Criminal Justice and the IT Revolution

by Terence Dunworth

ABSTRACT

This article examines the impact on American policing of the information-processing revolution that has taken place since the invention of the transistor. The objective is to assess the opportunities and challenges that this revolution has generated and to examine the responses that American policing has made. An organizing premise of the work is that although the IT revolution promises an enormous increase in information-processing capability, the present reality is that too few police departments are utilizing that capability effectively.

The work begins with a short historical overview of legislation and commissions that addressed or influenced information systems development in criminal justice from the mid-1800s until the Violent Crime Control and Law Enforcement Act of 1994. Reviews are then presented of the current state of policing information systems in the following areas: records management, criminal histories, computer-aided dispatch, crime analysis, uniform crime reporting, and computer networking.

The information system demands made by community- and problem-oriented policing are then examined. The argument is made that community-oriented policing differs in philosophy and approach from professional or traditional policing. The changes in policing that are required are strategic, not simply tactical. In particular, effective implementation of community-oriented policing depends on information gathering and processing systems that are radically different and

Terence Dunworth is the managing Vice President for Law and Public Policy with Abt Associates Inc. in Cambridge, Massachusetts.

more demanding than those needed for professional policing. Seven information domains are identified and reviewed. The claim is made that neglect of these domains, or failure to meet the IT imperatives they assert, will impede, perhaps cripple, the implementation of community policing. The article concludes with a prescriptive and optimistic look at the prospects for the 21st century.

ABSTRACT

It will not be long before personal computers are as common as telephones. This is one consequence of the information technology (IT)[1] revolution that has taken place since the invention of the transistor 50 years ago.[2] Of course, it is now a decade or so since the designation "personal" became inappropriate. What used to be "personal" during the first few years of the revolution has now become general. It is probably not too great a stretch to assert that virtually every organizational, business, and scientific use of information incorporates in some way IT that is encompassed by the rubric "personal computers." In addition, desktop and laptop systems are moving into public and private organizations, as well as homes, far more rapidly than the telephone did, and they seem certain to have, if they have not already had, a greater impact than the telephone on the way public and private activities are conducted.

This revolution has enormous implications for law enforcement, which is generally regarded as a fragmented and sometimes cumbersome processor and user of information.[3] It has provided a capacity for information management that has begun to radically change the way in which law enforcement conducts its business. Though it is true that the pace at which law enforcement has adopted the new IT lags behind many other elements of society, there is also an inevitability about that adoption. In the end, law enforcement will not have a choice. The IT revolution will have to be embraced.

In this paper, I have a narrow focus: the effect of the IT revolution on policing. This is because police departments are, in my opinion, the most dynamic users of the kind of information that the IT revolution is bringing into existence. Police departments use information to make strategic, tactical, and investigative decisions in ways that prosecutors, courts, and correctional agencies do not. Police departments do much more than record their activities, and they are faced with a constant need to adapt to a changing operational environment. In that sense, the IT revolution is a very good fit for their needs.

In the following section, I present a brief historical background of the application of information to law enforcement, beginning with early developments in the 19th century and culminating in the Violent Crime Control and Law Enforcement Act of 1994 (Crime Act).

Following the historical overview, I consider the promise and the reality of IT for policing by reviewing where policing stands with respect to a number of critical information systems areas: records management; criminal histories and offender identification; computer-aided dispatch and emergency response systems; crime analysis; the Uniform Crime Reporting (UCR) system and the National Incident-Based Reporting System (NIBRS); and computer networking technology and the Internet.

I then examine what I consider to be the IT mandate that community policing imposes on police departments. This section looks at the types of information that community policing requires for implementation, and the way that they differ from the information that police departments have traditionally collected.

The final section contains some reflections on policing IT and the 21st century. The potential for the generation of new knowledge and the risks associated with possible misuse of computerized police data are reviewed briefly, and a short conclusion brings the article to a close.

Historical Background

The first 100 years: 1830–1930

Though the intensity of our current focus on information systems in criminal justice is historically unparalleled, a demand for facts about crimes, those who commit them, and the response we muster goes back more than two centuries. Decker (1978)[4] identified early approaches by Bentham (urging data collection on British prisoners in 1778), Guerry (beginning a formalized system of French criminal statistics in 1833), and Quetelet (who commented at the same time on the issues surrounding the strengths and weaknesses of official French crime data).

Decker noted that in the United States, the effort to develop systematic information about crime dates back about a century and a half. In 1834, Massachusetts was the first State to begin collecting data on crimes. The Federal Government did the same, first in conjunction with the 1850 census and subsequently with later censuses. By the early 1900s, data from police reports were being compiled into criminal statistical reports, and Federal prisoner data and judicial statistics were being accumulated, printed, and disseminated by the Office of the U.S. Attorney General.

Though these early efforts were modest by today's standards, the Federal systems in particular generated what appear to have been reasonably accurate compilations of the activity of the Federal judicial system. These were used for decisionmaking about budgeting, facilities construction, and resource allocation issues. Data on crime in cities were another matter. Many police departments lacked the resources and perhaps the interest needed to compile comprehensive and accurate statistics, and the consequence was that knowledge about non-Federal crime and the local criminal justice environment was sketchy at best.

In the 1920s, the International Association of Chiefs of Police (IACP) responded to the need for a uniform, nationwide system of compiling statistics on

crime by developing and initiating a uniform crime reporting system, to which police departments were urged to voluntarily contribute crime data in a standardized format. In 1930, IACP cooperated with the Federal Government in arranging for the transfer of this system to the Federal Bureau of Investigation (FBI), where it is still housed.[5] The 1930 UCR report included 1,002 cities, with participation by 83 percent of cities with populations greater than 25,000.

Wickersham Commission: 1931

In 1929, the same year that UCR was launched, a National Commission on Law Observance and Enforcement was established by President Hoover. This came to be known as the Wickersham Commission, named after its chairperson, George W. Wickersham.[6] Though there had been locally based studies of criminal justice during the previous 10 years,[7] this was the first national evaluation of the system of justice administration in the United States.

The Commission published 13 reports in June 1930.[8] One of these, the *Report on Criminal Statistics*, was an assertion of the need for accurate, nationwide statistics on crime and the criminal justice system. The report reflected the influence of IACP's work on the UCR program, and specifically cited the UCR system as a model. However, the members of the Wickersham Commission wanted to go much further by creating a comprehensive system of national data, encompassing penal, judicial, and police data under one Federal agency. That agency would establish national data collection systems to achieve these objectives. The report also expressed reservations about the accuracy of the crime statistics currently being compiled as well as about their interpretation. In this respect, the Commission's observations were prescient—many of its concerns have been echoed repeatedly in subsequent commentary on UCR.

President's Commission on Law Enforcement and Administration of Justice: 1965

For the next three and a half decades, UCR data was systematically collected and came to be the Nation's only barometer of crime levels. However, little progress was made beyond this, except at the Federal level, where the creation of the Administrative Office of the U.S. Courts in 1938 consolidated Federal judicial and penal system data collection under the new agency, and led to the creation of a centralized process of data compilation and reporting that has persisted largely unchanged (except for computerization) to the present time.

Then, in 1965, President Johnson convened the President's Commission on Law Enforcement and Administration of Justice. The mandate of this Commission, with respect to issues pertaining to crime, was essentially

unlimited, and its extensive report was a wide-ranging and enormously influential document (President's Commission on Law Enforcement and Administration of Justice 1967; U.S. Department of Justice, Office of Justice Programs 1998).

The Commission's examination of information systems and statistics produced gloomy observations by Commission members. Henry Ruth, deputy director of the Commission, is quoted as saying: "Practically no data on the criminal justice system existed when the Commission began work. Not much police data existed. Court data were a mess" (Foote 1998). In addition, the Commission's survey of 10,000 households suggested that crime of all kinds was being seriously underreported to police, with the result that UCR could not be counted on to be an accurate measure of crime levels in the country (President's Commission on Law Enforcement and Administration of Justice 1967, v).

This led to what was in a number of respects a reaffirmation and clarification of the principles and approaches promulgated earlier by the Wickersham Commission, but never adequately adopted—namely, that policy should be informed by knowledge and facts; that the development, collection, and compilation of these data should be the responsibility of a National Criminal Justice Statistics Center; that State statistical centers should be established both to provide information and support to the Federal agency and to generate locally useful data; and that Federal funding should be provided to help accomplish these goals.

Federal legislation: 1968–94

The immediate outcome of the work of the President's Commission was the passage of the Omnibus Crime Control and Safe Streets Act of 1968, which has been the foundation for virtually all subsequent Federal legislation on State and local criminal justice matters. This Act created the Law Enforcement Assistance Administration (LEAA), which from 1968 until 1979 housed the National Institute of Law Enforcement and Criminal Justice (the precursor agency to today's National Institute of Justice) and the National Criminal Justice Information and Statistics Service (the precursor to today's Bureau of Justice Statistics). LEAA also managed Federal assistance to State and local criminal justice agencies,[9] and in 1973 established the National Crime Survey (NCS), which carried forward the approach undertaken by the President's Commission in its 1967 survey. Of NCS, Tonry (1997, 113–114) notes:

> Some observers would say that the National Crime Victimization Survey (NCVS) is the single most important research-and-statistics legacy of the President's Crime Commission. Considering that there were no victim surveys before the President's Commission sponsored the pilots, the NCVS is

> a remarkable accomplishment. Not only has it survived for nearly a quarter of a century, and been steadily improved during that period, but it has now achieved recognition as at least equal to the UCR as a source of information on crime trends and patterns.

Despite the promise inherent in the President's Commission's report and the subsequent legislation, the operational manifestation of the principles the President's Commission espoused did not generate long-term acceptance by Congress or the criminal justice community. By the late 1970s, LEAA was an agency whose time had come and gone. Congressional willingness to fund the agency dwindled from the peak reached in 1976, and by 1980, appropriations were effectively zero.[10]

This discontent with LEAA led to an overhaul of the Federal Government's approach to the management of its efforts to influence and assist State and local crime control activities. In 1979, Congress passed the Justice System Improvement Act of 1979, which took the building blocks created by LEAA and converted them into the Federal system for dealing with State and local criminal justice issues that we know today. The independent National Institute of Justice (NIJ) and Bureau of Justice Statistics (BJS) were created within the LEAA framework. An oversight office—the Office of Justice Assistance, Research, and Statistics (OJARS)—was also set up. When LEAA was formally abolished in 1982, the other three offices survived and the Comprehensive Crime Control Act of 1984 created a new structure, retaining NIJ as the research entity and BJS as the statistics entity. OJARS was renamed the Office of Justice Programs, but kept similar oversight responsibilities, and two new agencies were created—the Bureau of Justice Assistance to manage block grants, and the Office for Victims of Crime to handle victim issues. This organizational structure has survived to the present day and most subsequent legislation has authorized and appropriated funding within it. The exception was the Crime Act, which, among other things, created an independent agency, the Office of Community Oriented Policing Services (COPS), to manage the Clinton administration's 100,000 Cops on the Street program.[11]

Summary

A common theme about information and statistics can be found in the reports of the two Commissions and the legislation that has been enacted. This is that we do not know enough about crime and the criminal justice system, and we must gather, organize, and disseminate more information to develop good policy and make sensible operating decisions. Certainly, until 1967, this was the clarion call that was being explicitly sounded. Since 1967, various acts have

Though the emphasis on collecting facts and increasing our knowledge of the situation with which the criminal justice system must deal is an obvious first step in dealing effectively with crime, data alone cannot tell us what to do.

attempted to codify that call into an effective system for gathering, organizing, and disseminating information.

In some respects, these efforts can be considered a success. BJS now produces an impressive array of data series, covering a large variety of criminal justice topics. NIJ sponsors a wide range of empirical research and itself manages the Arrestee Drug Abuse Monitoring program, a significant data collection effort focusing on drugs and crime.[12] The FBI produces UCR on a nationwide scale. NCVS captures unreported as well as reported crime in ways that most observers consider highly credible and dependable. And at the local level, many police departments have replaced paper records with computerized information systems that would have been infeasible a decade ago.

However, there is a problem. Though the emphasis on collecting facts and increasing our knowledge of the situation with which the criminal justice system must deal is an obvious first step in dealing effectively with crime, data alone cannot tell us what to do. Though it is true that if we do not know the scope of the problem we face, our responses to it are not likely to be appropriately focused, an accumulation of facts is not an answer to policy and operational questions. The facts must be processed in some useful way. They must be analyzed, interpreted, and used as a basis for action. This is where difficulties arise.

Over the past decade or so, extraordinarily rapid increases in data processing capabilities have taken place. What used to take a roomful of hardware to do slowly and sometimes badly can now be done by a machine that we can hold in one hand. We can store vast quantities of records on a device smaller than an envelope. For a few hundred dollars, we can acquire a computing system that is more powerful than one that cost hundreds of thousands of dollars 20 years ago. But, in the field of criminal justice, there is a real question facing us: How do we make this new capacity work for us?

By and large, in the operational world, we do not know the answer. Agencies are acquiring capacity without knowing what to do with it, except to automate paper systems. This is fine, but it is not much of an advance in decisionmaking.

The next two sections of this paper will examine this issue in the context of local police departments. In many respects, police departments have the greatest need among criminal justice agencies for a clear understanding of their environment and the ways they can adapt to it. This makes them, potentially at least, the neediest consumers of the new information systems and technology that have come on line in recent years. For these reasons, they constitute a highly informative context within which to consider the impact of the IT revolution on criminal justice.

There now exists a real danger that the IT revolution will come to be seen as little more than a faster way of collecting information that used to be put down on paper. If this view prevails, policing will have missed the most important contribution that the IT revolution can make—namely, to assist policing to redefine itself along the lines that community and problem-oriented policing propose.

Policing and IT: Promise and Reality

The promise

This section reviews what has taken place in policing with respect to IT development in a number of important areas during the past three decades. The organizing theme is that the rapid technological advances that have taken place outside policing have promised and sometimes delivered significant improvements in information processing capabilities. It is further believed that the incorporation of these advances into police department operations will at least radically improve and perhaps revolutionize policing. Such advances span virtually all of the information gathering requirements pertaining to crime measurement, control, and response that police departments might need.

However, despite this promise, the reality in policing has been, and is, quite different. Large-scale data collection systems of crime measurement, such as NIBRS, have not yet come close to realizing their potential. Few departmentally based systems have been implemented at anything approaching the level that is technologically feasible. Even when implemented, such systems have often come to be viewed as disappointingly irrelevant to the functions that police departments must perform, and a jaundiced view of them is expressed with disturbing frequency by police officers and command staff.

The result is that there now exists a real danger that the IT revolution will come to be seen as little more than a faster way of collecting information that

used to be put down on paper. If this view prevails, policing will have missed the most important contribution that the IT revolution can make—namely, to assist policing to redefine itself along the lines that community and problem-oriented policing propose.

In the balance of this section, I will present an overview of the status of IT in policing across what I consider to be the most significant substantive areas: records management systems (RMSs), criminal histories and offender identification, computer-aided dispatch (CAD) and emergency response systems (ERS), crime analysis, UCR and NIBRS, and computer networking technology and the Internet.

The reality

Records management systems

An RMS is the informational heart of any police department's operations. It provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, and files about every aspect of police business. A comprehensive and fully functioning RMS should include crime and arrest reports, personnel records, criminal records, and crime analysis data. Even today, this is the exception rather than the rule. Though virtually all staff in any police department use and depend on the information that an RMS should contain, many departments have inadequate or incomplete systems.

Prior to the 1970s, nearly all police department recordkeeping was paper based. Gradual conversion to mainframe computer recordkeeping began in the 1970s, particularly for crime and arrest information. By the mid-1980s, an estimated 1,500 of the Nation's 17,000 police agencies were using mainframe computers to a limited extent. Characteristically, because of the high investment cost associated with mainframes, most departments shared time with other city agencies, and management of the machine and the system was outside the department. Typically, RMS was little more than a recordkeeping system, with functions that differed little from those provided by its paper predecessor. As late as 1993, a BJS survey found that one-third of local police departments did not use computers for any element of recordkeeping (Brady 1997).

Lack of control over the system, poor links between its elements, and, sometimes, police department disinterest in recordkeeping or lack of experience and understanding of computers resulted in limited utilization of RMS. Even today, many departments have only partial computerization of recordkeeping. Some have no automation on key elements of their RMS, and a number cannot, for

instance, perform simple tasks that computers ought to be able to do easily, such as automatically compile UCR, link arrests to crimes reported, and so on. Consequently, in such departments, these kinds of functions still have to be performed manually, if they are done at all.

More recently, some departments have begun to move to fully automated (computerized) RMS. Some of these departments have gone beyond simply automating recordkeeping procedures by implementing dynamic, relational databases as an integral element in information management.

In such departments, an RMS is no longer a standalone system; it can be interfaced to other systems in the city or county and to State law enforcement systems, which in turn provide access to national crime databases. More recent systems provide graphical user interface with menus, buttons, icons, and other easily recognizable screen images. Built-in editing and error checking can reject incorrect information as it is entered, thus prompting correction before it is stored.

Incident address records are a good example of this capability. When entered by hand, addresses frequently contain mistakes; error rates of 30 to 40 percent are common. Now, some departments have all legitimate city addresses stored in a master file that is scanned whenever an address is entered. Addresses not found are rejected and a prompt for correction is issued. This produces percentage accuracy rates in the high 90s, a critical accomplishment for use with other computer-based applications such as crime mapping.

Thus, a state-of-the-art RMS can be integrated with other systems, such as CAD. They can track all the functions of a police precinct, not just arrests and bookings, in one complete package. For example, the latest breed of RMS can manage budgets; keep an active inventory of supplies, property, and evidence; schedule K–9 care and vehicle maintenance; organize intelligence; track 911 data; and automate many other departmental functions. This new breed also supports access to a wide range of external databases, such as the National Crime Information Center (NCIC) and NIBRS, and has the ability to share information with other justice agencies at all levels of government.

These capabilities create significant new potential for police departments: to conduct advanced crime analysis; to ground strategic and tactical decisionmaking on sound information; to deploy resources on a proactive rather than simply a reactive basis; and to execute many other functions that either were impossible to perform under earlier systems or were performed under conditions of extreme uncertainty.

However attractive a picture is drawn, it must be recognized that implementation of an advanced RMS is not a simple matter. Turnkey systems are rarely viewed as attractive by departments considering vendor offerings, and this creates major design issues. Some departments that have committed to state-of-the-art systems spend many months, or even years, in the design phase. Those that do not run the risk of disappointment, disillusionment, and failure. The process takes a major commitment of resources and budget, and can be very difficult to justify to a city council that is already under severe budgetary pressure.

Even when acquired, an automated RMS requires extensive user training, which, because of the expense, departments may neglect or underfund. Officer resistance can also be a factor, because the modern RMS imposes information collection demands on officers that many view as irrelevant at best and obstructive at worst. Departments must normally consider hiring new staff or training inhouse staff to provide ongoing user training and support, system maintenance, and troubleshooting. In the past, police departments have not attempted to hire such staff, and they do not find it easy to do so now.

Another common concern addresses liability and security with respect to personnel files and other sensitive data such as investigation reports and criminal records. As computer-based applications have grown, so have security breaches. Even government systems that are protected by the most sophisticated national security systems have yielded to persistent hackers. When a major objective of computerization is to simplify the exchange of information among and between officers and headquarters, the risk of improper access is obvious.

Despite these caveats, it is evident that no department will be able to take full advantage of the benefits that the IT revolution offers if it does not acquire a modern RMS. In a real sense, all other IT applications depend on RMS. If it is absent or deficient, then a domino effect seems inevitable. The other applications either will not realize their potential, or they will fail outright.

Criminal histories and offender identification

As noted above, a critical component of recordkeeping involves criminal histories and offender identification. These have always been problematic areas for police departments. There are two main reasons for this. First, definitive identification at the time of arrest is sometimes difficult to achieve. Some arrestees simply give false names and carry no documents. The result is that a delay in identification occurs, and police records are, for a period of time that in some cases can be lengthy, inaccurate or incomplete, or both. Second, even when identification is made at the local level, linking the offender to records in other

jurisdictions can be a difficult and tedious process. Because arraignments usually have to be held within 48 hours of arrest, this can lead to bail decisions that would be quite different if the full history were known.

These problems were first widely discussed in 1967, with publication of the report by the President's Commission on Law Enforcement and Administration of Justice, which noted that criminal history records were frequently inaccurate, incomplete, and inaccessible. These problems persist. A data quality survey conducted in 1997 found that only 25 States reported that 70 percent or more of arrests from the past 5 years had entries for final dispositions in their criminal history database (Barton 1999).

What is obviously needed are identification and history systems that overcome these problems quickly and efficiently. Ideally, these should be integrated into RMS. Computerization offers that potential, though it would be accurate to say that the potential has not yet been realized.

Nevertheless, both Federal and State criminal history and identification systems have evolved significantly over the past few decades. States have established criminal history repositories that contain information about arrests occurring throughout their State. The FBI maintains criminal history systems for Federal offenders and national criminal record systems, including NCIC, the Interstate Identification Index, and an automated National Fingerprint File.

Over the past decade, the Federal Government has invested more than $200 million to improve the quality of criminal history records at the State and Federal levels. These records are not only critical to the day-to-day operation of virtually every Federal, State, and local criminal justice agency, they are also of increasing relevance to applications outside the criminal justice field. Most States permit some access to criminal history records by agencies outside criminal justice for employment, licensing, and other purposes.

Perhaps of greater portent are the mandates imposed by the Handgun Violence Prevention Act (known as the Brady law) and the National Child Protection Act of 1993. These significantly expanded the importance of criminal history records for determining eligibility to purchase a firearm and for screening childcare facility employees. Though there is a good deal of controversy about the constitutionality and efficacy of this process, some evidence exists that it has had an effect. BJS has reported that from March 1, 1994, to November 29, 1998, approximately 12,740,000 applications for handgun purchases were made. There were 312,000 rejections as a result of the background checks required by the Brady law (Manson, Gilliard, and Lauver 1999). Whether this should be considered many or few may be a matter of debate. What is not at

issue is the dependency of this result on automated information processing that could not even have been attempted a decade ago. Like it or not, the ability to perform such checks is a remarkable IT achievement.

Expansion of such checking seems assured for the future, and, given the expanding public and political attention being paid to gun violence, there seems no doubt that the checks considered necessary will become increasingly demanding and sophisticated. Anyone who has examined the amount and type of information generated by a single arrest knows that it can be complex and voluminous, perhaps involving several agencies within a single jurisdiction. Compiling a comprehensive criminal history involves multiple jurisdictions. To have complete, accurate, and timely access to such histories, each step in the process must be carefully executed, and the results must be subject to the most rigorous quality control.

To achieve these goals, Federal and State agencies will need to implement a number of different strategies. These will include conducting baseline audits of record systems to understand the nature and extent of data quality problems; entering backlogs of manual arrest and disposition records into automated files; developing long-term data quality improvement plans; and undertaking efforts to obtain unreported dispositions from courts and prosecutors. To date, this has been a Sisyphian task because much of the desired information exists only on paper or, even if automated, in nonstandardized form. Consequently, implementing dependable and uniform electronic interfaces between reporting agencies and the central criminal history repository will be a prerequisite for expanding the effective utilization of criminal histories. In fact, a good deal of work is being done to bring this about.

The key, in the end, will be the extent to which individual police departments develop the capacity to take advantage of the State and Federal systems that are being created. This is another of the IT challenges that departments face.

BJS currently manages a major Federal initiative—the National Criminal History Improvement Program (NCHIP)—that provides funding to the FBI and State criminal history repositories. The goal of NCHIP is to ensure that accurate records are available for use in law enforcement, including sex offender registry requirements, and to permit States to identify ineligible firearm purchasers; persons ineligible to hold positions involving children, the elderly, or the disabled; and persons subject to protective orders or wanted, arrested, or convicted of stalking and/or domestic violence. NCHIP also provides funding to the FBI to operate the National Instant Criminal Background Check System (established pursuant to

the permanent provision of the Brady law), the National Sex Offender Registry, and the National Protective Order File.

These developments move law enforcement closer to the goal of rapid identification and accurate recovery of history information. The key, in the end, will be the extent to which individual police departments develop the capacity to take advantage of the State and Federal systems that are being created. This is another of the IT challenges that departments face.

Computer-aided dispatch and emergency response systems

Responding to citizen calls for service has always been a central responsibility of law enforcement as well as other public safety services. Early systems by necessity involved either direct contact with a beat officer or hand processing of crime reports made to a station. Dispatch of officers was then handled from the station. Records concerning service calls were handwritten. The introduction of radio into patrol cars made voice dispatch by radio message a reality, and the advent of computerization created the possibility of CAD and automated records of calls and responses.

To make public safety response more effective, a single national emergency number was proposed in 1957 by the National Association of Fire Chiefs as a way to report fires nationwide. In 1967, the President's Commission on Law Enforcement and Administration of Justice also recommended the establishment of a nationwide number for reporting emergency situations, and in 1968, the Federal Communications Commission (FCC) collaborated with AT&T to establish the digits 911 as the emergency number throughout the United States.

Implementation of the 911 system was relatively slow. During the first decade of 911, roughly 17 percent of the country adopted the system. By the late 1990s, that figure had risen to approximately 85 percent.

As the 911 system grew, police departments, city governments, and citizens continued to view quick response to service calls to be a central measure of the effectiveness of a department. Heavy advertising of 911 took place, and public awareness of the system grew. This led to a steady increase in the demand for services that was channeled through the 911 system, with resulting upward pressure on police department resources and budgets. This was consistent with the view of policing as reactive rather than proactive. That is, police departments were expected to respond rapidly to citizen calls for service, and so should organize in such a way as to optimize that capability. Performance standards for departments frequently included "average response time" to 911 calls, and the objective was to have this be a matter of a few minutes. Generally speaking,

however, most cities and departments would no doubt consider that police resources did not increase commensurate with the demand for them. Nevertheless, citizen expectations of an immediate response remained.

At present, more than 97 million calls for service to 911 are made annually, and the number is growing. The proliferation of cellular phones appears to be contributing significantly to the growth. Cellular 911 calls in California have increased 750 percent in the past 10 years, amounting to more than 2.2 million in 1995. More than 10 percent of California 911 calls now come from cellular phones, and cellular callers wait an average of 26 seconds for an answer. Many of these calls are either duplicate reports of the same situation or nonemergencies.

Estimates on how many 911 calls of all kinds are for nonemergencies vary from city to city, but the range appears to be from 45 to 80 percent (U.S. Department of Justice, Office of Community Oriented Policing Services 1997). Such calls could, in principle, be handled outside the emergency response system, but determining their nonemergency nature is difficult during the call itself. An incorrect decision by a 911 calltaker can have fatal consequences, and consequently erring on the side of caution is the prudent course. The result is that many emergency responses are made to calls that in fact did not require quick reaction. It is a truism to note that this places excessive demand on the resources of police departments.

Another result is that legitimate 911 calls may get an inadequate response. For example, when the volume of calls is high, callers may be put on hold or may get a recorded message. In Los Angeles in 1995, 325,000 callers hung up the phone when they were not able to contact a dispatcher quickly (U.S. Department of Justice, Office of Community Oriented Policing Services 1997). The California Highway Patrol also concluded that overloaded cellular channels contributed to hangups by cellular callers (911 Dispatch Services, Inc. 1996).

In an effort to sustain a rapid response time to true emergencies while nevertheless curbing unnecessary responses, police departments began to experiment as early as 1976 with different ways to "manage demand" (Kennedy 1993). More recently, some jurisdictions have publicized alternate numbers for nonemergency calls. In August 1996, COPS petitioned the FCC to reserve the code 311 for use by communities as a nonemergency police and public service telephone number, and the FCC approved this designation in February 1997.

Support for the idea that 911 is overloaded and that 311 can help is not universal. In favor of the use of 311 as a universal nonemergency service number are COPS, the National Sheriffs' Association, and the National Troopers Coalition, as well as various police and fire departments. However, the National

Emergency Number Association (NENA), concerned that there would be public confusion between the uses for 911 and 311, did not support the establishment of the national nonemergency police number (Ellison 1996). NENA maintains that there is no national overload of the 911 system, and that there are already local nonemergency numbers in place in communities that require such a system. The Association of Public Safety Communications Officers also declined to support a mandatory three-digit number for nationwide nonemergency use, arguing that a greater concern was making 911 service available to the 32 million people in the United States without such access (Lorow 1997).

In October 1996, Baltimore, Maryland, in partnership with COPS, began a 2-year trial of 311. The Baltimore Police Department increased calltaking staff by up to 64 percent, contributing to a reduction in 911 answer time and abandoned calls, as well as to an overall drop in the number of 911 calls (Allen 1997).

Other jurisdictions soon followed Baltimore in implementing 311. In February 1999, eight jurisdictions were recipients of COPS funds totaling $3.85 million for the purpose of enhancing or creating a local 311 nonemergency system: Baltimore, Maryland; Birmingham, Alabama; Dukes County, Massachusetts; Houston, Texas; Los Angeles, California; Miami, Florida; South Pasadena/City of Pasadena, California; and Rochester, New York. Given a positive outcome in these jurisdictions, further moves toward a 311 approach seem likely.

No matter how the 911/311 issue is eventually resolved, CAD is now a fundamental component of response capacity in many police departments. The current generation of CAD systems is able to integrate Enhanced 911; identify the location and number of the originating call; provide mapping capabilities; and communicate directly with computers in patrol cars, national databases, and the department's RMS database. Further enhancements are certain as the IT revolution continues. As technological and cost barriers decline, a wider acceptance of CAD will be inevitable. Without doubt, CAD will be considered a prerequisite for effective policing in the 21st century for departments of all sizes.

Mobile data terminals

During the past decade, another important element of law enforcement response capability has been developed through mobile data terminals (MDTs). These allow wireless receipt and transmission of information to and from officers on foot or in patrol cars. Initially, MDTs were basically unsophisticated terminals that permitted transfer of rudimentary information between station and officer. Dispatch instructions, for instance, could be sent to the terminal rather than being put out over police radio. The officer could automatically record and transmit arrival times at the dispatch location. In the past few years, however,

technological advances have led to the introduction of laptop and notebook computers, pen-based computers, voice-based computers, and handheld ticket-issuing computers. These now match desktop machines in sophistication, and will continue to expand in capability. As miniaturization progresses, for instance, handheld devices that do not require patrol car installation seem certain to proliferate. This will free officers from patrol car dependence, and increase the scope and sophistication that officers on the street can exercise with respect to two-way information flow. In this sense, MDTs are becoming much more than aids to response.

First available around 1990, today's laptop models can be operated by officers on a standalone basis or combined with onboard radios, built-in cellular phones, or computer docking stations. In terms of technical capacity, law enforcement laptops equal any other machine. One difference is construction—enforcement laptops tend to be "ruggedized" to withstand the shocks and rough handling that a law enforcement environment potentially inflicts. When connected to cellular phone-based systems, laptops can send and receive data to and from remote sites. Some laptop computers provide touch-screen capability. The potential utility of these machines is obviously vast. Not only can they be used to transmit virtually any kind of information back and forth, but they can be used to provide rapid authorization for police actions through faxed warrant requests and approvals, thus eliminating the sometimes crippling delays that, in the past, could result from having to return to the station, write up a justification, submit it, and then return to the scene.

Handheld ticket-issuing computers, used principally in parking enforcement, enable officers to issue computer-generated citations and simultaneously check the vehicle for outstanding tickets. These systems contain as many as 40,000 records, including information on stolen or wanted vehicles, and can also be used to record field interviews.

Pen-based computers were first introduced in 1989 as clipboard-size mobile computers, weighing less than 5 pounds, that recognized handwriting and converted it to text. Some pen-based computers have radio capability. Pen-based computers can be mounted in patrol cars, but officers can remove and operate them for a limited distance from the vehicles. Because the software used to recognize handwriting was initially perceived as inflexible, pen-based computers have not gained large-scale acceptance in law enforcement. This is certain to change as departments see the benefits of the technology that is now common in business use of handheld devices (Gapay 1992). In fact, the problem departments will face is that handheld devices will become so functionally capable that they will eclipse the car-based laptop.

Computers that offer voice recognition and translation for input to computer files are in a similar category to pen-based systems. Rapid improvements in technology are making such devices much easier to use—by 1996, voice dictation technology was already 95-percent accurate at a dictation rate of more than 70 words per minute. The disadvantage is that the technology still requires considerable user (and machine) training. This burden declines each year, and is going to decline more as the technology gets better. Accurate computer "listening" to normal human speech will become generally available within the next few years. Given the obvious advantages of effective voice input over pen or keyboard, the use of voice recognition seems likely to be the next MDT advance. This promises a very significant reduction in the amount of officer and headquarters staff time that is presently consumed by the reporting function.

Though there are few empirical studies of the impacts of MDTs, their reported benefits include:

- Increasing the speed of information dissemination.
- Saving officers time and effort.
- Facilitating information sharing.
- Increasing reporting accuracy and uniformity.
- Enhancing response time.
- Increasing officer safety.

There are considerable obstacles to implementation of MDTs. These include expense, a lack of information about available products, a need for significant amounts of user training, and possible officer resistance to or misuse of the devices. All of these seem likely to decline in importance as progress continues, but their short-term effect has been to limit the implementation of MDTs in the policing world.

For example, a 1995 Police Executive Research Forum survey of 210 departments drawn in part from among 1995 COPS MORE (Making Officer Redeployment Effective) Federal grant recipients found that only a small percentage of police departments had MDTs in patrol cars (Bezdikian and Karchmer 1996). However, within that minority, many departments had been using laptops in patrol cars for years.

In 1997, NIJ sponsored a study by the National Law Enforcement and Corrections Technology Center on cross-jurisdictional communication

(so-called "interoperability"). A total of 1,344 agencies responded to the questionnaire. The agencies that were currently using MDTs employed them primarily for database information and free text (e.g., reports, queries). Nearly one-quarter of the agencies (24 percent) used database information (primarily agencies with 500 or more sworn officers), and 21 percent of all agencies used free text. However, the use of MDTs was far less common in smaller agencies—as low as 4 percent of agencies that employed fewer than 10 sworn officers.

Despite current limitations, more departments can be expected to use MDTs. Some Federal funds are being provided to assist purchase. An added impetus for implementation is to enable officers on the street to take advantage of the FBI's new NCIC 2000 and Integrated Automated Fingerprinting Identification System initiatives. MDTs also will assist departments in conforming to the new incident-based reporting standards of NIBRS. These clear advantages, coupled with declining cost and increasing ease of use, suggest that it will not be long until virtually every department uses MDTs of one type or another.

Crime analysis

Crime analysis is a process involving the systematic analysis of data drawn from series of criminal incidents, rather than focusing upon a single incident. It seeks to identify patterns of criminal activity, and the interaction between them and other events and conditions. In more concrete terms, Reuland (1997) identifies four specific functions for crime analysis:

To support resource deployment. Crime analysis for this purpose involves detecting patterns in crime or the potential for crime to enhance the effectiveness of daily patrol operations, surveillance, stakeouts, and other police tactics. These analyses influence personnel deployment and resource allocation.

To assist in investigating and apprehending offenders. By comparing files that contain modus operandi characteristics with files of new suspect attributes, departments hope to make more and better arrests.

To prevent crime. Crime analysts focus on identifying locations, times of day, or situations where crimes appear to cluster so that departments can take steps to harden these potential targets to make them less likely targets of crime.

To meet administrative needs. Law enforcement administrators need to provide other individuals and agencies with crime-related information, including city agencies, courts, government offices, community groups, and the media. Administrators may need to use crime analysis in this context for legislative, political, and financial purposes.

Crime analysis may also serve strategic purposes for planning agencies, crime prevention units, patrol and investigative commanders, and community relations units in terms of their program, planning, development, and evaluation functions.

It is clear that crime analysis is a process for which computerized data processing is tailormade. However, it is true that law enforcement agencies have been doing some form of crime analysis from time immemorial. Policing has not been random and has not been reactive to the exclusion of all other considerations. Crime analysis has always guided decisionmaking. However, the advent of desktop computers has increased the power and speed of crime analysis tremendously. Technically, what we can do now is orders of magnitude greater than what was possible a few years ago. Community policing and problem-oriented policing have provided another recent impetus to enhanced crime analysis. For these and other reasons, the number of departments with crime analysis units has been growing over the past several years.

The five stages of crime analysis illustrate the natural fit with the IT revolution:

Data collection. Law enforcement data are generated primarily from records and reports within the department. Data sources internal to the department include field interviews, offense reports, investigative reports, arrest reports, evidence technician reports, criminal history records, offender interviews, traffic citations, intelligence reports, and calls-for-service data. For community policing purposes, information is also likely to come from nonpolice sources, such as schools, utility companies, city planners, parks departments, social service agencies, courts, probation and parole agencies, other police agencies, and the Bureau of the Census (e.g., for demographics of a given area).

Data collation. Departments create databases capable of automated searches and comparisons. Basic database requirements include completeness, reliability, and timeliness.

Analysis. Departments analyze crime data to detect patterns of activity that can assist current investigations and predict future crimes. Crime mapping is an example of an increasingly popular analysis approach.

Dissemination. Departments prepare data for internal and external users. Face-to-face contact between crime analysts and officers and investigators, and with some other users, can be important for developing a mutual understanding of the data and their usability.

Feedback. Measuring users' satisfaction with the information they are given is essential. Crime analysts need to find out what products and formats work and do not work. They must also learn how end users plan to use their products. Analysts can use a simple, closed-ended survey form to obtain feedback, as well as personal contact.

The most prominent crime analysis technique to have been developed as a direct consequence of the IT revolution is computerized mapping. Although computers have been used to display and manipulate maps since the 1960s, the use of mapping software in criminal justice is a relatively new phenomenon. Its growth is due largely to the recent development of inexpensive yet effective and sophisticated PC-based mapping software packages and to the emphasis being placed on it by the Federal Government (National Partnership for Reinventing Government 1999). The application of mapping software to urban settings depends on the existence of addresses in the data being mapped. Consequently, mapping is most likely to be used for crime analysis in medium and large police departments where computerized address data are a byproduct of routine, day-to-day work (Rich 1995, 1996, 1998).

However, utilization is by no means universal. In 1994, 30 percent of 280 member departments of the IACP Law Enforcement Management Information Section (among the most active users of computer technology among local departments in the Nation) reported having used mapping software. A 15-month survey of 2,000 law enforcement agencies conducted by the NIJ Crime Mapping Research Center found that only 261 used any computerized crime mapping. Not surprisingly, larger departments (more than 100 sworn officers) were much more likely to use the technology (36 percent) than were smaller departments (3 percent) (Mamalian and La Vigne 1999).

Despite the widespread availability of computers and the growth of applications software that seems to closely fit policing's crime analysis needs, the majority of police departments have not yet embraced a comprehensive approach to crime analysis (Reuland 1997). A number of contributing obstacles can be identified:

- The perception by some sworn officers that crime analysis is not needed for real policing and contributes little to understanding the street conditions under which they have to work.
- The fact that crime analysis is often conducted by civilians, who lack the standing within the department to promulgate the results of their work and its implications for strategic and tactical decisionmaking.

- Uncertainty regarding hardware and software technology, and the difficulty of mastering the range of available techniques.
- Inaccurate or missing data in police records systems (e.g., addresses for mapping applications).
- Difficulty making arrangements to obtain necessary data from other agencies.
- Inadequate or nonexistent crime analysis training.
- Insufficient funding.

The principal obstacles to more widespread and better crime analysis seem likely to decline as hardware, software, and data acquisition costs decline, as user expertise increases, and as data quality improves. Nevertheless, many departments are still some distance away from the acceptance of crime analysis as an important policing tool.

Uniform Crime Reporting/National Incident-Based Reporting System

The discussions so far have focused primarily on IT as it relates to individual departments. However, critical needs exist with respect to aggregate measures of reported criminal activity and documentation of national crime trends. These needs have historically been addressed by the UCR system, which began operation in the early 1930s and has been in place with little change ever since. The system is dependent on local police departments, which voluntarily submit a variety of aggregate data to the FBI each year in standardized format. Compilations of UCR data, published annually by the U.S. Department of Justice under the title *Crime in the United States*, generate a statistical overview of data about law enforcement administration, operations, and management, and have served as a primary source of information for researchers and the public. *Crime in the United States* offers sections on UCR's major topics: crimes cleared, persons arrested, law enforcement personnel, and a Crime Index based on eight selected offenses. However, UCR is unable to link an offense to its associated arrest, and the system is believed to have a number of significant limitations.

Because of these perceptions, it was acknowledged in the mid-1970s that a revised and enhanced UCR was needed for use into the 21st century. This coincided with advances in information technology that made a more sophisticated system feasible. BJS and the FBI funded a substantial examination and reassessment of the UCR program, which culminated in the 1985 publication of a *Blueprint for the Future of the Uniform Crime Reporting System* (Poggio et al. 1985).

The *Blueprint* proposed NIBRS to replace the existing UCR system. The plan called for incident-based reporting, rather than aggregate reporting, represented by two levels of reporting complexity, the more detailed of which would be followed by only 3 to 7 percent of law enforcement agencies nationwide. Ultimately, the law enforcement community endorsed the NIBRS framework but elected to institute the more complex reporting level for all participating agencies.

To achieve standardization across jurisdictions, the FBI sponsored the development of new offense definitions and data elements for the new system. Based on the results of a pilot program at the South Carolina Law Enforcement Division, representatives of the law enforcement community in 1988 approved the revised UCR guidelines and voiced overwhelming support for the new system.

Representing both an expansion of UCR and a major conceptual shift, NIBRS is an "incident based" system that collects detailed information on individual crimes, including data on location, property, weapons, victims, offenders, arrestees, and law enforcement officers injured or killed. In addition, under NIBRS the scope of reporting is widened to cover 22 crime categories that include a total of 46 specific offenses, known as "Group A" offenses. For an additional 11 "Group B" offenses, NIBRS collects detailed data on persons arrested.

Whereas UCR requires local law enforcement agencies to report monthly aggregate figures on crimes and arrests, NIBRS asks local agencies to submit data on individual incidents for compilation at the State and Federal levels. This offers a potential for analysis that would be impossible using only UCR aggregates, but it also decreases local agencies' control over dissemination of information.

Despite the potential benefits of NIBRS to law enforcement management, training, and planning, law enforcement agencies have been relatively slow to adopt the system. As of May 1997, only 10 States were certified to report NIBRS data, and only 4 percent of U.S. criminal incidents were reported under NIBRS. Large law enforcement agencies have been especially reluctant to make the transition to NIBRS; as of May 1999, the Austin (Texas) Police Department remained the only agency serving a population over 500,000 to report NIBRS data.

According to a recent SEARCH study, law enforcement agencies see lack of funding as the primary obstacle to full adoption of NIBRS (Roberts 1997). Indeed, the costs associated with the transition can be substantial, especially as many law enforcement agencies have existing records management systems

that either are too antiquated to function effectively or are incompatible with NIBRS requirements.

The study also indicated that local law enforcement decisionmakers remain unsure of the benefits of NIBRS reporting and perceive several possible drawbacks to the new system. Although the greater accuracy offered by NIBRS is desirable in principle, some local officials fear a negative public reaction in the event that more precise reporting gives the impression of rising crime rates. Moreover, many officials view NIBRS as a tool for academic research rather than daily law enforcement, or are concerned that reporting the more detailed information requested by NIBRS will place an undue burden on officers in the field. Study participants also discussed the need for Federal agencies to encourage participation in NIBRS by reaffirming their commitment to the program and providing better education as to the aims and utility of the revised system.

It is essential to recognize that the technical and cost problems are not created by NIBRS information needs. They are a consequence of the outmoded and inadequate IT systems that many departments have in place. In fact, as departments upgrade and automate recordkeeping systems, they do generate computerized data that would meet all NIBRS needs, provided the requirement for cross-jurisdictional standardization of definition of offenses and other data elements can be achieved. Most big-city departments, for example, now have data systems that contain a good deal more than the NIBRS data elements, and some perform analyses that match in sophistication those contemplated by NIBRS advocates. This suggests that the main obstacles to more widespread implementation of NIBRS are not so much technical or financial, but rather derive from perceptions that NIBRS contributes little to local needs for crime analysis and information, while simultaneously containing a good deal of risk to local jurisdictions. In this sense, the potential contribution of NIBRS seems destined to be greatest at State, regional, and national levels. It remains to be seen whether the perceived value of this potential will be sufficient to mobilize the voluntary local participation on which NIBRS depends.[13]

Computer networking technology and the Internet

The topical reviews provided earlier in this section demonstrate that IT advances, combined with law enforcement agencies' increasing emphasis on crime prevention, community-oriented policing, and problem solving, are redefining the pursuit and use of criminal justice information. The development of incident-based reporting systems and increasingly sophisticated techniques of crime analysis have caused sharp increases in the volume and complexity of collected data. As this has occurred, new technologies have begun to play a crucial role in agencies' efforts to disseminate, share, and manage this torrent of criminal justice information.

Within the past 10 years in particular, computer networking—at its simplest, nothing more than linking two or more computers so they can share information—has revolutionized the way we exchange and access data. Many organizations use internal networks, or intranets, to connect the computers within that organization. When two or more individual networks are connected, an internet is formed. The most advanced public level of such systems is, of course, the Internet, a vast collection of interconnected computer networks worldwide, serving millions of users. The easy-to-use World Wide Web (known simply as the Web) is the most popular area of the Internet, and consists of sites dedicated to various topics.

This rapidly evolving technology has created a host of challenges for law enforcement officials, whose previously disconnected agencies seem especially suited to benefit from networking technology. Networking centralizes data in order to streamline administration and help agencies collect and manage huge volumes of crime-related information. Additionally, computer networking plays a valuable and expanding role in facilitating communication at all levels: among local, State, and Federal agencies; between local agencies and constituent communities; or across agencies within a given region or locality.

One of the Web's most common law enforcement applications has been the establishment of Web sites to facilitate communication with the communities served. As of August 1997, more than 500 local law enforcement agencies maintained Web sites, and the establishment and expansion of sites continues at a rapid pace (Goodman 1997). Information on the Web is presented in a lively and interactive format, and may be accessed by interested persons at any time from anywhere in the world. By allowing agencies to interact cheaply and easily with members of their constituent communities, an effective Web site can significantly enhance police-community relations and further community policing objectives. In responding to a faxback survey by the FBI, for example, most departments that have sites on the Web reported extensive use and positive responses from citizens (Sulewski 1997).

Web sites can fulfill multiple functions for law enforcement agencies. Most sites disseminate a range of public safety information, including self-protection tips, crime reports and advisories, news of recovered stolen property and local fugitives, clarifications of laws and answers to frequently asked questions, statistics and budgetary information, community announcements, and information about the agency and its staff. On some sites, communication is two way, allowing the public to interact with the agency that serves them. Citizens can use the Web to apply for permits, file reports on minor incidents, offer tips and information on crimes, and respond to the agency's performance. A Web site makes it more likely that community members will contribute to the agency's

work, since it is easier and quicker to use the Internet than to go to the agency's office. Web sites can also reduce recruiting costs for agencies, which are able to widen their pool of applicants and provide prospective employees with information.

The equipment required to establish a Web site and make quite sophisticated offerings is simple and relatively inexpensive: a computer, a word processing program, a Web processing application, and, for some applications, a digital camera and scanner. Personnel resources may be harder to come by, but a small industry of experts now exists and assistance is easy to obtain. As Internet use has spread among law enforcement agencies, Web design companies have developed expertise in creating law enforcement sites, and many Internet service providers have begun to donate access and expertise to local police and sheriff's departments (Sulewski 1997). Departments have found Web sites to be very cost-effective; once the site is set up, the cost of maintenance is minimal, and sites reduce expenditures for publishing public records and recruiting employees (Paynter 1998).

However, the Internet is not a panacea. Law enforcement agencies that use Web sites to connect to the community must be aware that not all residents use or have access to the Internet. There is an access bias, because low-income residents are less likely to be familiar with and have access to the Internet than affluent residents in the same area. Some will not have computers; others will not even have telephones. Thus, agencies should continue to pursue traditional methods of public education, such as posters or meetings, to reach everyone in the community.

A potentially valuable application of networking technology could lead to integrated justice information systems. These are essentially computer internets that would link numerous separate agencies—police departments, prosecutors, courts, etc. Integration may also be pursued among different levels of government, within geographic regions, and/or across disciplines. The cited benefits of integrated justice information systems are clear: They improve the quality of data available to all users; save time and money by eliminating redundant data entry; facilitate timely access to information; and permit accurate information sharing across distance and time. For many years, the fragmentation and lack of coordination among criminal justice agencies has been deplored; the criminal justice system, according to many, is not a system. Networking seems to offer the potential for addressing this problem.

Setting up an integrated system typically demands an extended planning process, requiring the participation of all stakeholders. The planning process involves building support for the project, assessing needs, planning strategy,

setting standards for data collection, identifying technological solutions, and establishing an oversight board for acquisitions and implementation. During the planning phases, particular attention must be given to setting information systems standards, which have been called "the linchpin to integration" (Roberts 1998). For successful integration, standardization is required in several areas: data definitions, a common language for use between information systems, communications protocols used between agencies, procedures for transferring different types of information (e.g., photos, fingerprints), and security.

The foregoing indicates that regardless of the advantages of integration, it should not be undertaken lightly. Rather, it is an extended process that requires substantial financial and human resources, as well as a sustained commitment from all involved agencies, to be completed successfully. A qualitative study conducted by SEARCH identifies the following primary obstacles to adoption of integrated justice information systems:

- Persistence of entrenched information processing systems and data at local agencies.
- Difficulty of coordinating interagency projects.
- Limited understanding of technological issues and capabilities.
- Need for systems to be private and secure.
- Fundamental interagency differences in recording/reporting systems.
- Shortage of information technology professionals.

Though the impediments to establishing integrated justice information systems are significant, a number of evaluations strongly suggest that the benefits of integration are worth the effort.[14]

The Imperatives of Community Policing

In the previous section, a summary was provided of the status of major IT elements of the policing environment. In most respects, that discussion centered on traditional aspects of information uses in policing, and considered what has transpired as the IT revolution has proceeded. The review indicated that some significant progress has been made, and that more can be expected. However, it also showed that IT changes in policing have yet to embrace many of the innovations that have come to be fairly commonplace in business and personal IT. It also attempted to convey a sense of the variability in IT from one jurisdiction to another and from one type of IT application to another.

What the section did not do was to look at the IT implications of the changes that have occurred in policing itself during the past 10 to 15 years. I turn to that issue now. The most significant of the changes are conceptual, and involve an effort to make policing more proactive and preventive in orientation. These trends have come to be known as community-oriented policing (often abbreviated as COP) and problem-oriented policing (often abbreviated as POP). Though there are important differences between these two constructs, the implications of the IT revolution are in my opinion similar for both of them, and I proceed in this article as if they were interchangeable from the IT point of view. Thus, when the terms community-oriented policing or COP are used, I would ask the reader to consider problem-oriented policing or POP to be included.

First, a brief definition of community-oriented policing is provided. Then an overview of the information domains that COP requires is undertaken. It is followed by consideration of the changes in types of analysis that are needed and the information systems that must be created for those changes to be accommodated.[15]

A brief definition of community-oriented policing

Though the terms "community-oriented policing" and "problem-oriented policing" have been on the tip of most law enforcement tongues for at least a decade,[16] and though a formal program of implementation of COP was enacted in the 1994 Crime Act,[17] generally accepted definitions of these approaches have proved somewhat elusive. It is not intended that this section of this IT article provide a resolution of the definitional issues (Greene 2000). The objective here is to consider the demands that community-oriented policing places on IT, and the corresponding challenges that the IT revolution places before COP/POP, however defined. The claim made, essentially, is that these demands and challenges apply in a broad fashion, and have more or less equal force regardless of the ultimate specification of the finer points of the COP/POP terms. Further, the claim is made that these demands and challenges are considerably greater under COP/POP than under the professional approach, and that, in fact, COP/POP cannot be effectively implemented unless they are satisfactorily met. The problem for the modern police department is how to do that.

To provide a framework for the IT discussion, a limited and quite generic review of the way in which community policing can be conceived (a) to differ from and (b) to be complementary to the "traditional" or "professional" models of policing is provided.[18] This is brief and the indulgence of the reader is requested with respect to the unsettled definitional issues.[19] A more detailed presentation is made of the information domains that COP/POP create and the way in which they are both dependent on and facilitated by the IT revolution.

COP is best conceived as a complementary approach to professional policing that redefines, extends, and expands the law enforcement approaches that have characterized policing for many decades. The Information Systems Technology Enhancement Project (ISTEP) notes:

> Community- and problem-oriented policing represent ways of providing public safety that are radically different from past practice. Under such models, the police are to be proactive, decentralized, and problem analytic. They are to use information more strategically while solving tactical problems. They are to be in greater communication with the public at large, integrated with other service delivery systems that impact the same geographic area, and internally more reflective and coherent. In sum, police agencies operating within the anticipated norms of COP/POP are to be thinking organizations able to adapt strategies and responses to an ever changing environment. (Dunworth et al. 2000)

A number of the key phrases in this statement signal the interdependence between COP/POP goals and IT that police departments use. In my view, antiquated IT systems will prevent effective implementation of COP/POP. Further, even state-of-the-art IT systems will not do the job unless they are focused on the new kinds of information that police departments must have. Police department IT must not only be faster, more reliable, easier, and so on. It also must be different. This section illustrates why and how this is so.

The information domains of community-oriented policing

The ISTEP view of policing carries with it certain information imperatives. If policing is to be different in the COP/POP fashion, how is this to be brought about? Part of the answer that ISTEP proposes is that new information previously seen as unnecessary has to be developed, and ways of using it that were not previously contemplated have to be found. The ISTEP project identifies seven key information domains that must be addressed for successful COP implementation:

- Community interface.
- Interorganizational linkages.
- Workgroup facilitation.
- Environmental scanning.
- Problem orientation.

- Area accountability.
- Strategic management.

Each domain merits a short exposition.

Community interface

This is one of the truisms about community-oriented policing, and under some definitions, is considered to be Community-Oriented Policing. The message is that the police should work in partnership with community organizations and individuals, and that a two-way exchange of information should be developed. When this is done, public attitudes toward the police change for the better (Dunworth and Mills, 1999), and departments benefit by getting improved information from the community (Rich 1998).

Interorganizational linkages

Under a community-oriented and problem-solving approach, the police must also work more closely with other government agencies (e.g., code enforcement, public works), nonprofit organizations, and the private sector. This means that law enforcement must use information systems maintained by other agencies and organizations and must share police information with them.

Workgroup facilitation

COP creates and imposes new or different information needs for officers and supervisors because of its focus on joint action and shared responsibility for geographic areas and problems. This responsibility spans segments of police activity that were often distinct under the professional model. For instance, robbery and patrol details may need to coordinate a problem-solving approach to a particular issue. Different shifts meet to pass information back and forth. The message is that temporal and functional distinctions between work groups need to be deemphasized and information sharing needs to be increased.

Environmental scanning

Under COP, careful attention must be paid to environmental issues, because problems need to be identified before they become stimulants to crime. This necessitates development and dissemination of data about such things as community characteristics, business cycles, land use, and crime patterns. For effective community-oriented policing, both police officers and police executives need substantial information about a wide range of existing and emerging issues and problems in the community.

Problem orientation

Much of traditional policing is incident driven. Departments react when crimes occur. These approaches cannot and should not be abandoned under community-oriented policing, but they are not sufficient for a successful COP approach. Information and analysis must be reoriented so they help officers and detectives to identify and analyze problems related to their new responsibilities, as well as to assess the effectiveness of responses after implementation.

The traditional idea that the demand for police services could be framed through the analysis of past calls-for-service data is no longer adequate.

Area accountability

COP emphasizes decentralized management of well-defined geographic areas. This mandates decentralizing command, control, and responsibility for those areas. Top command must be willing to do this. In addition, area commands must be given expanded and more sophisticated information about problems and resources than used to be the case. This information must permit an understanding of the range and kinds of problems that must be addressed: the knowledge, skills, and abilities of the workforce itself; the effectiveness of different kinds of interventions; and how to make resource allocation decisions that bring these elements together in the most effective way.

Strategic management

Community-oriented policing's greatest challenges probably arise in the context of strategic management. That COP retains all the management demands made by professional policing, and then adds more, is generally accepted. However, the magnitude and character of these new demands have not yet been systematically identified. At the least, top command must deal with three critical factors that were largely absent under the traditional approach: the needs and expectations of communities, links with other government as well as non-government agencies, and area accountability. The traditional idea that the demand for police services could be framed through the analysis of past calls-for-service data is no longer adequate. As noted earlier, acknowledging this does not and is not meant to dispense with the need to respond effectively to calls for service. COP adds something; it doesn't take something away. This makes the command function a good deal more difficult to perform.

The information needs of community-oriented policing

What this brief discussion of the information domains required by COP indicates is that the range and complexity of information needed for effective COP/POP are both significantly greater than is required to operate under the professional model. The ISTEP project summarized the differences in a way that is encapsulated in exhibit 1.

Most police departments would recognize the Professional Era information usage patterns as characterizing the way they have done business in the past. Few would be likely to assert that the information usage specified in the community-oriented policing column can be met by extant systems. In fact, meeting all the COP information demands that the ISTEP project identifies is a daunting undertaking that, even for the most ambitious and energetic department, would involve a substantial planning and design phase, significant new costs, and a considerable period of time.[20] Even if these obstacles are discounted, developing the information specified in the table would have been technically inconceivable nearly everywhere until the past few years. Even now, many jurisdictions would be unable to meet these demands. However, the IT revolution has created a situation in which the achievement of the COP information imperatives is technically feasible, provided jurisdictions can meet the challenges.

COP not only creates imperatives with respect to information assimilation, it also imposes analytic requirements that will necessitate new approaches and skills at all levels of the organization. Police departments have three reasonably distinct staffing levels: command executives, line supervisors and managers, and officers and detectives. Under the professional model, officers and detectives are the primary users of data about crime and suspects and make operational decisions in these areas. Supervisors and managers use quantitative data such as arrest productivity and case closure to evaluate subordinates, and sometimes use crime analysis reports to direct the tactics and targets of their units. Command executives make the primary use of analysis products to make strategic decisions about hiring, resource allocation, and deployment and to inform the public and civilian managers about specific events and overall crime trends and conditions.

To meet the information needs of these three groups, police departments have traditionally undertaken the following kinds of analyses:

- Crime analysis focusing on trends and patterns in ordinary street crime.
- Operations analysis focusing primarily on calls for service and the appropriate response to them.

Exhibit 1. Professional-era and COP information usage patterns

Information domain	Information usage patterns	
	Professional era	Community-oriented policing
Community interface	One-way flow of information; information incident oriented and obtained in reactive situations; narrow range of information desired (just the facts); interaction mainly limited to officers/detectives gathering raw data from crime victims and other complainants.	Two-way flow of information; proactive and problem-oriented information emphasized; wide range of information desired; all levels of police organization need both raw data about the community and analysis products; much greater emphasis on providing information to the community.
Interorganizational linkages	Little information sharing among police and other types of government as well as nongovernmental organizations; not seen as relevant or important.	Substantial information sharing; crucial to effective problem solving; two-way flow of information; information needed by line-level problem solvers as well as by managers and executives.
Work group facilitation	Not seen as very important; incident-oriented policing primarily an individual-level activity.	Problem solving and geographic focus enhance the importance of work groups; officers/detectives need more information to coordinate with their colleagues, and supervisors need more information to direct, control, and coordinate their subordinates, especially under conditions of functional diversity or temporal complexity.
Environmental scanning	Not seen as very important; primarily an executive-level activity; generally limited to serious crime issues in the community and major developments within the policing profession.	Seen as an important activity at all levels of the organization (beat area commanders, functional specialists, top executives); a officers, wide range of issues are seen as relevant (crime, disorder, drugs, fear, community relations, economic conditions, sociodemographic conditions, new technology, professional developments, etc.); an important area for analysis, not just raw data.

Exhibit 1 (continued)

Information domain	Information usage patterns	
	Professional era	Community-oriented policing
Problem orientation	Focus on incidents, not problems.	Policing and police-community partnerships focus primarily on problem solving; thus, raw data and, especially, analyses need to be organized and aggregated so they contribute to problem identification, problem analysis, the search for responses, and assessment; these data and analyses must be available to problem solvers—i.e., officers/detectives, citizens, community groups, other government agencies, and nongovernmental organizations, as well as police supervisors, managers, and executives.
Area accountability	Accountability primarily temporal (by shift) or functional (e.g., patrol, investigations); raw data and analysis not focused primarily on geographic areas.	Accountability primarily geographic; thus, data and analyses need to be geographically oriented; police officers/detectives, work teams, supervisors, commanders, and executives all need geographically based information to carry out their responsibilities effectively; citizens, community groups, other government agencies, and nongovernmental organizations also need geographically based information to effectively collaborate with the police in dealing with crime and disorder.
Strategic management	Commanders and executives rely on a narrow range of information (crime, calls for service) when analyzing service demands and designing service delivery systems; police management much more reactive, tactical, and defensive than strategic.	Police management more complex; wider range of objectives seen as relevant (crime control, order maintenance, fear reduction, public satisfaction, integrity, accountability); wider range of programs, policies, tactics, and strategies seen as potentially viable; thus, a more strategic approach to planning and management is required; this increases substantially the information needs of police executives.

Source: Cordner, Dunworth, and Greene 1998, 10–11.

- Intelligence analysis focusing on organized crime, drug trafficking, gangs, and repeat offenders.
- Administrative analysis focusing on a variety of organizational issues such as budgets, personnel turnover, fleet maintenance, and property inventory.

These requirements were supported by well-defined information systems:

Operations information systems. These include crime and arrest records, offender identification systems, stolen property records, and the like. Users are primarily officers and detectives, though the systems also are the foundation of aggregate police reporting to other systems such as UCR.

Command and control systems. These consist of calls-for-service management, emergency response to 911 calls, vehicle locator systems, etc. Mostly these function as aids to supervisors and managers in directing and controlling their subordinates, especially patrol officers.

Management information systems. These consist of a variety of databases pertinent to the internal management of the police organization, such as officer productivity, citizen complaints, and inventory. They are primarily administrative in orientation and are used by managers and executives in carrying out their administrative duties.

Under community policing, the traditional types of analysis remain important and cannot be ignored. They may, however, undergo significant change. Crime analysis, for example, will need to become more geographically focused and more attuned to the needs of officers and detectives as well as citizens and community groups. Operations analysis may become less concerned with response times and equalizing call-for-service workloads across shifts and more concerned with matching resources to problems.

In addition to such adjustments, community policing promotes two fundamental types of changes. First, supervisors and managers and, especially, officers and detectives have to make much greater use of analysis products. This is essential if they are to meet their newly delegated responsibilities in areas such as prevention, community and interagency partnerships, and problem solving, as well as to enhance their geographically based knowledge and responses. Second, external demand for police data and information by citizens, community groups, and others will greatly increase as these entities take on more responsibility, in partnership with the police, for controlling crime and disorder. The exposure of these external groups to police data and analysis represents a very significant expansion in the number of users of police information and, further, thrusts police staff at all levels into an unfamiliar informational environment.

To support such new information usage patterns, several new types of analysis become important:

- Community analysis, which looks at the characteristics of neighborhoods and communities, including conditions such as fear, disorder, and police-community relations, as well as socioeconomic and demographic characteristics.
- Problem analysis addressing specific issues that have been, or should be, targeted by officers/detectives and their collaborative partnerships.
- Program evaluations to assess the effectiveness of programs, tactics, and strategies.
- Policy analysis to consider longer range options and their consequences.

Command and control systems need to focus less on efficient incident handling and accountability for each minute of time, and more on effective problem solving and on accountability for conditions in geographic areas of responsibility.

Although each of these new types of analysis might serve multiple audiences, community analysis and problem analysis tend to produce information of particular value to COP operatives (officers, detectives, citizens, community groups, etc.), whereas program evaluation and policy analysis primarily serve the needs of managers and executives.

These adjustments in the type and application of analyses create a need for corresponding changes in the nature and type of information systems that police departments will have to generate and maintain. For example, operations information systems will need to supply COP operatives with more geographically based information, more information about problems and not just incidents, and more analysis products instead of just raw data. Command and control systems need to focus less on efficient incident handling and accountability for each minute of time, and more on effective problem solving and on accountability for conditions in geographic areas of responsibility. Finally, management information systems need to focus more on substantive issues and on quality rather than just on internal administrative processes.

In addition to these expansions of existing systems, COP creates a need for at least three other new kinds of information systems:

Geographic information systems. Systems that relate data to locations and that result in maps and other products pertinent to identifying and analyzing geographically based problems and conditions, and the way they change over time.

It would seem that the technology revolution has been a prerequisite to effective community-oriented policing, and that at least some of the confusion surrounding the definition of COP derives from an inadequate grasp of the information imperatives that COP imposes.

Problem-solving information systems. Databases and systems that capture information about completed and ongoing problem-solving efforts and that aid officers and citizens in identifying, analyzing, and responding to substantive problems in communities.

External information systems. Systems that aid the police in obtaining data and information from other organizations and from the public, and that also aid those entities in obtaining information from the police.

IT implications for police departments

The discussion presented above leads to certain inevitable conclusions that have enormous implications for community-oriented policing and the police departments that seek to implement it:

- First, COP has features that have far-reaching implications for information gathering and processing. These include the need for citizen input, a much expanded geographic focus of policing work, a commitment to prevention, partnerships with community organizations and agencies outside the criminal justice system, environment scanning, problem solving, and new management strategies.
- Second, COP changes the types of information needed by frontline police officers as well as by managers and executives, and it also creates new sets of potentially demanding information users: citizens, community groups, other government agencies, and nongovernmental organizations.
- Third, COP significantly changes the types of analysis that police departments must perform as well as the ways in which the analyses are organized and disseminated.
- Fourth, existing police information systems will need to be adjusted and new systems will need to be developed to provide the data required by analysts and by COP operatives.
- Fifth, specific new domains of police information are necessary, not just desirable, for the successful implementation of community-oriented policing.

Clearly then, community-oriented policing creates both new and qualitatively different information needs for police agencies and their COP partners. The technology revolution appears to have created the tools and techniques to meet these needs. In fact, it would seem that the technology revolution has been a prerequisite to effective community-oriented policing, and that at least some of the confusion surrounding the definition of COP derives from an inadequate grasp of the information imperatives that COP imposes. Without taking the imperatives into account, it would be difficult to see how COP is all that different from the professional model.

A mistake, though, would be to assume that the only thing necessary to satisfy these new needs is the advanced information processing technology that has come into being. Besides technological solutions, police departments seeking to fully implement COP will have to deal with at least three other issues specific to the policing environment:

- Reconceptualizing the domains of police-related information.
- Locating and gathering new types of policing data.
- Analyzing data and producing policing information that is timely and relevant.

These three elements of the solution to the information-related needs created by COP will, if anything, be more challenging than the advanced technological aspects of the situation. Departments that fail to fully take them into account are unlikely to successfully implement community policing, no matter how firm the department's commitment to the concept.

Outlook for the 21st Century

To characterize the IT developments of the past 50 years as a revolution is no overstatement, in my view. The changes in IT that have taken place *are* revolutionizing our lives. And, even more rapid change is surely at hand. For the foreseeable future, we can expect the pace of IT innovation and development to continue to be extraordinarily rapid. This will be particularly noticeable within what can be thought of as the current IT paradigm. For instance, further miniaturization and increased speed of components will likely characterize most advances.[21] Memory and storage capacity of machines will increase even as the machines themselves shrink in size. As long as monopolistic or oligopolistic conditions do not prevail, the unit cost of these developments will continue to fall as installations proliferate.[22] We are able to do now what was prohibitively expensive 10 years ago. In the early 21st century, it will be possible to routinely do for a few hundred dollars what is technically or financially infeasible now.

Though, as I have tried to illustrate in this article, the law enforcement world is not at the forefront of the revolution (and probably should not be), it is nevertheless moving inexorably in the same direction. The IT revolution is bringing change that cannot be avoided in law enforcement's way of doing business. I would argue that it should not be avoided, because, properly managed, the change can be beneficial. But, as law enforcement makes these changes, there will be side effects. Some of these will probably also be beneficial, but some bring risk.

In this final section, I will first summarize in very general terms what I think law enforcement—police departments in particular—will face. I will then briefly review two likely side effects, one almost certainly positive, one possibly negative. The former is the probable advancement in policy-relevant knowledge that can be derived from the expanded information that police departments will have available. The latter is the risk of misuse of the information, and the invasion of privacy that might ensue.

The information future for policing

In the 21st century, officers on the street or in their cars will have instantly available at the touch of a button more information than can presently be mustered in most police department headquarters. For example, wireless transmission of images as well as text or data will become commonplace. Maps, scene diagrams, photographs, paintings, sketches, fingerprints—all will move back and forth effortlessly. Handheld DNA scanners are being predicted within 10 years (McCullagh 1999). On the spot DNA checks will become possible through wireless transmission of the scanner's reading and an instantaneous comparison with millions of DNA records in a central data bank.

The major question for police departments will not be whether information at this level of sophistication is going to be available. The question will be whether it can be used effectively.

For this to happen in a way that is helpful and useful, policing will have to change. The way things are done will have to be different. New kinds of information will have to be processed and incorporated into police strategy and tactics. Officer training will require redefinition and reorientation.

Of course, the basics of law enforcement will have to be retained. A significant portion of future criminal activity will have characteristics similar to criminal activity of the past. A robbery will still involve a robber and a victim, and police officers will still need to respond to calls for service, especially emergency calls, in the way they always have. In this sense, policing will need to

retain the traditional elements of law enforcement, while adding new approaches and techniques that at present are either nonexistent or in their infancy.

One way to look at COP and POP is that they are the first wave of the new policing. These approaches have not been implemented in full in any comprehensive sense anywhere, but a number of departments are pushing the concepts forward. When this is done effectively, different and expanded IT and IT utilization are at the forefront of the effort. The point was made in the section "The Imperatives of Community Policing" that the information imperatives created by COP are just that: imperatives. If they are not heeded, COP will not be implemented, or at least will meet little more than a small fraction of its potential.

Yet, the impediments to adoption of COP's IT requirements are substantial. Significant investments of resources, time, and money will all be required, and, perhaps most important, police departments will have to change. In some senses, several catch-22 problems must be resolved.

For one thing, it is difficult to see the benefits of the new IT until it is in place and operational. But it will never be in place and operational if departments do not accept its benefits on faith, because the path outlined previously is very difficult to successfully implement on a piecemeal basis. This makes it highly desirable for the Federal Government to promote the incorporation of new technology into departmental operations through any means that are available: financial support, training and technical assistance, widespread dissemination and promulgation of the benefits of advanced IT, conferences, and so on.[23]

There is another catch-22 in the interplay between design and cost. It is well known that development and design issues are difficult and expensive to overcome. It is not uncommon to see departments struggle with the design issues surrounding automation for a number of years. It is also easy to find departments that have had significant problems with vendors who proved unable to deliver the system promised. Given this, it is perhaps not realistic to expect departments to accept turnkey systems. There will be an inevitable desire to tailor new systems to idiosyncratic requirements and standards. The result would be a series of one-of-a-kind systems, which would constitute an astronomically expensive IT trajectory for policing as a whole, as well as for individual departments. Yet there is a powerful belief in most departments that their situation is unique. It will be difficult to reconcile these two tendencies.

Another problem exists with respect to officer training and capabilities. What do we want a police officer to be? It was already noted above that the response capability that is loosely defined as "traditional" policing needs to be retained. Can the officer who does that well also be the officer who processes and uses

the new kind of information that is going to be available? The answer to this question is not clear. For instance, being comfortable using or even perhaps writing a Visual Basic® program to tease out the nuances of crime patterns in a precinct is not going to seem very pertinent to an officer confronting an armed burglar in a dark alley. The question is: Shall we, should we, expect a police officer to take care of both of these kinds of tasks? Is that a desirable goal? A feasible goal? Does this require a police officer for all seasons, and is such an officer available? That is a matter for careful debate that is beyond the scope of this article, but is something that must be addressed.

However, if these and probably other issues that I have not touched on or thought about are resolved, then the biggest remaining problem facing police departments as IT advances is effective utilization. A comparison can be drawn to automated word processing, which, so far, is probably the most frequently used aspect of the IT revolution. Sophisticated word processing software is now provided free with many PC purchases, and, if not free, can be obtained at relatively low initial cost. But, many users are able to employ only small portions of the word processing capability that is accessible to them. The instruction manuals are inches thick, and most users would not consider the software they access to be user friendly, except for the most simple and rudimentary tasks. Even the individuals who make a living using the software (secretaries, writers, etc.) usually acknowledge that they have mastered only a portion of the capacity of their programs.

Expanded IT in police departments will face problems that are at least as large. The danger will be that officers will not have the time, inclination, training, and disposition to learn what the IT demands, absorb what it offers, and incorporate it effectively into their daily work. In my opinion, this is the single biggest IT challenge for police departments.

Knowledge and risk

As noted above, the effects of IT advances in police departments will have repercussions beyond the operational needs of the departments themselves. One such side effect is a potential increase in knowledge about crime, criminals, and the criminal justice system. Most of us would consider this to be a benefit. But knowledge can be used for ill as well as good, and this risk looms particularly large at a time when misuse of personal data and assaults on personal privacy are already considered by many to be a major societal problem. We need to ask ourselves a number of questions. What is the balance between these two facets of the IT revolution in policing? Does the good outweigh the bad? Is there a way to maximize the former and minimize the latter? I will not presume to provide answers to these questions, but I will try to outline their dimensions.

Better information gathering, processing, and dissemination offers benefits in at least four distinct areas:

- **Strategic and tactical decisionmaking by police departments.** This simply reiterates the theme that has been developed during this article. The more information a police department has and the better its methods of processing that information, the greater the likelihood that strategic decisionmaking will be rationally based. Further, improvements in IT serve as a tactical force multiplier—the officer on the street will be more effective, and more public service will result from an 8-hour shift.

- **Cross-jurisdictional cooperation and collaboration.** Good information will create a better foundation for effective cross-jurisdictional interaction. Departments will be able to make a more effective contribution concerning their own knowledge and experience, and will also be able to better utilize information provided by other jurisdictions. Cooperation and collaboration on matters of common interest will be enhanced.

- **Aggregation at State, regional, and national levels.** Aggregate statistics such as those produced by UCR are no better than the quality of the data provided by individual police departments. Improved data at the local level leads to improved aggregations at higher levels. Better compilations and more accurate statements of trends will be the result.

- **Stimulation of research.** A common complaint among researchers is that the research they do is not often used. There are a number of reasons for this. Some are ideological and not susceptible to easy change (Travis 1996). Others are a consequence of the informational impediments that researchers have characteristically faced. These have tended to mean that research costs too much, takes too long, and produces results that are too often equivocal (Dunworth, Haynes, and Saiger 1997). This is particularly true of research that has focused on police departments.[24] However, with more dependable and more comprehensive computerized data, policing research will be better positioned to increase our basic knowledge about crime, and inform policymaking at local, State, and national levels.

Few would resist the assertion that these improvements are desirable. Many would agree that they are necessary. Looked at from that point of view, these are side effects of the IT revolution that we can applaud. But we cannot leave it at that. We have to look at the other side of the coin. As information about crime, criminals, and suspects becomes more detailed and more easily accessible and manipulable, we must consider whether potential misuses of such information are possible, and if so what we should do about it.

I think there are three areas where the proliferation of information could lead to problems. These all involve matters of privacy and security of individuals.[25]

Inaccuracy of data

As more and more information is accumulated about individuals, it becomes increasingly important that the information be accurate and dependable. This is true not only in the law enforcement world. None of us want our good credit records to be reported as bad, for example. But, when we are speaking of a law enforcement context, the negative effects of inaccurate or incomplete data about individuals can be devastating. Many police departments collect data on possible gang members. Some use a series of markers to assess likely gang membership (clothing, nicknames, tattoos, associates). Above a certain threshold (e.g., perhaps three out of four "hits"), the person is flagged as a gang member. There may be no known criminal activity associated with such a person, but the person may subsequently be treated as if there were. An argument can be made that the potential for the prevention and control of crime is enhanced by this procedure. But, it is not necessary to be anti-law enforcement or a gang sympathizer to be troubled by the approach. What if the information is inaccurate?

Unrestrained official use

A lot of the information about persons that gets into police files is developed through investigation of complaints and crimes. Such development is a normal and proper exercise of police power and responsibilities. When this information is paper based, access to it tends to be limited. Inside the department, neither civilian nor sworn staff spend their time rummaging through files about cases with which they personally have no association. Departments would not, for example, copy an investigative file and send it out to another agency or a business without a very good reason. But, when such information becomes computerized, it is an easy matter to apply different standards. It becomes a simple matter for data on individuals to be made available to other law enforcement agencies, to other public agencies that request it, to businesses, and perhaps even to individuals. All that is needed is for an officially approved reason to exist. The reason might be to check a would-be gun purchaser under the Brady law; to approve an application for a driver's license; to make a decision about a job applicant; or to

The risk at present seems to be that the rapidity of the movement toward computerization will outstrip the establishment of appropriate protections of individual privacy.

decide whether to rent an apartment. Some of these seem obviously legitimate uses of police data; some seem questionable. Either way, once transmitted, control of the information is lost. The information could go anywhere and be used for any purpose. Is this what we want?

The human mind is advancing, it is producing new knowledge and capabilities at an astounding rate, and police departments must keep up. The IT revolution and police department utilization of the capacity it generates is a journey, not a destination.

Unauthorized access

A paper file in a police department filing cabinet or an officer's desk drawer has a symbolic boundary around it. Not only is it inaccessible to outsiders, it is not likely that unauthorized insiders will go looking through it. Such barriers disappear when the file is computerized. Insiders and outsiders have opportunities to get to it, sometimes without creating any record of access. If there is any doubt about this, it is only necessary to reflect on the number of known breaches of supposedly secure national databases by hackers. If hackers can get into files that are protected by national security systems, it is hard to see why computerized police files will not be extraordinarily vulnerable. Obviously, this is not what any police department (or any other law-abiding citizen) would want. But, it is hard to be confident that it could be stopped.

What this brief discussion suggests is that critical concerns exist about data quality and integrity, and about internal and outside access to sensitive information. Unrestrained or improper access seems certain to lead to abuses, and so deserves very careful attention. It may well be that dealing with these concerns may bring a limit to the amount and type of information that is considered proper to maintain in computerized police files, and/or in safeguards that may result in less than optimal technical use of the burgeoning IT capability. The risk at present seems to be that the rapidity of the movement toward computerization will outstrip the establishment of appropriate protections of individual privacy.

Conclusion

Among the many timeless observations made by Thomas Jefferson, one strikes me as having particular relevance to the policing response to the IT revolution. On July 12, 1816, Jefferson wrote a letter to Samuel Kercheval, an extract from which is reproduced on one of the chamber walls of the Jefferson Memorial. Jefferson said:

> I am not an advocate for frequent changes in laws and constitutions, but laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with the change of circumstances, institutions must advance also to keep pace with the times. We might as well require a man to wear still the coat which fitted him when a boy as civilized society to remain ever under the regimen of their barbarous ancestors.

Jefferson, of course, was making a very general point with this statement. But, taking a few liberties, I would propose that the situation he denotes is precisely the one facing police departments. The human mind is advancing, it is producing new knowledge and capabilities at an astounding rate, and police departments must keep up. The IT revolution and police department utilization of the capacity it generates is a journey, not a destination. It may be best conceived as a journey that has stops along the way. A certain amount of time will be spent at each stop, during which the features and amenities available at the stopping point are used, hopefully to good effect. However, sooner or later the features and amenities will become outmoded and inadequate. Then the journey will have to be resumed, and travel to the next stop will be required. At that next stop, what is available will be more advanced and, potentially, more helpful. It will also be more demanding. It will probably introduce more risk.

This evolving process will never end. There will not be a point at which the ultimate destination has been reached. The amount of time spent at each stop is probably declining as the interval between each new advance diminishes. Police departments are going to be continually challenged to adapt to changing circumstances, and, to a very significant extent, these circumstances are going to be circumscribed by information and the technology used to manage it.

In conclusion, we must acknowledge that IT and its uses by law enforcement agencies are continually expanding and seem virtually unlimited. The challenge for police departments will be to take the (risky) step of dynamically embracing the new potential.

I have been assisted in this article, particularly in the discussions of the current status of information technology and of the application of IT to community-oriented policing, by the information contained in a number of presently unpublished working papers prepared by Abt Associates staff members Gary Cordner, Peter Finn, Jack Greene, Kristen Jacoby, Julia Kernochan, Tom Rich, and Shawn Ward in connection with the Information Systems Technology Enhancement project, of which I am the project director. With gratitude, I have made use of

the background materials contained in those papers, although the individuals named are not responsible for, and do not necessarily agree with, the interpretations I have made and the conclusions I have drawn.

Notes

1. In this paper I will use IT as a general shorthand term to designate information technology and its associated hardware and software elements.

2. Asserting that the revolution has taken place in the past five decades is a practical construct that focuses attention on the development and contribution of the desktop computer, which was made possible by the invention of the transistor in 1947. It is not meant to do a disservice to earlier pioneers in the field, whose efforts were prerequisites for the desktop and the IT foundation that we take as commonplace today. This includes an array of seminal conceptual and practical developments, including, but not necessarily limited to, the following: Blaise Pascal's "Arithmetic Machine" (1642); Gottfried Leibniz's "Stepped Reckoner" (1694); Charles Babbage's "Analytical Engine" (1835); George Boole's binary logical operators (1859); Herman Hollerith's punched cards (1886); the Harvard Mark I created by Howard Aiken and IBM (1939); the ENIAC (Electronic Numeric Integrator and Calculator) created by J. Presper Eckert and John W. Mauchly (1946); the stored program concepts developed by John von Neumann in 1946 that in many respects opened the door to the logic underlying digital computers; and finally, of course, the development that ultimately made desktops and laptops a practical reality—the invention of the transistor in 1947 by Walter Brattain, John Bardeen, and William Shockley.

3. For an excellent overview of IT developments and their relevance to the justice system, see Coldren (1996). See the many other articles in Scherpenzeel (1996) for a comprehensive examination of computerization and criminal justice issues.

4. Decker (1978) provides a useful, though brief, overview of the historical development of statistical reporting on crime.

5. A helpful summary of the UCR system can be found on the FBI Web page at http://www.fbi.gov/ucr/ucrquest.htm. The page provides responses to frequently asked questions about UCR, and is an excellent introduction to the topic. The bibliography to this article contains an extended list of references. An additional crime reporting system that has the potential for at least supplementing and perhaps replacing UCR was proposed and adopted in the mid-1980s. It came to be called the National Incident-Based Reporting System and is discussed later in this article.

6. Publications on the Wickersham Commission are numerous. For an Internet reference, see the University Publications of America Web site at http://www.upapubs.com/guides/wickersham.htm. This excerpts from Walker (1997). For other selections, see Calder (1993) and the National Commission on Law Observance and Enforcement (1931).

7. The most significant of these was the Cleveland Survey of Criminal Justice. Led by Felix Frankfurter and Roscoe Pound, this inquiry produced *Criminal Justice in Cleveland* (Cleveland Foundation 1922).

8. A 14th report, on a particular case of abusive police behavior, was suppressed at the time of the original publications but was later released.

9. A review of Federal legislation from 1968 through 1994 can be found in Dunworth et al. (1996). A more focused assessment of the legacy of the 1967 Commission is provided by Tonry (1997).

10. LEAA was officially terminated on April 25, 1982 (U.S. Senate 1983, 3). A vast literature on LEAA exists. For an entry to it, see Allinson (1979), Diegelman (1982), and Feely and Sarat (1980).

11.The long-term future of COPS is in some doubt at the time of writing (late fall 1999). Budget negotiations for FY2000 appropriations led to a significant reduction in funding for COPS. Given the highly political nature of the "100,000 Cops on the Street" program of the Clinton administration, it is difficult to predict what will happen to this office when its statutory life ends in fall 2000. Some are predicting that, at the least, its status as an independent agency within the U.S. Department of Justice will be lost.

12. I refer here to the Arrestee Drug Abuse Monitoring (ADAM) program, the successor to the Drug Use Forecasting (DUF) program, which systematically collects and analyzes urine samples from arrestees in jails in 35 U.S. cities and then correlates the results with interviews of those arrestees.

13. As of May 1997, in addition to the 10 States certified to report NIBRS data, 24 States were testing NIBRS and another 8 States were developing NIBRS programs for further exploration. In the next few years, Phase III of the NIBRS Project will seek to encourage NIBRS' adoption through several measures: devoting resources to instituting NIBRS reporting at several large local law enforcement agencies; providing technical assistance to agencies desiring to implement NIBRS; building "national dialogue" on NIBRS in an effort to increase awareness and understanding of the program; and producing a video-tape demonstrating effective use of NIBRS data, using local agencies as exemplars.

14. See, for example, North Carolina Department of Correction (1998) and Stratton (1993). The North Carolina site documents North Carolina's Justice Wide Area Network (JWAN). JWAN, located in Hendersonville, North Carolina, links the town's probation office, sheriff's department, police department, district attorney's office, day reporting center, and other criminal justice agencies. Completed with a grant from the Governor's Crime Commission, this relatively simple network relies on laptop computers and custom adaptations of common software. Officers are able to report electronically, share photos of probationers with other agencies, and search for offenders according to physical characteristics. Although officers now spend more time on reporting, they are more mobile and the information they provide is much more helpful to others in the office.

Stratton (1993) discusses the All County Criminal Justice Information Network (ACCJIN) in Contra Costa, California, established in 1990, which links 23 preexisting criminal justice information systems into a network. The network is composed of two message-switching computers, a private packet-switching setup, and customized common software applications. The information system has radically improved all areas of criminal justice work in the county, from jail administration to dispatching to communication among offices (previously accomplished by fax and photocopy). The program's successful completion is traced to good communication, adequate funding, and effective definition of criteria.

15. This section draws heavily from work done under the Information Systems Technology Enhancement Project (ISTEP), of which I am the project director. This COPS project is examining how police departments are adapting to the new IT that has become available in the past decade or so. ISTEP is referenced liberally, and the references identify a variety of earlier papers that are available in mimeograph on request. In particular, this section depends on an earlier version of the conceptual foundation of the ISTEP project that was placed in the public domain in mimeograph form at a COPS conference held in Washington, D.C., in November 1998 (Cordner, Dunworth, and Greene 1998). Copies of that document are available on request. A more recent report on ISTEP, published by the COPS office in May 2000 is entitled "Police Department Information Systems Technology Enhancement Project." It contains the conceptual foundation, five case studies, and a cross-site synopsis of significant issues. It can also be obtained from the COPS Web site (http://www.usdoj.gov/cops/index.html), cross referenced under ISTEP.

16. For early discussions of community-oriented policing and problem-oriented policing, see Goldstein (1979), Greene and Mastrofski (1988), Manning (1984), Police Foundation (1981), and Trojanowicz (1983).

17. The Violent Crime Control and Law Enforcement Act of 1994 established direct Federal-to-local aid for community policing, which completely bypassed traditional block grant mechanisms for such Federal aid (e.g. the Byrne Formula Grant Program, the Local Law Enforcement Block Grant Program). In addition to support for the hiring of police officers, the Act also authorized expenditures for information systems technology (manifested in the COPS MORE program).

18. There is no intention here to suggest that COP or POP runs counter to tradition or is nonprofessional. A differentiating term is needed and, in this article, the designation "professional" will be used to identify the era of policing that saw the introduction of professional standards and training for police officers. There is also no intention to suggest that COP/POP makes such professional standards unnecessary or obsolete. Just the opposite, in fact. COP/POP is considered to be complementary to the professional approach. For further discussion of this topic, see Larson (1990).

19. Much of the content of this section is drawn from work done for the COPS ISTEP project. A number of presentations of this work have been made at recent COPS and

National Institute of Justice (NIJ) conferences (e.g., the COPS/NIJ National Conference on Community Policing, held in Washington, D.C., November 1998), and earlier discussions have been written up. See, in particular, Cordner, Dunworth, and Green (1998) and Greene, Rich, and Ward (1999). Publication of revised versions of these works by COPS is forthcoming.

20. Phase 1 of the ISTEP project produced five case studies in addition to Cordner, Dunworth, and Greene (1998) and Greene, Rich, and Ward (1999).These are based on the experiences of the five police departments that agreed to contribute their IT insights and experiences to the ISTEP work: Charlotte-Mecklenburg, North Carolina; Hartford, Connecticut; Reno, Nevada; San Diego, California; and Tempe, Arizona. Some of these departments exemplified the careful, costly, and time-consuming approach that community-oriented policing IT requires. All Phase I ISTEP reports have been published by COPS (May 2000) and also are accessible through the COPS Web site.

21. Gordon Moore, one of the founders of INTEL, predicted in what has come to be known in the industry as "Moore's Law" that transistor density and speed would double every 12 months. From about 1950 until 1965, this was true. Since then, doubling has taken place about every 18 months.

22. Laptops, like desktops, have been steadily declining in price, while features and power have been steadily increasing. Though common sense suggests that there must be some end, or at least slowing, in these trends, there is little evidence that slowdown has begun yet.

23. This process is already under way. The Office of Community Oriented Policing Services is planning a series of IT technical assistance conferences during the first 6 months of 2000. The objective will be to provide assistance to the departments receiving COPS funding under the COPS MORE program, which supports a variety of initiatives, IT development being one of them.

24. For an illustration of the particular difficulties associated with policing research, see Dunworth and Saiger (1994). This study began as a five-city inquiry using police department data. Two of the five cities had to be dropped because the data did not support the spatial analysis that the project performed. In the others, Thomas maps were used to manually correlate police department data with housing development boundaries. In a more recent project, the advances made in police department data are illustrated by the fact that longitude/latitude coordinates were developed for more than 90 percent of specific incidents contained in citywide databases in five cities for which such databases were obtained. See Dunworth et al. (1999).

25. A cross-national discussion of privacy and security issues can be found in Csonka (1996).

References

Allen, Gary. 1997. 311: One number, two reasons for calling. *DISPATCH Monthly* (September). Retrieved 30 March 2000 from the World Wide Web: http://www.911dispatch.com/web_story/stories_97/story-3-sep97.html.

Allinson, Richard S. 1979. LEAA's impact on criminal justice: A review of the literature. *Criminal Justice Abstracts* 11:608–648.

Barton, S.J. 1999. *Survey of State criminal history information systems, 1997.* NCJ 175041. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

Bezdikian, V., and C.L. Karchmer. 1996. *Technology resources for police: A national assessment.* Washington, D.C.: Police Executive Research Forum.

Brady, T. 1997. The evolution of police technology. In *Technology for community policing.* Conference Report, NCJ 163601. Washington, D.C.: U.S. Department of Justice, National Institute of Justice and Office of Community Oriented Policing Services.

Calder, James D. 1993. *The origins and development of Federal crime control policy: Herbert Hoover's initiatives.* Westport, Connecticut: Praeger.

Cleveland Foundation. 1922. *Criminal justice in Cleveland.* Cleveland: Cleveland Foundation.

Coldren, J. David. 1996. Change at the speed of light: Doing justice in the information age. In *Computerization in the management of the criminal justice system. Proceedings of the Workshop and the Symposium on Computerization of Criminal Justice Information at the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,* edited by Richard Scherpenzeel. HEUNI Publication Series no. 30. Helsinki/The Hague: European Institute for Crime Prevention and Control.

Cordner, Gary, Terence Dunworth, and Jack Greene. 1998. Police Department Information Systems Technology Enhancement Project: Conceptual framework. Working paper, Abt Associates, Cambridge, Massachusetts.

Csonka, Peter. 1996. Council of Europe and data protection: Free flow of information versus privacy. In *Computerization in the management of the criminal justice system. Proceedings of the Workshop and the Symposium on Computerization of Criminal Justice Information at the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,* edited by Richard Scherpenzeel. HEUNI Publication Series no. 30. Helsinki/The Hague: European Institute for Crime Prevention and Control.

Decker, S.H. 1978. Evolution of crime statistics as a police problem. *Journal of Police Science and Administration* 6 (1) (March): 67–73.

Diegelman, Robert F. 1982. Federal financial assistance for crime control: Lessons of the LEAA experience. *Journal of Criminal Law and Criminology* 73:994–1011.

Dunworth, Terence, Gary Cordner, Jack Greene, Timothy Bynum, Scott Decker, Thomas Rich, Shawn Ward, and Vince Webb. 2000. Police department Information Systems Technology Enhancement Project ISTEP. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

Dunworth, Terence, and Gregory Mills. 1999. *National evaluation of Weed and Seed*. Research in Brief, NCJ 175685. U.S. Department of Justice, National Institute of Justice.

Dunworth, Terence. Forthcoming. *The national evaluation of the Youth Firearms Violence Initiative*. Research in Brief. U.S. Department of Justice, National Institute of Justice.

Dunworth, Terence, Scott Green, Peter Jacobson, and Aaron J. Saiger. 1996. *National assessment of the Byrne Formula Grant Program: The Anti-Drug Abuse Act of 1988: A comparative analysis of legislation. Report no. 2.* Research Report, NCJ 163382. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Dunworth, Terence, Peter Haynes, and Aaron J. Saiger. 1997. *National assessment of the Byrne Formula Grant Program.* Research in Brief, NCJ 162203. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Dunworth, Terence, and Aaron J. Saiger. 1994. *Crime in public housing: A three city analysis.* Research Report, NCJ 145329. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Ellison, John. 1996. NENA's response to President Clinton. Letter from John Ellison, President, National Emergency Number Association, to President William J. Clinton, 2 August. Retrieved 30 March 2000 from the World Wide Web: http://www.nena9-1-1.org/president.htm.

Feely, Malcolm, and Austin Sarat. 1980. *The policy dilemma: Federal crime policy and the Law Enforcement Assistance Administration.* Minneapolis: University of Minnesota Press.

Foote, Joseph. 1998. An overview for the Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and Administration of Justice. In *The challenge of crime in a free society: Looking back looking forward. Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and Administration of Justice.* Research Forum, NCJ 170029. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs.

Gapay, L. 1992. Pen computing minimizes paperwork. *Law Enforcement Technology* 19 (4) (April): 18–19, 50–51.

Goldstein, H. 1979. Improving policing: A problem oriented approach. *Crime & Delinquency* 25 (2): 236–258.

Goodman, M.D. 1997. Working the Net: Exploiting technology to increase community involvement and enhance service delivery. *Police Chief* 64 (8) (August): 45–53.

Greene, J., and S. Mastrofski, eds. 1988. *Community policing: Rhetoric or reality.* New York: Praeger.

Greene, Jack, Thomas Rich, and Shawn Ward. 1999. Police Department Information Systems Technology Enhancement Project: Cross-site report. Working paper, Abt Associates, Cambridge, Massachusetts.

Handgun Violence Prevention Act. U.S. Public Law 103–159. 103d Cong., 1st sess., 30 November 1993.

Kennedy, D.M. 1993. *The strategic management of police resources.* NCJ 139565. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Larson, R.C. 1990. *Rapid response and community policing: Are they really in conflict?* East Lansing: Michigan State University, School of Criminal Justice, National Center for Community Policing.

Lorow, C. 1997. 3–1–1: It's one of several non-emergency options. *APCO Bulletin* (November). Retrieved 30 March 2000 from the World Wide Web: http://www.apcointl.org/bulletin/bull97/november/ november8.html.

Mamalian, C.D., and N.G. La Vigne. 1999. *The use of computerized mapping by law enforcement: Survey results.* Research Preview, FS 000237. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Manning, P. 1984. Community policing. *American Journal of Police* 3 (2): 205–227.

Manning, W.W. 1997. Should you be on the Net? *FBI Law Enforcement Bulletin* 66 (1) (January): 18–22.

Manson, D.A., D.K. Gilliard, and G. Lauver. 1999. *Presale handgun checks, the Brady interim period, 1994–98.* NCJ 175034. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

McCullagh, Declan. 1999. The marker of a criminal. *Wired,* 19 November. Retrieved 30 March 2000 from the World Wide Web: http://www.wired.com/news/politics/0,1283,32626,00.html.

National Child Protection Act of 1993. U.S. Public Law 103–209. 103d Cong., 1st sess., 20 December 1993.

National Commission on Law Observance and Enforcement. 1931. *Reports.* Washington, D.C.: U.S. Government Printing Office.

National Partnership for Reinventing Government. 1999. *Providing 21st century tools for safe communities: Report of the Task Force on Crime Mapping and Data-Driven Management.* Washington, D.C.: U.S. Department of Justice.

911 Dispatch Services, Inc. 1996. California 911 cellular has nearly collapsed. *DISPATCH Monthly* (October). Retrieved 30 March 2000 from the World Wide Web: http://www.911dispatch.com/web_story/stories_96/story-4-oct96.html.

North Carolina Department of Correction. 1998. Officers use technology to work more closely with police. *Correction News* (March). Retrieved 30 March 2000 from the World Wide Web: http://www.doc.state.nc.us/NEWS/983news/JWAN.htm.

Paynter, R.L. 1998. Internet connections. *Law Enforcement Technology* 25 (8) (August): 28–32.

Poggio, E.C., S.D. Kennedy, J.M. Chaiken, and K.E. Carlson. 1985. *Blueprint for the future of the Uniform Crime Reporting program. Final Report of the UCR Study.* NCJ 98348. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

Police Foundation. 1981. *The Newark foot patrol experiment.* Washington, D.C.: Police Foundation.

President's Commission on Law Enforcement and Administration of Justice. 1967. *The challenge of crime in a free society.* Washington, D.C.: U.S. Government Printing Office.

Reuland, M.M. 1997. *Information management and crime analysis: Practitioners' recipes for success.* Washington, D.C.: Police Executive Research Forum.

Rich, T.F. 1998. Crime mapping by community organizations: Initial successes in Hartford's Blue Hills neighborhood. In *Crime mapping case studies: Successes in the field*, edited by N.G. La Vigne and J. Wartell. Washington, D.C.: Police Executive Research Forum.

———. 1996. *The Chicago Police Department's Information Collection for Automated Mapping (ICAM) Program.* Program Focus, NCJ 160764. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

———. 1995. *The use of computerized mapping in crime control and prevention programs.* Research in Action, NCJ 155182. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Roberts, D.J. 1998. *Integrated justice information systems for State and local jurisdictions: An overview of planning activities for the Office of Justice Programs, U.S. Department of Justice.* Washington, D.C.: U.S. Department of Justice, Office of Justice Programs.

———. 1997. *Implementing the National Incident-Based Reporting System: A project status report.* NCJ 165581. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

Scherpenzeel, Richard, ed. 1996. *Computerization in the management of the criminal justice system. Proceedings of the Workshop and the Symposium on Computerization of Criminal Justice Information at the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.* HEUNI Publication Series no. 30. Helsinki/The Hague: European Institute for Crime Prevention and Control.

Stratton, N.R.M. 1993. Birth of an information network. *FBI Law Enforcement Bulletin* 62 (2) (February): 19–22.

Sulewski, K.D. 1997. Faxback response: Previous question: How has the Internet helped your agency? *FBI Law Enforcement Bulletin* 66 (1) (January): 23–25.

Tonry, Michael. 1997. Building better policies on better knowledge. In *The challenge of crime in a free society: Looking back looking forward. Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and the Administration of Justice.* Research Forum, NCJ 170029. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Travis, Jeremy. 1996. Criminal justice research and public policy in the United States. In *Computerization in the management of the criminal justice system. Proceedings of the Workshop and the Symposium on Computerization of Criminal Justice Information at the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,* edited by Richard Scherpenzeel. HEUNI Publication Series no. 30. Helsinki/The Hague: European Institute for Crime Prevention and Control.

Trojanowicz, R. 1983. An evaluation of a neighborhood foot patrol program. *Journal of Police Science and Administration* 11 (4): 410–419.

U.S. Department of Justice, Office of Community Oriented Policing Services. 1997. COPS Facts: 3–1–1 national nonemergency number. Washington, D.C.

U.S. Department of Justice, Office of Justice Programs. 1998. *The challenge of crime in a free society: Looking back looking forward. Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and the Administration of Justice.* Research Forum, NCJ 170029. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

U.S. Senate. 1983. Senate Committee on the Judiciary. *Justice Assistance Act of 1983: Report of the Senate Committee on the Judiciary on S. 53 with additional views.* 98th Cong., 1st sess., S. Rept. 98–220.

Violent Crime Control and Law Enforcement Act of 1994. U.S. Public Law 103–322. 103rd Cong., 2d sess., 13 September 1994.

Walker, Samuel. 1997. *Popular justice: A history of American criminal justice.* 2d ed., rev. New York: Oxford University Press.