Criminal Justice and the IT Revolution

Terence Dunworth
Managing Vice President, Abt Associates

IT WILL NOT BE LONG until 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 the general 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, with a rapidity that is far greater than occurred with the telephone, and they seem certain to have (may already have had) a greater impact than the telephone on the way public and private activities are conducted.

The revolution has enormous implications for the criminal justice system, 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 article, I have a narrow focus—the effect of the IT revolution on the criminal justice system. This is because criminal justice agencies are, in my opinion, the most dynamic users of the kind of information that the IT revolution is bringing into existence. Criminal justice agencies use information to make strategic, tactical, and investigative decisions in ways that other agencies do not. Criminal justice agencies do a lot 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 nineteenth century and culminating with the 1994 Crime Act.

Following the historical overview, I consider the promise and the reality of information technology for law enforcement, reviewing where law enforcement stands with respect to a number of critical information systems areas: records management; criminal histories and offender identification; the Uniform Crime Reporting System and the National Incident Based Reporting System; and computer networking technology and the Internet.

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

Historical Background
The First 100 years—1830 to 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 for more than two centuries. In a 1978 article,[4] Decker 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 U.S. 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 federal 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, and they were used for decision-making about budgeting, facilities construction, and resource al-

An earlier version of this article appeared in NIJ's *Criminal Justice 2000, vol. 3, Policies, Processes, and Decisions of the Criminal Justice System.*

location issues. Data on crime in cities was another matter. Many law enforcement agencies 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 (UCRs), 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 1002 cities, with 83 percent participation of all cities with populations greater than 25,000.

Wickersham Commission, 1931

In 1929, the same year that the UCRs were 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 chair George W. Wickersham.[6] Though there had been locally based studies of criminal justice during the previous ten years,[7] this was the first national evaluation of the system of justice administration in the U.S.

The Commission published 13 reports in June of 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 the IACP's work on the UCRs, and specifically cited the UCR system as a model. However, the members of the Commission wanted to go much further than the UCRs, by creating a comprehensive system of national data encompassing penal, judicial, and police data under one umbrella federal agency which 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 the interpretations of them that were being made. In this respect, the Commission's observations were prescient—many of its concerns have been repeatedly echoed in subsequent commentary on the UCRs.

Presidential Commission, 1965

For the next three and a half decades, the UCRs were 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.[9]

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."[10] In addition, the Commission's survey of 10,000 households suggested that crime of all kinds was being seriously under-reported to police, with the result that the UCRs could not be counted upon to be an accurate measure of crime levels in the country.[11]

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 should be the responsibility of a National Criminal Justice Statistics Center; that state statistical centers should be established to both 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: 1968–1994

The immediate outcome of the work of the 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, 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,[12] and, in 1973 established the National Crime Survey, which carried forward the approach undertaken by the Commission in the 1967 survey mentioned above. Of the Crime Survey, Tonry notes:

> Some observers would say that the National Crime Victimization Survey 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.[13]

Despite the promise inherent in the Commission's report and the subsequent legislation, the operational manifestation of the principles the Commission espoused did not generate long-term acceptance by Congress or the criminal justice community. By the late 1970s, the 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.[14]

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. An 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, BJS as the statistics entity, renaming OJARS to the Office of Justice Programs (OJP) with similar oversight responsibilities, and creating two new agencies—the Bureau of Justice Assistance (BJA) to manage block grants and the Office for Victims of Crime (OVC) to handle victim issues. This organizational structure has survived to the present day and most subsequent legislation authorized and appropriated funding within it. The exception was the 1994 Crime Control Act, which, among other things, created an independent agency, the Office of Community Oriented Policing Services (OCOPS) to manage the 100,000 Cops on the Street program of the Clinton administration.

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 don't know enough about crime and the criminal justice system, and we must develop more information in order 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 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 a significant data collection effort focusing on drugs and crime.[16] The FBI produces Uniform Crime Reports on a nationwide scale. The National Crime Victimization Survey 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 don't 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 twenty 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 don't know the answer. Agencies are acquiring capacity without knowing what to do with it, except to automate paper systems. This is fine, but it isn't much of an advance in decision-making.

In the next two sections of this article, this issue will be examined in the context of local law enforcement agencies. In many respects, local law enforcement agencies 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 most needy consumers of the new IS/IT that has 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.

Law Enforcement and IT—Promise and Reality

The Promise

This section reviews what has taken place in law enforcement with respect to IS/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 law enforcement have promised and sometimes delivered significant improvements in information processing capabilities. It is further believed that the incorporation of these advances into law enforcement operations will at least radically improve and perhaps revolutionize law enforcement. Such advances span virtually all of the information gathering requirements pertaining to crime measurement, control and response that law enforcement agencies might need.

However, despite this promise, the reality in law enforcement has been, and is, quite different. Large-scale data collection systems of crime measurement, such as the National Incident Based Reporting System, 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 law enforcement agencies must perform, and a jaundiced view of them is expressed with disturbing frequency by officers and command staff.

The result is that there now exists a real danger that the IS/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, law enforcement will have missed the most important contribution that the IT revolution can make—namely, to assist law enforcement to redefine itself along the lines proposed by community-oriented and problem-solving philosophies.

In the balance of this section, I will present an overview of the status of IT in law enforcement across what I consider to be the most significant substantive areas. These are: Records Management Systems; Criminal Histories and Offender Identification; Crime Analysis; Mobile Data Terminals; Uniform Crime Reporting and the National Incident Based Reporting System; and Computer Networking Technology and The Internet.*

The Reality

The Reality Records Management Systems (RMS)

A Records Management System (RMS) is the informational heart of any law enforcement agency's operations. It provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, and files about every aspect of law enforcement business. A compre-

* I have been assisted in this section by the information contained in a number of presently unpublished working papers prepared by Abt Associates staff members Peter Finn, Kristin Jacoby, Julia Kernochan, Tom Rich, and Shawn Ward. I have made use of the background materials contained in those papers, though the individuals named are not responsible for, and do not necessarily agree with, the interpretations I have made and the conclusions I have drawn.

hensive and fully functioning RMS should include crime and arrest reports, personnel records, criminal records, and crime analysis data. Even today, this is in fact the exception rather than the rule. Though virtually all staff in any law enforcement agency use and depend upon the information that an RMS should contain, many agencies have inadequate or incomplete systems.

Prior to the 1970s, nearly all law enforcement agencies' record-keeping was paper-based. Gradual conversion to main-frame computer record-keeping began in the 1970s, particularly for crime and arrest information, and by the mid-1980s, an estimated 1,500 of the nation's 17,000 law enforcement agencies were using main-frame computers to a limited extent. Characteristically, due to the high investment cost associated with main frames, most agencies shared time with other city agencies and management of the machine and the system was outside the department. Typically the RMS were little more than record-keeping systems, with functions that differed little from those provided by their paper predecessors. As late as 1993, a Bureau of Justice Statistics survey found that only two-thirds of local law enforcement agencies were using computers for some elements of record keeping.[17]

Lack of control over the system, poor links between its elements, and, sometimes, law enforcement agency disinterest in record-keeping or lack of experience and understanding of computers resulted in limited utilization of the RMS that were developed. Even today, many departments have only partial computerization of record-keeping. Some have no automation on key elements of the records system, and a number cannot, for instance, perform simple tasks that computers ought to be able to do easily, such as automatically compile UCR reports, link arrests to crimes reported, and so on. Consequently, in such agencies, these kinds of functions still have to be performed manually, if at all.

More recently, some agencies have begun to move to fully automated (computerized) records management systems. Some of these agencies have gone beyond simply automating record-keeping procedures to implementing dynamic, relational databases as an integral element in information management.

In such agencies, RMS systems are no longer stand-alone systems; they can be interfaced to other systems in the city or county and to State law enforcement systems, which in turn provided 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 30–40 percent are not uncommon. Now, some agencies 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, state-of-the-art RMS can be integrated with other systems, such as Computer Aided Dispatch (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 will 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.

They also support access to a wide range of external databases, such as the National Crime Information center (NCIC) and National Incident Based Reporting System (NIBRS), and have 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 decision-making on sound information; to determine resource deployment on a pro-active rather than simply a reactive basis; and to execute many other functions that were either 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, automated RMS systems require 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 at best irrelevant and at worst obstructive. Agencies must normally consider hiring new staff or training in-house staff to provide ongoing user training and support, as well as system maintenance and troubleshooting. Historically, police departments have not attempted to hire such staff.

Another common concern addresses liability and security with respect to personnel files and other sensitive data such as investigation reports and criminal files. 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 upon the RMS. If it is absent or deficient, then a domino effect seems inevitable. The other applications will either not realize their potential, or they will fail outright.

Criminal Histories and Offender Identification

As noted above, a critical component of record-keeping 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. Second, even when identification is made at the local level, linking the offender to his/her records in other jurisdictions can be a difficult and tedious process. Since 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 the 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 of the 50 states surveyed reported that 70 percent or more of arrests from the past five years in their criminal history database had entries for final dispositions.[18]

What is obviously needed are identification and history systems that overcome these problems quickly and efficiently. Ideally, these should be integrated into the 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 a national criminal records systems, including the National Crime Information Center (NCIC) and the Interstate Identification Index (III).

Initially, most states maintained something akin to a manual index card system that contained a list of arrested persons, perhaps with accompanying paper folders that contain documentation about individual arrests. Over time, most states have automated these files to some extent. Individual law enforcement agencies can query them via remote terminals. At the national level, the FBI is currently moving towards an automated National Fingerprint File (NFF).

Over the past decade, the federal government has invested more than $200 million to improve the quality of criminal history records at 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 non-criminal justice applications. Most states permit some access to criminal history records by agencies outside criminal justice for employment, licensing, and other purposes.

Perhaps of greater significance are the mandates imposed by the Brady Act and the National Child Protection Act of 1993.[19] 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. The Bureau of Justice Statistics 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.[20] 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. In order 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: 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 due to the fact that much of the desired information exists only on paper or, even if automated, in non-standardized form. Consequently implementing dependable and uniform electronic interfaces between reporting agencies and the central criminal history repository will be a prerequisite for expansion in the effective utilization of criminal histories. In fact, a good deal of work is being done to bring this about.

The Bureau of Justice Statistics (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 the NCHIP program 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 Handgun Violence Prevention Act), the National Sex Offender Registry (NSOR), 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 criminal justice agencies develop the capacity to take advantage of the state and federal systems that are being created. This is another of the IT challenges that criminal justice agencies face.

Mobile Data Terminals (MDTs)

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 radio. Officers 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 hand-held ticket issuing computers. These now match desktop machines in sophistication, and, in the future, will continue to expand in capability. As miniaturization progresses, for instance, hand-held 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 on-board 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 virtually any kind of information be transmitted back and forth, they can be used to provide rapid authorization for law enforcement 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.

Hand-held 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, which 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, first introduced in 1989, are clipboard-size mobile computers, weighing less than five pounds, that recognize handwriting and convert 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 hand-held devices. (Gapay 1992)

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 over 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:

- speed of information dissemination
- saving officers time and effort
- facilitating information sharing
- increasing reporting accuracy and uniformity
- enhancing response time
- increased officer safety

There are, however, some 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 (PERF) survey of 210 departments drawn in part from among 1995 COPS MORE federal grant recipients found that only a small percentage of police departments had MDTs in patrol cars.[21] However, within that minority, many departments had been using laptops in patrol cars for years.

In 1997, the National Institute of Justice sponsored a study by the National Law Enforcement and Corrections Technology Center on the ability of different agencies to communicate across jurisdictions with each other (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 MTDs 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 National Crime Information Center (NCIC) 2000 and Integrated Automated Fingerprinting Identification System (IAFIS) initiatives. MDTs will also assist departments to conform to the new incident-based reporting standards of the National Incident Based Reporting System (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

The International Association of Crime Analysts (I.A.C.A.) offers this statement about crime analysis:

> Crime analysis is a scientific process in the sense that it involves the collection of valid and reliable data, employs systematic techniques of analysis, and seeks to determine, for predictive purposes, the frequency with which events occur and the extent to which they are associated with other events.

In more concrete terms, Reuland identifies four specific functions for crime analysis:[22]

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

2) *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.

3) *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.

4) *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 programmatic, planning, development, and evaluation functions.

It is clear that crime analysis is a process for which computerized data processing is tailor made. However, it is true that law enforcement agencies have been doing some form of crime analysis from time immemorial. Policing hasn't been random and it hasn't been reactive to the exclusion of all other considerations. Crime analysis has always guided decision-making. However, the crime analysis that we think of now is orders of magnitude different from what was performed prior to the advent of desktop computers. These have increased the power and speed of crime analysis tremendously. The advent of community policing has 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:

1) *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 non-police 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).

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

3) *Analysis.* Departments analyze crime data to detect patterns of activity that can predict future crimes. Crime mapping has become an increasingly popular analysis approach (see below).

4) *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.

5) *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 upon it by the federal government.[23] The application of mapping software to urban settings depends upon 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 by-product of routine, day-to-day work.[24]

However, utilization is by no means universal. In 1994, 30 percent of 280 member departments of the International Association of Chiefs of Police 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 National Institute of Justice Crime Mapping Research Center found that 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).[25]

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.[26] A number of obstacles that inhibit a commitment to crime analysis can be identified:

- the perception by some sworn officers that crime analysis is not 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 decision-making;
- 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 non-existent crime analysis training; and
- insufficient funding.

The principal obstacles to more agencies conducting 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 Uniform Crime Reporting (UCR) system, which began operation in the early 1930s and has been in place with little change ever since. The system is

dependent upon 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 the UCR's major topics: crimes cleared, persons arrested, law enforcement personnel, and a Crime Index based on 8 selected offences. However, the UCR system 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 system was needed for use into the 21st century. This coincided with advances in information technology that made a more sophisticated system feasible. The Bureau of Justice Statistics 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.*[27]

The *Blueprint* proposed the National Incident Based Reporting System (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 percent 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 (SLED), 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 the 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.[28] Indeed, the costs associated with the transition can be substantial, especially as many law enforcement agencies have existing records management systems that are either too antiquated to function effectively or are incompatible with NIBRS requirements.

The study also indicated that local law enforcement decision-makers 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.

Of course, 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 record-keeping systems, they do generate computerized data that would meet all of 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 instance, now have data systems that contain a good deal more than the NIBRS date 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 it 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 regional, state, and national levels. It remains to be seen whether the perceived value of this potential will be sufficient to mobilize the voluntary local commitment to participate upon which NIBRS depends.[29]

Computer Networking Technology and the Internet

The topical reviews provided earlier in this section demonstrate that advances in information technology, combined with law enforcement agencies' increasing emphasis on crime prevention, community policing, and problem solving, is 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 last ten years in particular, computer networking–linking two or more computers so that 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 over 35 million users per year.[30] 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 the 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, over 500 local law enforcement agencies maintained web sites, and the establishment and expansion of sites continues at a rapid pace.[31] 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.[32]

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, who 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 a 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 departments.[33] 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.[34]

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, in order 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, needs assessment and strategic planning for the project, 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."[35] 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 indicated 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 indicated 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 inter-agency 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.[36]

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 information technology 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. 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. We are able to do now what was prohibitively expensive ten 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 criminal justice world is not at the forefront of the revolution (and probably shouldn't be), it is nevertheless moving inexorably in the same direction. The IT revolution is bringing change in the system's way of doing business that cannot be avoided. I would argue that it shouldn't be avoided, because, properly managed, the change can be beneficial. But, as criminal justice agencies make 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 criminal justice agencies—law enforcement agencies 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 agencies 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 Criminal Justice Agencies

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 agencies. 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 ten years.[37] 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 criminal justice agencies 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, agencies 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 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 officers will still need to respond to calls for service, especially emergency calls, in the way they always have. In this sense, the criminal justice system will need to retain the traditional elements of its business, while adding new approaches and techniques that at present are either non-existent or are in their infancy.

The impediments to successfully implementing IT solutions are very substantial. Significant investments of resources, time, and money will all be required, and, perhaps most important, agencies 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 agencies do not accept its benefits on faith, because the path outlined above 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.[38]

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 agencies struggle with the design issues surrounding automation for a number of years. It is also easy to find agencies that have had significant problems with vendors who proved unable to deliver the system that was promised. Given this, it is perhaps not realistic to expect agencies 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 criminal justice as a whole, as well as for individual agencies. Yet there is a powerful belief in most agencies 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 an officer to be? It was already noted above that the response capability that is loosely defined as "traditional" 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 an officer to take care of both of these kinds of tasks? Is that a desirable goal? A feasible goal? Does this require an 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 haven't touched on or thought about are resolved, then the biggest remaining problem facing criminal justice agencies 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 utilizing the software (secretaries, writers, etc.) will usually acknowledge that they have mastered only a portion of the capacity of their programs.

Expanded IT in criminal justice agencies 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 biggest single IT challenge for criminal justice agencies.

Knowledge and Risk

As noted above, the effects of IT advances in criminal justice agencies will have repercussions beyond the operational needs of the agencies 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 criminal justice agencies? 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 Decision-Making By Criminal Justice Agencies.* This simply reiterates the theme that has been developed during this article. The more information an agency has and the better its methods of processing that information, the greater the likelihood that decision-making will be rationally based.
- *Cross-Jurisdictional Cooperation and Collaboration.* Good information will create a better foundation for effective cross-jurisdictional interaction. Agencies 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 the Uniform Crime Reporting system are no better than the quality of the data provided by individual agencies. 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.[39] Others however 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.[40] This is particularly true of research that has focused on police departments.[41] However, with more dependable and more comprehensive computerized data, policing research will be better positioned to increase our basic knowledge about crime, and inform policy-making 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 that.

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.[42]

- *Inaccuracy of Data.* As more and more information is accumulated about individuals, it becomes increasingly important that the information be accurate and dependable. This isn't only true in the law enforcement world, of course. None of us want our good credit records to be reported as bad, for instance. But, when we are speaking of a law enforcement context, the negative effects of inaccurate or incomplete data about individuals can be devastating. Quite a lot of police departments collect data on possible gang members for instance. 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. And, departments would not, for instance, 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; it might be to approve an application for a driver's license; or to make a decision about a job applicant; or to decide whether or not 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?
- *Unauthorized Access.* A paper file in a 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's hard to see why computerized files in criminal justice

agencies will not be extraordinarily vulnerable. Obviously, this is not what any criminal justice agency (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 criminal justice 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 towards 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 criminal justice 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 criminal justice agencies. The human mind is advancing, it is producing new knowledge and capabilities at an astounding rate, and criminal justice agencies must keep up. The IT revolution and criminal justice agencies utilization of the capacity it generates is a journey not a destination. It may in fact 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.

This evolving process is going to be never-ending. There isn't going to 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. Criminal justice agencies 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 then, we must acknowledge that IS/IT and its uses by criminal justice agencies are continually expanding and seem virtually unlimited. The challenge for criminal justice agencies will be to take the (risky) step of dynamically embracing the new potential.

Endnotes

[1] During 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 computer; 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 J. David Coldren, "Change at the Speed of Light: Doing Justice in the Information Age," in "Computerization in the Management of the Criminal Justice System," Richard Scherpenzeel, Editor. *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, European Instititute for Crime Prevention and Control: Helsinki/The Hague, 1996. See also the many other articles in this document for a comprehensive examination of computerization and criminal justice issues.

[4] Decker, S.H., "Evolution of Crime Statistics as a Police Problem," *Journal of Police Science and Administration,* Vol 6, Issue 1 (March, 1978), pp 67–73. IACP, Alexandria, VA. This article 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 the UCRs, 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 the UCRs was proposed and adopted in the mid-1980s. It came to be called the National-Incident-Based Reporting System (NIBRS) and is discussed below in Section 3.

[6] Publications on the Wickersham Commission are numerous. For an Internet reference, see the University Publications of America web site *http://www.upapub.com/guides/wickersham.htm.* This excerpts from Samuel Walker, *Popular Justice: A History of American Criminal Justice,* 2d ed., rev. (New York: Oxford University Press, 1997). For other selections, see: James D. Calder, *The Origins and Development of Federal Crime Control Policy: Herbert Hoover's Initiatives* (Westport: Praeger, 1993) and the National Commission on Law Observance and Enforcement (1931). Reports Washington, D.C.: U.S. Government Printing Office.

[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: The Cleveland Foundation, 1922).

[8] See the National Commission *Reports (op cit).* A fourteenth report, on a particular case of abusive police behavior, was suppressed at the time of the original publications, but was later released.

[9] For the original report of the Commission, see 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. For a recent perspective on the commission and its effects, see the report of the Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and Administration of Justice—U.S. Department of Justice, Office of Justice Programs, The Challenge of Crime in a Free Society: Looking Back Looking Forward (1998). National Institute of Justice, NCJ 170029, Washington, D.C.: U.S. Government Printing Office.

[10] Reported by Joseph Foote, *An Overview for the Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and Administration of Justice*, p. 3. Printed in The Challenge of Crime in a Free Society: Looking Back Looking Forward, op. cit.

[11] See *Summary,* page v, The Challenge of Crime in a Free Society, op. cit.

[12] A review of federal legislation from 1968 through 1994 can be found in Terence Dunworth, Scott Green, Peter Haynes, Peter Jacobson, and Aaron J. Saiger, *National Assessment of the Byrne Formula Grant Program, Report #2: The Anti-Drug Abuse Act of 1988—A Comparative Analysis of Legislation, National Institute of Justice,* December 1996, NCJ 163882, 63 pages. A more focused assessment of the legacy of the 1967 Commission is provided by Michael Tonry, in *Building Better Policies on Better Knowledge,* printed in Looking Back Looking Forward, op. cit.

[13] Tonry, op.cit., pp 113–114.

[14] LEAA was officially terminated on April 25, 1982 (see S. Rept. 98–220, p. 3). A vast literature on LEAA exists. For an entry to it, see: Richard S. Allinson, *LEAA's Impact on Criminal Justice: A Review of the Literature,* Criminal Justice Abstracts, December 1979, pp 608–648; Robert F. Diegelman, *Federal Financial Assistance for Crime Control: Lessons of the LEAA Experience,* Journal of Criminal Law and Criminology, 73:3, 1982, pp 994–1011; Malcolm Feely and Austin Sarat, *The Policy Dilemma: Federal Crime Policy and the Law Enforcemnent Assistance Administration* (Minneapolis: University of Minnesota Press, 1980).

[15] The Violent Crime Control and Law Enforcement Act of 1994, U.S.C. 18, Ch. 47, Sec. 320603.

[16] I refer here to the Arrestee Drug Abuse Monitoring Program (ADAM), the successor to the Drug Use Forecasting Program (DUF), 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.

[17] Brady, T. *The Evolution of Police Technology. Presentation to the Technology for Community Policing Conference,* hosted by the National Law Enforcement and Corrections Technology Center. Washington, D.C.: U.S. Department of Justice, June 1997.

[18] SEARCH. 1999. *Survey of Criminal History Information Systems, 1997.* NCJ 175041. Washington, DC: Bureau of Justice Statistics

[19] The Brady Act of 1993 (went into effect in 1994) was an amendment to the Gun Control Act of 1968. See U.S.C. Section 922.

[20] Bureau of Justice Statistics.1999. *Presale Handgun Checks, the Brady Interim Period, 1994–98.* NCJ 175034. Washington, DC: Bureau of Justice Statistics.

[21] Bezdikian, V. and C.L. Karchmer. *Technology Resources for Police: A National Assessment.* Washington, D.C.: Police Executive Research Forum, July 1996.

[22] Reuland, M.M. Information Management and Crime Analysis: Practitioners' Recipes for Success. Washington, D.C.: Police Executive Research Forum, 1997.

[23] See for instance, National Partnership for Reinventing Government, *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, July 12, 1999.

[24] See a number of articles by Rich, T.F.: "Crime Mapping by Community Organizations: Initial Successes in Hartford's Blue Hills Neighborhood." In *Crime Mapping Case Studies: Successes in the Field,* N. La Vigne and J. Wartell, eds. Washington, DC: Police Executive Research Forum, 1998; "The Chicago Police Department's ICAM Program." *Program Focus.* Washington, DC: National Institute of Justice, 1996. "The Use of Computerized Mapping in Crime Control and Prevention Programs." *Research in Action.* Washington, DC: National Institute of Justice, 1995.

[25] Mamalian, C.D. and N.G. La Vigne. "The Use of Computerized Mapping by Law Enforcement: Survey Results." *Research Preview.* FS000237. Washington, DC: National Institute of Justice, 1999.

[26] Reuland, op. cit.

[27] E. Poggio. et al. (1985). Blueprint for the future of the Uniform Crime Reporting Program: Final Report of the UCR Study. NCJ 98348. Washington, D.C.: Bureau of Justice Statistics.

[28] Roberts, D.J. (1997). "Implementing the National Incident-Based Reporting System: A Project Status Report." NCJ 165581. Washington, D.C.: Bureau of Justice Statistics.

[29] 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's 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 produce a videotape demonstrating effective use of NIBRS data, using local agencies as exemplars.

[30] Manning, W.W. "Should You Be on the Net?" *FBI Law Enforcement Bulletin,* 66(1) (January 1997): 18–22.

[31] Goodman, M.D. "Working the Net: Exploiting Technology to Increase Community Involvement and Enhance Service Delivery." *Police Chief,* 64 (8) (August 1997): 45–53.

[32] Sulewski, K.E. "Faxback Response: Previous Question: How Has the Internet Helped Your Agency?" *FBI Law Enforcement Bulletin,* 66(1) (January 1997): 23–25.

[33] Ibid.

[34] Paynter, R.L. "Internet Connections." *Law Enforcement Technology,* 25(8) (August 1998): 28–32.

[35] Roberts, D.J. *Integrated Justice Information Systems for State and Local Jurisdictions: An Overview of Planning Activities for the Office of Justice Programs, US Dept. of Justice.* Washington, D.C.: Office of Justice Programs, July 1998.

[36] For example, see the following two examples.

North Carolina Department of Correction. "Officers Use Technology to Work More Closely With Police." http://www.doc.state.nc.us/NEWS/983news/JWAN.htm. This site documents North Carolina's Justice Wide Area Network (JWAN). JWAN, located in Hendersonville, NC, 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 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, N.R.M. "Birth of an Information Network." *FBI Law Enforcement Bulletin,* 62(2) (February 1993): 19–22. The All County Criminal Justice Information Network (ACCJIN) in Contra Costa, California, established in 1990, 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.

[37] See, for instance, Declan McCullagh, *The Marker of a Criminal,* Wired Digital Inc., November 19, 1999. Accessible through: http://www.wired.com/news/politics.

[38] This process is already under way. The Office of Community Oriented Policing Services is planning a series of IT technical assistance conferences for the first six 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.

[39] See Jeremy Travis, *Criminal Justice Research and Public Policy in the United States,* in Scherpenzeel, op. cit. Pp 115–125.

[40] For comments on the general problems associated with research see Terence Dunworth, *National Assessment of the Byrne Formula Grant Program,* National Institute of Justice Research in Brief, p. 8. June 1977.

[41] For an illustration of the particular difficulties associated with policing research, see Terence Dunworth, *Crime in Public Housing: A Three City Analysis,* National Institute of Justice, 1993. 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% of specific incidents contained in city-wide databases in five cities for which such databases were obtained. See, Terence Dunworth et al, *The National Evaluation of the Youth Firearms Violence Initiative,* National Institute of Justice, 1999.

[42] A cross-national discussion of privacy and security issues can be found in Peter Csonka, *Council of Europe and Data Protection: Free Flow of Information versus Privacy,* in Scherpenzeel, op. cit, pp. 103–112.