

**MANAGING AND USING CRITICAL INFORMATION**  
**IN THE**  
**LAW ENFORCEMENT ENVIRONMENT**

Steven D. Ashley

The object of this paper is to examine current management of critical information by American law enforcement agencies, and to consider how legal requirements and existing technology have shaped current practices. Critical information in this context is defined as operational information that results from high-risk law enforcement practices such as use of force, arrest of individuals, or motor vehicle pursuit.

## **PAST PROBLEMS: CRITICAL INFORMATION IN THE HISTORICAL CONTEXT**

American law enforcement agencies have historically failed in the collection of data related to high-risk activity. Even in departments where data collection has been attempted, compilation of that data has been rare and generally disorganized. Two primary reasons are frequently given for this failure; fear of aiding plaintiff's attorneys by providing a ready-made collection of data, and the difficulty of gathering meaningful data from officers within the context of their daily activities.

The first of these reasons is largely based upon a fundamental misunderstanding of the legal system, accompanied by what could uncharitably be called a "herd mentality". Many department executives believe that to collect information in one place is to make life easier for the plaintiff's bar. Similarly, to allow information to remain scattered about in individual files is to make life more difficult for attorneys, thereby reducing the likelihood that plaintiffs will be able to access the information. This position is difficult to defend in the current legal climate.

Secondly, collection of critical data has been hampered by the systems in everyday use. In the past, many departments emphasized actual patrol time, relegating "paperwork" to a secondary role. Institutional philosophies ranged from, "...it's not important, as long as the job gets done..." to, "...we don't have time for that, we have to do real police work..."

These philosophies ignore the reality of law enforcement, that the only lasting record of what is accomplished is the paperwork. Without the benefit of accurate documentation, subsequent review by the legal system is often difficult and inaccurate, giving rise to a, "he said, she said" approach to defense of police actions.

Administratively, managerial decision-making has been severely hampered by a lack of adequate information regarding the intricacies of "street" activities and their logical impact on administrative functions such as policy development and training. The danger here is that police managers and supervisors, removed from the daily swirl of routine law enforcement activity, may base decisions not on the reality of law enforcement as it currently exists, but on their memories of their time on the "street".

### **Early Systems for Collection and Use**

The earliest "systems" for tracking critical information involved mere verbal reporting up and down the chain of command. While this method worked in the short term, particularly in very small agencies, much information was lost or not collected at all. Additionally, little clear institutional memory existed. In essence, this method

constituted the ubiquitous “war stories”. The potential for selective memory and inaccuracies was great, while analysis of data across incidents was almost impossible.

Law enforcement quickly learned that it was necessary to write things down, giving rise to various report writing systems. In fact, some authors suggest that, “...virtually every improvement in law enforcement has resulted from the study of written records.” (Patterson and Smith, p.3). Still today, many small, rural departments use a simple report writing system that constitutes little more than file memoranda. These are simple narrative reports, with little, if any, data collection capability.

Of course, once officers began submitting reports, some sort of quality control system was needed. Generally, this involved supervisory review. However, in many departments, the primary emphasis of the review process was grammar and spelling, accuracy of facts, and completeness of detail for prosecutorial purposes. Little attention was paid to minute details regarding the techniques, tactics and tools used to control the suspect. The focus was on the presentability of the report, and the complete reporting of the elements of the offense. All too often, this is still the norm.

## **THE CURRENT LEGAL ENVIRONMENT**

There has been much discussion in the legal arena regarding the need for law enforcement to properly direct and supervise the involvement of officers in high-risk activities. In fact, the United States Supreme Court has made it clear that policymakers have an obligation to review the daily activities of governmental employees in order to assure that those activities likely to result in potential constitutional violations are addressed with training programs (*City of Canton, Ohio v. Geraldine Harris, 489 U.S. 378 (1989)*). To not do so, according to the Court, is to be deliberately indifferent (and therefore unreasonable) to the potential constitutional violation. This is particularly true as regards the use of force to make an arrest.

Most cases filed against law enforcement officers and agencies for inappropriate or excessive use of force, and for illegal arrests, are filed in federal court. This is due to the constitutional limitations on such activity, as well as the potential for plaintiff’s attorneys to collect their fees from the defendant (*Graham v. Connor, 490 U.S. 386 (1989)*). Many of the resultant lawsuits contain language regarding the obligation for departments to manage officers’ selection of force implements or techniques. Additionally, it is common for court opinions to focus on the need for job related training; i.e. training that is commensurate with the duties of officers.

In order for departments to demonstrate the job relatedness of their use of force training programs, they need to collect data regarding use of weapons and techniques, the success rates of various control methods, and the types and numbers of injuries to officers and suspects.

In order for this information to be as useful as possible in this regard, and as an analysis tool for departmental planning and management, it must be both valid and reliable. As such, the information must be as accurate as departmental managers can make it, through development of simple, effective data collection mechanisms. One important aspect of this is that the officers must see the collection process, and the planned usage of the data, as non-threatening. If officers believe that the information they record will be used against them personally in some way, they may be inclined to inaccurately or incorrectly report data. This undermines the entire reporting process, and indicates a fundamental breakdown in the labor-management relationship.

### **Public Access to Information**

Despite the fact that many in the public believe that police critical data management practices are highly suspect (Enochs, 1995), another area of legal concern, and one that has gained much attention within the past few years, is that of public access to police information and statistics. The federal Freedom of Information Act, as well as various state “sunshine” laws, or open information laws, guarantee citizens access to most public information (Doherty, 1996). While some sensitive information can be protected (e.g. on-going investigations, etc.), other information must be available and released upon demand within a specified time frame (ACLU, 1997). In fact, some state courts have reaffirmed this requirement by ordering departments to release information (ACLU, 1998).

The need to respond to legal requests for information and records, to demonstrate the job relatedness of policies and training programs, and to comply with the requirements of various “open information” statutes, points to the need to collect, analyze, and maintain accurate databases of critical information.

There are two other dimensions to consider as regards the current legal environment. The first of these is the completeness of critical data, and the second is the ability to ascertain what information should not be released and to act to secure it.

Departments are frequently accused of acting inappropriately in a high-risk incident, leading to the serious injury or death of a citizen. When this occurs, it is not uncommon for the public and the news media to examine the elements of the particular incident, without considering the broader context within which it occurred. In order to properly manage its risks, law enforcement must manage its needs and the expenditure of its limited resources based upon a cost-benefit analysis of its most frequent activities. However, law enforcement incidents are examined as individual occurrences, often without heed to the larger context. An excellent example of this is a high-speed pursuit.

The facts of a particular pursuit related incident, despite a tragic outcome, may not support an ultimate finding of liability on the part of the police. However, the media, and the “Court of Public Opinion”, may damn the actions of the police, based on the outcome and distorted perceptions of the frequency with which similar outcomes occur. In short, the primary focus may be on the number of catastrophic

incidents over the past few years, without regard to the broader context of similar incidents where no catastrophic outcome occurred.

For example, it sounds bad to say that a dozen people have been injured in police pursuits in the last three years. But if a department has accurately collected all the pertinent data, it sounds less bothersome to say that over the past three years, out of 15,000 traffic stops<sup>1</sup>, 12 people have been injured. One can readily see the importance of collecting information on all incidents, regardless of outcome.

Just as important as collecting and presenting available data for release is the identification of information that cannot or should not be released. Court cases have generally held that sensitive information regarding internal practices, on-going investigations, and some personnel information are generally exempt from freedom-of-information requests, and may be protected (*Gifford v. Freedom of Information Commission*, 227 Conn. 641, 631 A. 2d 252 (Conn. 1993)).

In order to effectively achieve this security, systems must be structured so as to allow for the differentiation of various types of information. When considering what we have defined as critical data, security questions generally apply to on-going investigations, or perhaps to the release of information regarding a specific incident. Generally, critical data that is aggregate in nature, and therefore not attributable to a specific occurrence or incident, can and should be released.

## **LAW ENFORCEMENT'S CURRENT PRACTICES**

Incident reporting and data collection practices have improved significantly over the past 10 to 15 years. Most medium to larger size law enforcement agencies are making use of some sort of computer technology, although many are still working with older systems that are frequently "hand-me-downs" from some other branch of government, or the private sector.

Some departments are connected to an internal mini-mainframe computer operated by the governmental entity, while others have such a system in-house. Still others are working with desktop personal computers (PCs), that are sometimes networked and sometimes not.

There are growing numbers of departments utilizing an Intranet, wherein several police agencies are connected to one another through a private "network". In this way, much information can be shared regarding crime trends, demographic analysis, on-going investigations, and multi-jurisdictional criminal activities. At the same time, law enforcement is increasingly gaining access to the Internet, with all of its advantages, and attendant access security issues.

There are still many small departments that do not have access to computer technology within their own agency. It is not uncommon for such agencies to rely on computers owned by other branches of government, or on personal computers

---

<sup>1</sup> Based on 12 officers averaging 5 traffic stops per workday, each working 250 days per year.

owned by the officers themselves. In these departments, what computer-based paperwork there is usually is centered upon the completion of basic crime reports and routine correspondence, with little time, equipment or resources left over for data collection and analysis. Still, such departments can and should collect copies of specific types of reports, and file them together for collective review.

The determinant of the levels of departmental information connectivity does not seem to be size as much as it seems to be the level of sophistication and problem solving capabilities of the decision-makers. With the availability of both state and federal grant money, as well as the proliferation of community oriented policing, many small departments have become quite sophisticated in their use of electronic communications and computing technology.

One technology that is growing quickly among agencies of all different types and sizes is that of laptop computer use. Many departments are beginning to install laptop computers in patrol vehicles, and some are issuing them to individual officers.

These machines are most typically used for receipt and transmission of mobile data transmissions, through a linkage with the agencies' communications system. They are also used for preparation of written reports in the field, often with online transmission of the completed report to a central processing area, where reports are reviewed and stored.

This technological development does much to provide the framework for the recommended collection of critical information. If an officer can complete an online form quickly and easily, and transmit it to a central collection point, the information so collected will be more timely and more accurate. Additionally, programs located in the central computer can analyze the data automatically, thereby negating the necessity for manual input of information by a second party. This system enables faster, more accurate collection and analysis of critical information, while reducing the potential for input errors and other problems associated with the human element.

There has been a parallel development of off-site data collection mechanisms geared toward analysis of critical information. The FBI Uniform Crime Report (UCR) system has been in existence for many years, and once involved writing information by hand onto large "rainbow" forms, which were then mailed to a central office for collation and reporting. Now, many agencies are submitting the same information on-line. While only about 80% of agencies in the United States participate in the UCR system, the increasing ease of data submission may lead to greater involvement on the part of non-participating agencies.

This is important, as the UCR reporting system provides much of the background against which individual departments compare and contrast their local critical data. Greater participation by more agencies, with continued emphasis on completeness and accuracy of information, will lead to greater overall validity of critical information.

One specific data collection effort deserves mention here, that being the *Use of Force Database Project* promulgated by the International Association of Chiefs of Police (National Institute of Justice, 1996). This project, when fully underway, will comprise a searchable database of use of force information, providing even more clearly delineated information against which to view a local agencies' data and practices.

### **Using the Data**

Several specialized uses of critical data have already been discussed, such as legal defense of local practices, and response to FOIA requests. Beyond these, two broader uses of such data can have a significant impact on the internal practices of an agency. The first of these is the establishment of a formal review process, while the second involves the enhanced training of officers, supervisors and trainers.

In the past, normal practice in most agencies has been for an initial supervisory review of reports and data, with occasional review by upper management. The most useful approach to such review would result in the establishment of an Incident Review Committee (sometimes referred to as a Safety Committee).

Such a committee would be charged with reviewing all incident reports resulting from high-risk incidents, particularly those wherein an injury to officers or citizens occurs. This review should be geared toward continued development of policies, training and supervisory methods, or perhaps analysis of the efficacy of equipment and techniques. The aim of this process should be to improve these departmental mechanisms, so as to reduce the potential for future harmful outcomes. Any incident review geared toward disciplinary or other outcomes should be a separate process.

Because of the limited training resources available in most departments, maximum utility must be derived from any training effort. Rather than participating in training on a hit-or-miss basis, departments should review critical data to determine the type, quantity, and frequency of training needed to address officers' daily high-risk activities.

In many departments, the tendency is to focus on the types of high-risk activities that have the most severe potential outcomes (e.g. pursuit driving, use of deadly force). While these types of outcomes can be very costly, in both dollars and in public ill will, they are not usually the most frequent of occurrences.

In fact, when the overall frequency and cost of high-risk activity is considered, the greater risk is usually from the more common daily occurrences (any one of which could escalate into one of the infrequent catastrophic incidents). Instead of pursuit driving, efforts should be focused on driving skills in general; instead of deadly force, training efforts should be geared toward overall use of force issues.

In this way, as the more frequent incidents are better managed and controlled, the likelihood of a more costly catastrophic incident is significantly reduced. This is known as the Inverse Frequency/Severity Relationship, and is made possible by the Law of Large Numbers<sup>2</sup>.

## **THE NEED FOR FURTHER TECHNOLOGICAL DEVELOPMENTS**

The most significant need in the short term is for simpler, more affordable alternatives for incident reporting, data collection and analysis. This should lead to more widespread use of modern technology. Most departments struggle with the affordability of new technology, both in the initial acquisition costs, and in the training and assignment of manpower resources to facilitate operation of new systems. So they continue to use older, outdated systems that are incapable of fully utilizing newer, more user-friendly features and equipment. One example of this shortfall in capability is in the attempted use of digital imaging (i.e. scanners and digital cameras) with older computers. The slow speed and low resolution output that older computers manifest when using these new devices frequently leads to frustration on the part of users.

Simpler systems are needed, at least for the immediate future, as many older officers are frequently less computer literate and more computerphobic than their younger counterparts. The more user-friendly systems are, the more likely these older officers are to use them accurately and completely, thereby assuring more accurate reporting and collection of critical data.

Simpler software systems for analysis and reporting of information would lead to greater use of information by first line supervisors, as well as the officers themselves. Generally, what information is currently available is often only accessible by training coordinators and executive level management.

## **CONCLUSION**

Despite the fact that many law enforcement agencies have moved slowly to develop incident reporting and data collection systems, many are now taking advantage of existing technologies. The current legal environment, and other managerial pressures, clearly indicate the need for continued improvement in both incident-reporting systems and data collection, review and use practices.

As this movement toward more widespread collection and reporting of data continues, the need for simpler, more affordable systems becomes more evident. In the short term, simplicity should be emphasized due to the make-up of the work force. Ultimately, this will be less of an issue, as more computer literate officers move upward through the ranks.

---

<sup>2</sup> The larger the population sample is, the more predictable certain outcomes are.

Perception of information as a valuable resource, to be accurately and thoroughly collected, and carefully analyzed, is the key element in the continued development of police incident reporting and data collection/analysis systems.

As these systems continue to proliferate and evolve, departments will be better positioned to defend officers' actions, while enhancing officer safety and efficiency through more comprehensive, job-related training.

## REFERENCES

- Albrecht, G.L., Halleck, J.W., Lardner, J., & Milton, C.H. (1977). Police Use of Deadly Force. Washington, DC: The Police Foundation.
- Alpert, G.P., & Fridell, L.A., (1992). Police Vehicles and Firearms: Instruments of Deadly Force. Prospect Heights, IL: Waveland Press.
- Avery, M., Blum, K., & Rudovsky, D. (1996). Police Misconduct: Law and Litigation, 3<sup>rd</sup> ed. New York: Clark Boardman.
- Beach, Jr., R.W., Morris, E.R., & Smith, W.C. (1993). Emergency Vehicle Operations: A Line Officer's Guide. Tulsa, OK: Pecos Press.
- Doherty, J. (1996). Public Records Disclosure for Washington Cities and Towns. Washington: Municipal Research & Services Center of Washington.
- Enochs, L. (1995, October). See No Evil, Heart No Evil: Why We Can't Track police Abuse. Jinn, pp. 1-2.
- Fighting Police Abuse: A Community Action Manual [pamphlet]. Washington, DC: ACLU (American Civil Liberties Union).
- Fridell, L.A., & Pate, A.M. (1995). Toward the Uniform Reporting of Police Use of Force: Results of a National Survey. The Criminal Justice Review, 20(2), 123-145.
- Fridell, L.A., & Pate, A.M. (1993). Police Use of Force: Official Reports, Citizen Complaints, and Legal Consequences. Washington, DC: The Police Foundation.
- Geller, W.A., Toch, H. (Eds.). 1995. And Justice for All: Understanding and Controlling Police Abuse of Force. Washington, DC: Police Executive Research Forum.
- National Institute of Justice. (1996). National Data Collection on Police Use of Force. Washington, DC: U.S. Government Printing Office.
- Nowicki, E. (Ed.). (1993). Supervisory Survival. Powers Lake, WI: Performance Dimensions Publishing.
- Patterson, F.M. & Smith, P.D. (1968). A Manual of Police Report Writing. Springfield, IL: Charles C. Thomas.

Rhode Island Supreme Court Opens Access to Police Brutality Records [news release]. Washington, DC: ACLU (American Civil Liberties Union).

***While compliance to the loss prevention techniques suggested herein may reduce the likelihood of an incident, it will not eliminate all possibility of an incident.***

***Further, as always, the reader is encouraged to consult with an attorney for specific legal advice.***