O.C.?

V CLASSIFICATION

1. How was information classified by originator of message?

2. Should information be up or down-graded?

VI RELIABILITY

1. Under the condition existing at a time could this information have been obtained?

2. How reliable was source in the past?

3. Is the source dependable?

4. Is the source trustworthy?

VII LEGALITY

1. Was data legally obtained?

2. Would inclusion of data into system violate any ethical code or legal statue?

VIII ACCURACY

1. Is it possible for reported fact to have taken place?

2. Is report consistent within itself?

3. Is report confirmed or corroborated by information from other sources or agencies?

4. Does report agree with other available information, if not which report is more likely to be true?

IX RECLASSIFICATION

1. How does the classification of the new information compare with the classification of same information on hand?

2. Does information received concern a principal figure in organized crime?

3. Does information received concern a known criminal associate in O.C.?

4. Does information received concern a newly identified person reported to be an associate in O.C.?

X DETERMINING TYPE OF INFORMATION

1. Is information of tactical or strategic value?

XI PERTINENCE (NEED TO KNOW)

1. Could it possibly be of interest to agency on location basis?

2. Could it be of interest on a functional basis?

3 Is agency in possession of original information (message)?

4. Is agency authorized to receive data?

XII PRIVACY CONSIDERATIONS PRIOR TO DISSEMINATION OF INTELLIGENCE

1. Will privacy be violated by disclosure of intelligence?

2 Will it harm individual needlessly?

3. What is to be gained by dissemination of this intelligence?

XIII SECURITY CONSIDERATIONS PRIOR TO DISSEMINATION

1 Is it OK to disclose this intelligence as far as contributing agency is concerned?

2 What are the risks of methods of transmittal?

3 What would be the most secure way of transmittal-considering urgency?

END