Criminal Justice Discovers Information Technology

by Maureen Brown

ABSTRACT

During the last half of the 20th century, information technology became a central force in the field of criminal justice. Information, with its associated technologies, provided a critical support structure for operations. Yet, it also created new dilemmas for criminal investigations, prosecutions, and prevention. While information technology assumed a major role in supporting the socioeconomic framework, it also mandated a fundamental rethinking of legislative policies pertaining to security, privacy, and criminal activity. The rise of the information-centric economy brought a host of opportunities and challenges to the field of criminal justice. Issues pertaining to information technology operations, policy, and criminology pose substantial challenges to the field of criminal justice as it enters the next millennium.

Maureen Brown is Associate Professor at the University of North Carolina at Charlotte.

The shift from an industrial to an information-based economy was one of the most significant changes occurring in many nations in the last 20 years of the 20th century. By the turn of the century, the production, sale, and service of information and its associated technologies provided a critical support structure to the world economy. Given the promise that information technology might afford, global investments in information technology grew to more than $500 billion annually (G2 Research 1997). This chapter considers the growth of information technology (IT), its adoption by various actors in the criminal justice system, and the implications for the goals of and expectations for the criminal justice system.

The chapter has two sections. The first section uses a timeline to describe the growth of IT within various sectors of the criminal justice system. The operational aspect elaborates on the extent to which computer technology has permeated police, court, and corrections agencies to promote service delivery. Conversely, the criminal perspective examines issues surrounding computer crime and its impacts on policies and programs. Finally, the civil side examines the changes pertaining to civil rights. Exhibit 1 provides a synopsis of many of the milestones that mark the technological changes of the last half of the century.

The second section discusses major hurdles and challenges confronting the field of criminal justice. Although computer-based innovations began as tools to advance transaction-based processes—a goal that was easily achieved—by the end of the century, criminal justice professionals pursued more ambitious goals for IT, hoping that IT would enhance organizational knowledge. Managers expected cases, problems, and events to be identified, tracked, and evaluated more easily, thereby improving productivity and performance. In striving to meet the expectations, however, several hurdles were encountered at every stage of the IT-adoption process. In addition to the technological challenges, organizational hurdles impeded procurement, implementation, operations, and maintenance, regardless of organization size. For example, large organizations experienced problems with system design and personnel training; small jurisdictions suffered from funding and expertise limitations. Specifically, the next section sheds light on

In addition to the technological challenges, organizational hurdles impeded procurement, implementation, operations, and maintenance, regardless of organization size. For example, large organizations experienced problems with system design and personnel training; small jurisdictions suffered from funding and expertise limitations.

Exhibit 1. Major information technology events and implementation milestones in the criminal justice system

1946 – The first large-scale electronic general purpose digital computer was created by Dr. John W. Mauchly and J. Presper Eckert: the Electronic Numerical Integrator and Computer (ENIAC).

1951 – The first commercially available electronic digital computer (UNIVAC I) is introduced by Remington Rand. The UNIVAC I correctly predicts that Dwight D. Eisenhower will win the presidential election.

1952 – Dr. Grace Hopper invents the first high-level programming language.

1955 – The New Orleans police department installs the first electronic data-processing machine, a vacuum tube-operated calculator with a punch card sorter and collator that summarizes arrests and warrants.

1958 – Second-generation computers are built with transistors replacing vacuum tubes. There were roughly 2,500 computers in use in the United States.

1960 – The programming language COBOL is developed by a committee headed by Dr. Hopper.

– The St. Louis Police Department installs the first computer-aided dispatch system.

1964 – The computer chip is introduced, leading to the third generation of computer machines. By 1964, the number of computers in use in the United States has grown to 18,000.

– The Crime Commission report produces recommendations on police technology.

– The Federal Bureau of Investigation inaugurates the National Crime Information Center (NCIC), providing a national computerized filing system on wanted persons, stolen vehicles, weapons, and other items of value. The system processes more than 6,580 transactions per day.

– Allegheny County, Pennsylvania, installs data-processing equipment to improve operations in civil court.

1966 – The National Law Enforcement Telecommunications System, a message-switching facility that links all State police computers with the exception of Hawaii, is established.

– The Freedom of Information Act (FOIA) passes.

1967 – The Advance Regional Justice Information system is established by the San Diego police department for clearing investigative cases.

continued

Exhibit 1 (continued)

1968	– The first use of an 8-inch floppy magnetic storage disk is demonstrated by Alan Shugart of IBM. – The Omnibus Crime Control Act establishes the Law Enforcement Assistance Administration (LEAA) program, which includes a mandate to increase the use of IT. – AT&T announces the creation of 911. – The National Institute of Justice (NIJ) is created to, among other goals, "advance technology assimilation."
1969	– The ARPANET network, predecessor to the Internet, is established. – The first microprocessor chip is developed by Dr. Ted Hoff. – The National Consortium for Justice Information and Statistics is established.
1970	– The fourth generation of computers arrives with the invention of the large-scale integration chip, which contains roughly 15,000 circuits. – LEAA begins to spur technology innovation efforts over the next 12 years by providing roughly $50 million to State and local law enforcement agencies. – The Fair Credit Reporting Act of 1970 passes.
1971	– The microprogrammable computer chip is developed by Dr. Ted Hoff. – Intel introduces the first microprocessor, the 4004, capable of 60,000 operations per second. – The National Center for State Courts (NCSC) is created as an independent nonprofit organization dedicated to improving the administration of justice.
1973	– The first court-operated, computer-aided transcript (CAT) system is installed.
1974	– C programming is developed. – The Federal Privacy Act of 1974 passes.
1975	– IBM introduces the first laser printer. – The first commercially successful microcomputer, the Altar, becomes available. – One of the first major studies investigates local-level police, corrections, and courts information technology activities.
1976	– Steve Wozniak and Steve Jobs build the first Apple computer.
1977	– NCSC begins the Court Improvement Through Applied Technology Project.

Exhibit 1 (continued)

1978	– NCSC publishes *Computer Use in the Courts: Planning, Procurement, and Implementation*.
1979	– The first spreadsheet, VisiCalc, is introduced.
	– CompuServe, the first public online service, is founded.
	– NCSC survey reveals that 500 State-level courts are employing data-processing techniques while 100 courts are actively participating in local criminal justice information systems.
Mid- to late 1970s	– LEAA funds projects such as State Judicial Information System and Gavel-A National Model Trial Court Information System.
1980	– The first hard drive, the Winchester, is introduced, revolutionizing storage for personal computers.
	– Bill Gates, working for IBM, develops MS-DOS.
	– Enhanced 911 is developed.
	– The Privacy Protection Act of 1980 passes.
1981	– The Silicon 32-bit chip is produced.
	– IBM introduces the personal computer; more than 300,000 are sold in the United States.
	– The Police Foundation Survey reports that almost all law enforcement agencies serving 1 million or more persons have some sort of computerized searching capability.
1982	– A total of 3,275,000 personal computers are sold.
	– Hayes introduces the 300-bps smart modem.
	– LEAA is abolished.
	– Compaq, Inc., is founded.
1983	– Seven percent of U.S. households own computers; in 5 years, the number jumps to 20 percent.
1984	– IBM introduces the Intel 80286 microprocessor.
	– Apple introduces the Macintosh computer.
	– NCSC releases the State Judicial Information System Project report.

continued

Exhibit 1 (continued)

- NCSC hosts the first National Court Technology conference.
- Congress creates the State Justice Institute (SJI) to foster joint innovations in Federal and State courts.
- The Justice Assistance Act creates the Office of Justice Programs, which currently consists of the Bureau of Justice Assistance (BJA), the Bureau of Justice Statistics, NIJ, the Office of Juvenile Justice and Delinquency Prevention (OJJDP), and the Office for Victims of Crime (OVC).
- The Computer Fraud and Abuse Act of 1984 passes.

1986

- SJI opens.
- The International City Management Association releases a second major study examining law enforcement, corrections, and courts systems in local government.
- NIJ funds first assessment of the impact of a map-based crime analysis system in Chicago.
- The Computer Fraud and Abuse Act of 1986 and the Electronic Communications Privacy Act of 1986 pass.

1987

- The 80386 microprocessor is introduced.
- SJI begins awarding grants for technology innovations.

1988

- The Computer Matching and Privacy Protection Act of 1988 passes.

1989

- The Intel 486 becomes the world's first 1 million transistor microprocessor. At a size of .4″ x .6″, it can execute more than 15 million instructions per second.
- Tim Berners-Lee invents the first Internet-based hypermedia that becomes known as the World Wide Web (WWW).
- NCSC and SJI release the first issue of *Court Technology Bulletin*, a bimonthly publication on technology in the courts.
- NCSC's Technology Information Exchanges Services begins.
- The Forum on the Advancement of Court Technology (FACT) is formed to facilitate dialogue between vendors and court managers regarding the application of technology in court operations.

Exhibit 1 (continued)

1990

- Microsoft Corporation releases Windows 3.0, selling hundreds of thousands of copies. More than 54 million computers are in use in the United States.
- The Technology Information Services (TIES) program fields more than 1,000 requests for information on IT.
- TIES opens the Court Technology Laboratory.

1991

- The World Wide Consortium releases standards that describe the framework for linking documents on different computers.
- Senator Al Gore proposes the High Performance Computing and Communications (HPCC) initiative for building a high-speed "digital highway" for Federal agencies.
- The U.S. Department of Justice establishes the Computer Crime Unit within the Criminal Division.

1992

- Microsoft releases Windows 3.1.

1993

- The successor to the Intel 486, the Pentium microprocessor, is introduced. It contains 3.1 million transistors and is capable of performing 112 million instructions per second.
- The HPCC initiative is significantly expanded to the National Information Infrastructure, a broadband digital network allowing universal access.
- The White House launches its first Web page.
- Two-thirds of all police departments are using computers in criminal investigations, crime analysis, budgeting, and staff allocation.
- More than 90 percent of police departments serving populations of more than 50,000 are using computers for criminal investigation, budgeting, dispatch, and staff allocation.
- The College of William and Mary unveils Courtroom 21.

1994

- Netscape Navigator 1.0 is launched.
- The Violent Crime Control and Law Enforcement Act of 1994 is passed.
- Memorandum between the U.S. Department of Justice and the U.S. Department of Defense to conduct joint research on information systems development efforts is written.
- NIJ opens the National Law Enforcement and Corrections Technology Center (NLECTC) to promote the use of technology in criminal justice.

continued

Exhibit 1 (continued)

- *Technology Beat*, a serial published by NLECTC focusing on technology in criminal justice, is first published.
- The Computer Abuse Amendments Act of 1994 passes.

1995
- Microsoft releases Windows 95.
- TIES TIS fields more than 2,000 requests for information on IT.
- Justice Information Network (JUSTNET) is established to promote information collection and dissemination.
- NIJ establishes the Office of Science and Technology.
- The National Criminal Justice Reference Service (NCJRS) goes online.
- BJA funds the National Criminal History Program, awarding a total of $112 million to every State to improve criminal history information systems.
- Roughly 83 percent of all State prosecutors use computers.

1996
- Microsoft releases Windows NT 4.0.
- Telecommunications Act of 1996 passes.
- More than 76 percent of full-time large prosecutors' offices and 70 percent of medium offices have adopted some sort of integrated computer system. Systems typically include courts, law enforcement, and district attorney's offices.
- The Computer Abuse Amendments Act of 1996 passes.

1997
- Internet Explorer 4.0 is released.
  Approximately 50 million users are connected to the WWW.

1998
- Windows 98 is shipped.
- E-commerce (electronic commerce) allows buyers to obtain merchandise over the Internet.
- More than 10 million people are telecommuting.
- The Crime Identification Technology Act of 1998 (Public Law 105–251) passes, making more than $1.25 billion available for integrated justice systems.

1999
- Intel releases the Pentium III microprocessor, which provides enhanced multimedia capabilities.
- Microsoft introduces Office 2000.

the operational, criminal, and civil challenges as the criminal justice system struggles to take full advantage of the information age.

Some of the difficulties agencies experience in taking advantage of IT stem from the rapidity and scope of its developments. In a span of 25 years, the computer industry grew to comprise 10 percent of the gross domestic product in the United States. In two short decades, the field of IT became larger than the auto, steel, mining, petrochemical, and natural gas industries combined. For example, between 1988 and 1995, IT sales grew 14 percent in constant dollars (U.S. Department of Commerce 1997), with the Government sector accounting for roughly $80 billion every year in IT expenditures (G2 Research 1997). By 2000, IT represents a major global economic support structure (Tapscott and Caston 1993). The discussion that follows highlights the changes that occurred within the fields of IT and the resulting impacts on police, courts, and corrections.

On the downside, IT requires substantial investments in training, maintenance, and coordination. In addition to these operational costs, IT can introduce security breaches. Data that were once on paper in filing cabinets behind locked doors are now stored on hardware that may be vulnerable to theft and destruction.

IT adoption and implementation creates both benefits and costs. IT can assist with efficiency and productivity gains by allowing tasks to be conducted in parallel, by eliminating steps in a process, and by reducing the amount of time it takes to conduct a task. IT can also aid decisionmaking through its ability to store, condense, and display large quantities of information for developing and evaluating operational initiatives. However, the benefits of IT do not come without significant resource investments. The hurdles and challenges of adoption and implementation can negate the recognition of benefits. On the downside, IT requires substantial investments in training, maintenance, and coordination. In addition to these operational costs, IT can introduce security breaches. Data that were once on paper in filing cabinets behind locked doors are now stored on hardware that may be vulnerable to theft and destruction. Yet another downside of IT relates to its role in crime. As discussed later, the adoption of IT has created additional incentives and mechanisms for the perpetration of crimes such as embezzlement, pornography, and sabotage. Although this chapter concentrates on the operational benefits of IT and the civil and criminal impacts, it is recognized that the costs of IT for society as well as criminal justice agencies and other organizations are substantial.

The 1960s and 1970s—The Age of Discovery

The operational stream

Prior to the 1970s, computer technology made tremendous theoretical gains, laying the foundation for its future application to various industries and occupations. These theoretical gains between the 1940s and 1970s led to significant technological advances from the 1960s through the 1990s. Pivotal moments included the release of the first commercially available computer in 1951; the New Orleans Police Department's adoption of the first arrest and warrant computer system in 1955; and the St. Louis Police Department's installation of the first computer-aided dispatch system in 1960.

In 1964, advances appeared in both computer design and application of computers to criminal justice: The third generation of computer machines appeared as the computer chip was introduced; the number of computers in the United States grew to 18,000; Allegheny County, Pennsylvania, installed the first court-based data processing system; and the Federal Bureau of Investigation (FBI) launched the National Crime Information Center (NCIC). NCIC provided the first nationwide computer filing system containing wanted persons, stolen vehicles, and weapons. At its inception, the system provided more than 6,580 transactions per day to 15 different agencies.

By 1966, the National Law Enforcement Telecommunications System was adopted, linking all State police departments in the continental United States. In 1967, San Diego police began using computer technology to clear investigative cases. At the same time, President Lyndon Johnson's Crime Commission Report contained more than 200 recommendations, 11 of which dealt specifically with police technology.

The Omnibus Crime Control Act of 1968 established the Law Enforcement Assistance Administration Program (LEAA). Over the next 13 years, LEAA disbursed more than $50 million in grant funding for police technology (Northrop, Kraemer, and King 1995). Spurred in part by the findings of the Crime Commission, a long-term subsidy program administered by the LEAA provided seed money for technology adoption (SEASKATE 1998).

Also in 1968, the National Institute of Justice (NIJ) was created. One of its many missions was to advance technology assimilation within criminal justice agencies. AT&T also unveiled the 911 system. Heralded as a pivotal event in police operations, the 911 function encouraged broader use of computer technology in law enforcement.

The first microcomputer chip was developed in 1969. The National Consortium for Justice Information and Statistics (NCJIS; a private, nonprofit membership organization dedicated to improving the criminal justice system through the effective application of information and identification technology) also appeared in 1969 (http://www.corp.search.org/About_SEARCH.htm).

In the 1970s, IT continued to advance, and the criminal justice system began using computers to streamline operations and enhance customer service. The decade began with the arrival of the fourth generation of computers, which used integration chips with 10,000 more circuits than the chips of 5 years earlier. In 1971, Intel released the first microprocessor capable of 60,000 operations per second, and the National Center for State Courts (NCSC) was established to promote technology innovation in the courts.

In the 1970s, criminal justice managers were discovering what computers were and how they might assist operations. Although some adoption had occurred, for the most part it was a time of discovery and learning.

In 1975, one of the first major studies investigating computer technology in criminal justice, based on the computerization efforts of 310 counties and 403 cities, was released by the University of California's Public Policy Research Organization (PPRO) (Matthews, Dutton, and Kraemer 1976). The study found that despite advances in the IT field, local criminal justice bureaucracies did not rely heavily on computer systems to support many critical functions.

In the 1970s, computer-based automation had been adopted more widely by law enforcement agencies than corrections and courts. As shown in exhibit 2, uniform crime reporting, parking tickets, and traffic accidents were the most common applications used by county law enforcement agencies. For cities, the most commonly computerized functions in law enforcement were uniform crime reporting, traffic violations, and criminal offense files. In total, across the 713 jurisdictions, uniform crime reporting (27 percent), parking tickets (27 percent), and traffic violations (24 percent) were the most frequently automated functions. Although large urban departments appeared to be recognizing the benefits of IT, these same departments felt that many applications yielded disappointing results (Colton 1975). Implementation was slower than was expected, and disagreement was widespread about IT's usefulness for operations. Despite LEAA's $50 million during the 1970s for technology assimilation, operational benefits—outside of dispatch and record reporting arenas—went largely unrealized. In law enforcement, by the close of the 1970s, IT was used primarily for recordkeeping, record searching, and record reporting.

Exhibit 2. 1975 survey results of local government automation of law enforcement, corrections, and courts activities

	Cities		Counties		Total	
	#	%	#	%	#	%
Law enforcement activities						
Alias name files	65	16	4	1	69	10
Criminal offense files	112	28	48	15	160	22
Dispatching	65	16	19	6	84	12
Field interrogations	44	11	12	4	56	8
Fingerprint population	28	7	13	4	41	6
Intelligence compilation	21	5	6	2	27	4
Juvenile offense files	64	16	28	9	92	13
Modus operandi	47	12	10	3	57	8
Parking tickets	149	37	41	13	190	27
Stolen property	82	20	30	10	112	16
Stolen vehicles	88	22	33	11	121	17
Traffic accidents	131	33	32	10	163	23
Traffic violations	124	31	47	15	171	24
Uniform crime reporting	143	35	48	15	191	27
Correction activities						
Arrest records	120	30	47	15	167	23
Jail population	36	9	38	12	74	10
Court activities						
Child support records	9	2	71	23	80	11
Court calendars and scheduling	33	8	44	14	77	11
Court case disposition	28	7	30	10	58	8
Court disposition records	31	8	52	17	83	11
Court docketing	43	11	44	14	87	12
Detention records	14	3	23	7	37	5
Fines, collateral, and bail collections	32	8	44	14	76	11
Jury selection	28	7	105	34	133	19
Juvenile probation	12	3	25	8	37	5
Plaintiff/defendant records	20	5	45	15	65	9
Probation records	15	4	43	14	58	8
Wants and warrants	102	25	1	.3	103	14

Sources: Matthews, Dutton, and Kraemer 1976; Matthews et al. 1976.

In the mid-1970s, correctional operations, which lacked financial capital for computerization, remained largely manual in nature. As shown in exhibit 2, the PPRO study revealed that no more than 15 percent of county correctional systems had automated arrest records and only 12 percent had automated jail population records. Although counties appeared slow to innovate, cities were making a bit more progress. Thirty percent of the cities had automated arrest records and 9 percent had automated jail population records. Overall, by 1975 only approximately 23 percent of local government agencies had computerized arrest records and only 10 percent had automated jail population records.

Although court systems demonstrated a higher level of computerization than did correctional departments, progress remained slow and uneven. According to Polansky (1996), by the early 1970s, many major urban courts had begun building court information systems. But there was little systems analysis and planning, and systems—designed and programmed by people who knew little about courts—never showed the results to justify high costs. Despite these difficulties, the first court-operated, computer-aided transcript system was installed in Allegheny County, Pennsylvania, in 1973. In the 1975 PPRO study, roughly 35 percent of courts automated jury selection, while court disposition records; court calendars and scheduling; court docketing; and fine, collateral, and bail collection remained primarily manual. As shown in exhibit 2, the most common IT applications among the courts were jury selection (19 percent), warrants (14 percent), and court docketing (12 percent). By the end of the decade, a nationwide survey conducted by NCSC indicated that approximately 500 courts were using data processing to some extent (Polansky 1996).

In summary, in the 1970s, criminal justice managers were discovering what computers were and how they might assist operations. Although some adoption had occurred, for the most part it was a time of discovery and learning. By the close of the decade, several major publications had been developed by major professional organizations to assist managers in computerizing operations. For example, NCSC published a series of reports, one titled *Guides for Court Managers,* and LEAA funded a report called *Computer Use in the Courts: Planning, Procurement, and Implementation Considerations.* In 1978, American University published *Criminal Courts Technical Assistance Project.* According to Colton (1979), in the 1970s, criminal justice managers were intimidated by and cautious of IT yet very interested in the potential benefits it might offer.

The criminal stream

During the 1960s and 1970s, networking and computer hardware and software had not advanced to the point where legislation concerning the perpetration of computer crimes was necessary. Most of the systems at that time were mainframes that were relatively closed to the public. Although computer crime more than likely took place, no Federal or State legislation existed in that area. IT crimes were prosecuted under penal codes that related to the particular offense, such as theft, embezzlement, or fraud. It was not until the technological changes of the 1980s that computer crime began to emerge as an important problem. Few anticipated the technological changes the next decade would bring and did not place much emphasis on the need to deter computer crime.

The civil stream

The growth of IT during the 1960s and 1970s sparked intense debate over the right to privacy versus the right to access information. By the late 1990s, the criminal justice arena would find itself in the difficult position of enforcing ambiguous privacy legislation and lobbying for international treaties on data security issues. The right to individual privacy has been a longstanding constitutional issue—the Fourth Amendment to the Constitution guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The evolution of large databases and the associated technologies that promote collection, collation, and dissemination call into question the appropriate balance between individual privacy and rights of access.

Advances in IT would give rise to debates over encryption, promotion of commerce, protection of privacy, protection of public safety, and national security—issues affecting the daily operations of criminal justice agencies.

The Freedom of Information Act (FOIA) became law in 1966. The Act established, for the first time, a presumption that records in the possession of executive-branch agencies and departments are accessible (Mason, Mason, and Culnan 1995). FOIA guarantees the right of people to know about the business of government. The Act requires government agencies to reveal on demand many of their records and documents. Since 1966, FOIA has been amended a number of times, each time strengthening citizens' access rights to government information.

The 1970s also brought a number of Federal enactments substantively affecting interpretations of data rights of individuals. The Fair Credit Reporting Act, enacted in 1970, regulated how consumer credit reporting services could disclose personal information. The Act defined various legal terms about credit reporting, described permissible uses for credit reports, detailed consumers' rights in disputing credit reports, and established the enforcement responsibilities of the Federal Trade Commission (FTC) (Mason, Mason, and Culnan 1995, 246).

On the heels of the Fair Credit Act, the Federal Privacy Act of 1974 prohibited government agencies from using data for purposes other than those for which they were collected. In essence, it protects individual rights to privacy from government misuse of Federal records containing personal information. The Act requires agencies to collect and maintain only data relevant to their mission and forces agencies to account for every use of their information. A final piece of legislation of the 1970s, the Right to Financial Privacy Act of 1978, stipulated that personal financial records held by banks may not be released without a search warrant.

Interest group coalitions began to form during the 1970s, sparking debate over what information should be collected and disseminated and for what purposes. In the following years, this debate would influence where the criminal justice system balanced privacy rights against public access. Advances in IT would give rise to debates over encryption, promotion of commerce, protection of privacy, protection of public safety, and national security—issues affecting the daily operations of criminal justice agencies.

A Flurry of Activities—The 1980s

The operational stream

In the 1980s, the criminal justice system attempted to capitalize on the promises of IT. In 1980, Bill Gates developed the Microsoft Disk Operating System (MS DOS). MS DOS, coupled with the development of the 32-bit silicon chip, allowed IBM to introduce the first personal computer in 1981. During this same time, a Police Foundation survey reported that almost all law enforcement agencies serving areas with more than 1 million people had some sort of computerized searching capabilities (SEASKATE 1998). The study also suggested that procurement was a poor surrogate measure for use and institutionalization. Many departments had invested heavily in computers, but the investment had failed to produce comprehensive benefits in productivity and efficiency. In September 1982, *Police Magazine* asked, "Why is law enforcement not making more effective use of data processing?" This question has persisted, and in the ensuing 20 years, research has begun to reveal that factors such as organizational support, training, and culture affect benefit attainment.

By 1982, LEAA was abolished due to unrealistic expectations, wasteful use of funds, mounting red tape, and uncertain direction (SEASKATE 1998). Nonetheless, LEAA did contribute to bringing IT into the criminal justice system through programs like State Judicial Information Systems and Gavel-A National Model Trial Court Information System Project.

In 1984, IBM released the first 80286 processor, allowing more than 6 million operations per second, and NCSC hosted its first National Court Technology Conference in Chicago. By 1986, the U.S. Congress had created the State Justice Institute (SJI) to foster technology innovations in State and local courts.

During this same period, the International City Management Association released a followup survey of local governments similar to the one conducted by PPRO in 1975. The study examined all cities and counties with populations of 25,000 or more, and sampled 1 in 3 with populations between 10,000 and 25,000. Exhibit 3 shows the results from 1,032 jurisdictions. Results demonstrated substantial strides by local law agencies in their technology adoption rates. Roughly 40 percent had automated incident and accident reporting systems, 35 percent used computers for administrative tasks, and 17 percent had computer-aided dispatching. Nineteen percent used IT for scheduling purposes. In addition, 27 percent planned to adopt computerized dispatching systems, 24 percent had planned to automate incident and accident reports, and 23 percent had planned to incorporate computer technology into administrative tasks. By 1985, 90 percent of the 403 U.S. cities with populations of more than 50,000 were using IT in their criminal justice systems.

In 1976, roughly 20 percent of police officers surveyed suggested that investigative cases would be unworkable without IT. Just 12 years later, 80 percent of police officers claimed that without computerized information, cases would be unworkable (Northrop, Kraemer, and King 1995). Four out of five police officers indicated that computers made it easier to get information, that the information was often accurate, and that time-saving benefits were frequent. Clearly, according to this study, law enforcement agencies were benefiting greatly from IT. But, benefits notwithstanding, difficulties persisted. The systems most detectives and officers employed were cumbersome, particularly for collating leads and information from a variety of sources. Especially problematic were collaborations with other agencies. Systems incapable of permitting searches by external entities inhibited interagency efforts to capture offenders operating in a wide territory.

Correctional agencies continued to lag in their technology adoption efforts. Although nearly one-third of the agencies reported automated wants and warrants, only a small percentage (12 percent) reported automated jail management records.

Exhibit 3. Application software in local government criminal justice agencies in 1985 (N=1,032)

	#	%
Law enforcement		
Incident/accident reports	433	42
Administration	358	35
Resource management/scheduling	196	19
Traffic accidents	433	42
Dispatching	171	17
Corrections		
Warrants	274	27
Jail management	124	12
Courts		
Wants and warrants	274	27
Jury selection	222	22
Fines, collateral, and bail collections	214	21
Court calendars and scheduling	161	16

Source: Adapted from Scoggins, Tidrick, and Auerback 1986.

About as many departments were planning for automation; 16 percent planned to automate wants and warrants, and 15 percent planned to adopt technology to assist with jail management.

For courts, the study revealed that roughly 20 percent applied computer technology to jury selection and to fines and fees collections. Approximately 15 percent applied computer technology to court scheduling and 10 percent to office administration. More local governments planned to incorporate technology in the courts: 14 percent had planned to automate court scheduling; 13 percent, fines and fees collections; 6 percent, jury selection; and 6 percent, the public attorney's office.

Because the 1975 and 1986 surveys overlapped in seven key areas—traffic accidents, dispatch, jail population, wants and warrants, court scheduling, jury selection, and fines collection—comparisons describe the growth over the decade. Automation of traffic accident reports saw the greatest gain from 23 to 42 percent. The second-fastest growth rate occurred in the wants and warrants area, which increased 13 percent. The remaining areas of dispatch, jail population, jury selection, court scheduling, and fines collection did not witness substantial growth.

Issues such as work process dependencies, computer code complexity, and questions about potential gains may have slowed automation in these areas.

By the mid-1980s, SJI had emerged as a major provider of technical assistance to State and local courts. Beginning in 1984, the NCSC's court technology conferences attracted thousands of professionals to witness successful technology projects (Polansky 1996). Furthermore, the agency launched the Forum on the Advancement of Court Technology in 1989 to facilitate dialogue between vendors and court managers on technology issues.

Unprecedented increases in computing power and capacity took place during the 1980s. Whereas in the early 1980s mainframe computers executing 200,000 transactions per second were the norm, by the end of the decade, Intel had released a microcomputer chip capable of executing more than 15 million operations per second. Moreover, the cost of computing power had dropped significantly while ease of use had increased. Thus, by the close of the 1980s, criminal justice agencies were more inclined to view technology as a feasible, reliable, and necessary support mechanism for operations.

The criminal stream

With the rise of personal computers and networking came the realization that IT provided new ways to commit crime. During this time, the U.S. Department of Justice (DOJ) defined computer crime as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." Until 1984, no computer crime laws existed for prosecuting many of the infractions occurring. The Computer Fraud and Abuse Act of 1984 was the first legislative act focusing directly on computer crime. The Act established a felony offense for (1) accessing a computer without authorization; (2) obtaining information via unauthorized access from the financial records of a financial institution; (3) accessing a computer to use, destroy, modify, or disclose information found in a computer system; and (4) interfering with government operations on a computer.

Although the Act addressed some of the deficiencies in the law, criminal justice professionals complained it was too ambiguous and narrow in scope to provide adequate protection. With overwhelming bipartisan support, the Act was amended in 1986. The Computer Fraud and Abuse Act of 1986 expanded the 1984 legislation and made it a felony to commit computer fraud; to alter, damage, or destroy information contained in a "Federal interest computer"; to traffic in computer passwords; and to either conceal or possess counterfeit or unauthorized access devices. Despite the well-understood need for such legislation, figures on the extent of computer-related crime were not available.

The civil stream

Several laws passed during the 1980s sought to balance the rights of individual privacy versus rights to access information. The Electronic Communications Privacy Act of 1986 protected all forms of electronic transmissions from unauthorized interception. The Act also prohibited any person or entity from knowingly divulging the contents of any communication carried on a network service. It also allowed citizens to recover damages and bring civil suits if their wire, oral, or electronic communications were illegally intercepted. The Video Privacy Protection Act forbade retailers from releasing or selling video rental records without customer consent or a court order. Recognizing the ease with which records could be matched, thereby threatening privacy rights, the Computer Matching and Privacy Protection Act of 1988 was passed. The Act regulated the matching of Federal, State, and local records. It sought to ensure privacy, integrity, and verification of data for computer matching, and to establish data integrity boards within federal agencies. It required Federal agencies to enter into written agreements with other agencies or non-Federal entities before disclosing records for use in computer matching programs. The Act also mandated that individuals whose records are to be matched receive advance notification. In addition, it called for establishing procedures for retaining and destroying data after matching. The Data Integrity Board was empowered to oversee and coordinate the implementation of the Act and to prescribe procedures for verifying information produced through computer matching.

A Demand for Knowledge Support— The 1990s

The operational stream

More than 54 million computers were in use in the United States by 1990, and by 1991, Senator Al Gore's initiatives to establish a national data communication network—the information superhighway—were under way. In 1993, the White House launched its first Web page, and more than 90 percent of police departments serving populations of more than 50,000 were using computers for criminal investigation, budgeting, dispatch, and staff allocation (Reaves and Smith 1995).

A 1993 survey of 3,270 State and local law enforcement agencies with 100 or more full-time sworn officers—of which 661 responded—showed that the percent of large law enforcement agencies maintaining computerized files jumped from 39 to 55 percent in 3 years. The 1993 computer penetration rates in law enforcement appear in exhibit 4. From 1990 to 1993, the percent maintaining computerized traffic citation data rose from 30 to 46 percent, and computerization of calls for service from 30 to 45 percent (Reaves and Smith 1995). By 1993, among responding agencies, 97 percent had access to personal computers,

Exhibit 4. Law enforcement and management administration, computers and information systems, 1993 (N=661)

	#	%		#	%
Digital terminal, car mounted	214	32	Arrests	598	90
Handheld	71	11	Calls for service	576	87
Laptop	371	56	Criminal history	489	74
Mainframe	549	83	Driver's license information	291	44
Mini	358	54	Evidence	440	67
Personal	644	97	Fingerprints	247	37
Owns AFIS	81	12	Inventory	445	67
Shared AFIS	190	29	Payroll	476	72
Terminal access to AFIS	189	29	Personnel	550	83
Budgeting	546	83	Stolen property	485	73
Crime analysis	546	83	Stolen vehicles	473	72
Crime investigation	547	83	Summonses	252	38
Dispatch	541	82	Traffic accidents	467	71
Fleet management	385	58	Traffic citations	456	69
Jail management	202	31	UCR/NIBRS	271	41
Manpower allocation	386	58	UCR summary	494	75
Recordkeeping	623	94	Vehicle registration	316	48
Research	369	56	Warrants	502	76

Source: Reaves and Smith 1995.

83 percent had access to a mainframe computer, and 32 percent had access to car-mounted digital terminals. Ninety-four percent stated that they had automated their records and 83 percent said that they used technology to assist in crime investigations. Ninety percent had arrest histories automated and 87 percent kept calls-for-service histories. Many departments had also automated many business functions. Personnel and payroll records as well as stolen property and stolen vehicle records were largely automated. In short, by the early 1990s, computerization of routine transactions in law enforcement was largely complete.

In 1994, DOJ and the U.S. Department of Defense established a formal partnership to conduct joint research on a variety of technologies including information systems. Furthermore, the 1994 Crime Act passed Congress, leading to the establishment of the National Law Enforcement and Corrections Technology Center (NLECTC). NLECTC was established to help identify, develop, manufacture, and adopt new products and technologies specifically designed for law enforcement and criminal justice applications. According to Attorney General Janet Reno, NLECTC was to be "part of a new law enforcement information network that will make it easier for law enforcement to find useful products and assist industry in identifying law enforcement requirements" (U.S. DOJ, NIJ 1994).

The Justice Information Network (JUSTNET) system was established in 1995 by NLECTC. JUSTNET serves as an online gateway to technology product and service providers as well as an information hub for services of interest to the law enforcement and correctional communities. Through JUSTNET, users have access to interactive bulletin boards on a variety of topics, a comprehensive database of law enforcement products and technologies, and NLECTC publications. In 1995, the Bureau of Justice Assistance (BJA) awarded a total of $112 million to every State to improve criminal history information system technology.

By the mid-1990s, concern about underutilization of IT in corrections led to NIJ and the National Institute of Corrections (NIC) sponsoring several studies on the adoption rate of technology in corrections. A survey of 49 correctional institutions concluded, "Correctional officials were unanimous in describing management information systems as essential to their work. However, their biggest complaint was that their systems were under utilized" (Kichen, Murphy, and Levinson 1993, 7). The survey suggested that the underutilization resulted from poorly designed information systems and a lack of sufficient equipment and adequate training. Although IT had become an integral support mechanism in many daily operations (see exhibit 5), systems were not well managed, negating many potential benefits.

A second correctional survey released in 1995 (U.S. DOJ, NIC 1995) examined 148 Federal, State, and local corrections agencies; these consisted of 48 State and Federal adult prisons, 44 large jails and jail systems, and 56 community correctional agencies. By this time, IT was in use in numerous corrections operations. Approximately 80 percent of adult facilities, nearly 70 percent of community corrections agencies, and approximately 60 percent of large jails had access to a local area network with electronic mail capability. The majority of the facilities also had access to NCIC and local or State online offender information (see exhibit 6). Interestingly, even though the vast majority of the facilities were satisfied with their technology, negative comments such as "minimally adequate," "slow," and "cumbersome" surfaced.

A third survey of State and Federal correctional information systems, released in 1998 (U.S. DOJ 1998), focused not on hardware access but rather on the extent to which electronic data were available to support correctional operations

Exhibit 5. Computer adoption in corrections, 1993 (N=49)

	#	%		#	%
Offender case management			**In program data**		
Admissions/releases	44	96	Good time	37	80
Parole	40	87	Disciplinary reports	29	63
Classification	36	78	Grievance	18	39
Inmate activities			**Accounting***		
Work assignment	35	76	Payroll	39	85
Education	33	72	Accounts payable	36	78
Movement control	29	63	Purchasing	33	72
Offender history			**Personnel***		
Prior record tracking	37	80	Leave status	35	76
Detainers	35	76	Training	32	70
Medical/mental health records	20	43	Staff scheduling	23	50

* Administrative/facilities support.

Source: Adapted from Kichen, Murphy, and Levinson 1993.

in all 50 State-level institutions. Respondents identified the data collected and maintained in electronic format and data availability for computation. The survey asked if State correctional departments maintained a database of 207 specific items deemed critical by the researchers. The data categories included offender profiles, behaviors, and release information. It turned out that no department collected all of the data elements. Collection rates ranged from 16 to 85 percent, and 32 departments captured at least 50 percent of the critical data elements. Only 40 departments maintained data on offender behavior and only 38 maintained data on crimes committed by offenders under some form of supervision. Unfortunately, the study failed to evaluate data quality.

In contrast to correctional experiences, by the 1990s, virtually no court, no matter how small, had not embarked on an IT project to improve services and reduce costs (Polansky 1996). NCSC established the Technology Information Exchange Service (TIES). TIES, in turn, initiated programs to assist with IT innovation, including the Court Technology Laboratory and the Technology Information Service (TIS). TIS issued more than 2,000 information packets to

Exhibit 6. Information systems in corrections, 1995

	#	%
Adult prison systems (N=48)		
Computer local area network (LAN) with e-mail capability	37	77
Computer wide area network (WAN) with e-mail capability	24	50
Federal online offender information system (NCIC)	34	71
Local or State government information system (not for offender data)	19	40
Local or State online offender information system	34	71
Large jails/jail systems (N=44)		
Computer local area network (LAN) with e-mail capability	25	57
Computer wide area network (WAN) with e-mail capability	13	30
Federal online offender information system (NCIC)	42	95
Local or State government information system (not for offender data)	19	43
Local or State online offender information system	42	95
Community-based corrections (N=56)		
Computer local area network (LAN) with e-mail capability	38	68
Computer wide area network (WAN) with e-mail capability	26	46
Federal online offender information system (NCIC)	40	71
Local or State government information system (not for offender data)	24	43
Local or State online offender information system	50	89

Source: Adapted from the U.S. Department of Justice, National Institute of Corrections 1995.

interested court personnel on issues such as case management systems, imaging, video technology, and judicial electronic document and data interchange. In the early 1990s, the TIS program fielded more than 1,000 requests annually from court agencies on IT adoption. By 1995, the annual rate of requests had doubled (Walker 1996). In the early 1990s, the Court Technology Laboratory opened; its mission was to investigate the feasibility of alternative technologies in courts.

In 1993, the College of William and Mary unveiled Courtroom 21, "the courtroom of the 21st century today." It was heralded as the most technologically advanced trial and appellate courtroom in the world. With the goal of improving the timeliness of court trials while keeping costs low, the high-tech courtroom was designed to test the impact of employing state-of-the-art technology in court hearings. Some capabilities of the courtroom included instant access to LEXIS and FolioViews, real-time stenograph transcription (immediate transcription benefits the hearing impaired and permits reviewing testimony), two-way live audio-video for witness testimony, videotaping of proceedings, consecutive translation of up to 143 languages, and animated presentations and monitor display of evidentiary items (Lederer 1997). In April 1997, the William and Mary Law School conducted an experimental jury trial to assess the facilities. The visual presentation of evidence resulted in substantial time savings in witness examinations (Lederer and Solomon 1997).

During the earlier stages of IT adoption, managers hoped to speed processing and streamline manual work processes. They focused largely on transactions such as traffic tickets, dispatch, and payroll. Over the years, however, improvements in hardware and software allowed organizations to use IT not only to support transactions, but also to provide information-generating knowledge.

By 1994, roughly 83 percent of all prosecutors' offices used IT for office management, individual criminal matters, and case management (DeFrances, Smith, and van der Does 1996). Popular topics included electronic filing (including digital signatures), courtroom automation, video technologies, imaging, and court reporting technologies. The researchers sampled 308 chief prosecutors from the estimated 2,350 that try felony cases (see exhibit 7). The study also found that many offices experienced data-related problems. Poor data quality may have resulted from data coding limitations and/or a lack of quality assurance procedures. Eighty-five percent of offices reported problems with accessible data quality, including incomplete information on adult criminal records. Close to 60 percent cited problems with data accuracy and roughly 40 percent reported timeliness problems.

The NCIC system had also been upgraded to include single prints of wanted persons by the 1990s. As mentioned earlier, at its inception in 1964, 15 agencies used the system and executed roughly 6,580 transactions per day. By the 1990s, more than 79,000 agencies accessed the system, executing approximately 1.5 million transactions per day.

Technical advances in computing processing, storage, and communications stimulated hope for service delivery improvements among criminal justice managers. During the earlier stages of IT adoption, managers hoped to speed processing and streamline manual work processes. They focused largely on transactions such as traffic tickets, dispatch, and payroll. Over the years, however, improvements in hardware and software allowed organizations to use IT not only to support transactions, but also to provide information-generating knowledge. By using that

Exhibit 7. Computer use among prosecutors, 1996

	%
Office management	
Caseload statistics	60
Budgeting	46
Expenditures	38
Employment records	17
Information on individual criminal matters	
Adult criminal history records	48
Processing/outcome evidence about cases	41
Arrest of individuals	36
Juvenile delinquency history records	25
Case management by attorneys	
Form or letter preparation	82
Prewritten motions	71
Jury instructions	65
Court dates	55
Subpoenas	55
Discovery requests	51
Witnesses	50
Physical evidence	16

Source: DeFrances and Steadman 1998.

knowledge effectively, managers can improve the quality of service delivery. It was during the 1990s that scholars and practitioners alike began to focus on ways knowledge workers might strengthen organizations. As advances were made, practitioners expected technology to support knowledge and demanded that staff become information literate and knowledge oriented.

The shift in requirements from transactions to knowledge became apparent in many fields, and these expectations have dominated criminal justice bureaucracies. The interdependencies of the criminal justice agencies as well as the potential crime-reducing benefits from sharing and integrating data and knowledge have probably promoted a more holistic approach to information collection and analysis.

The critical need for criminal justice agencies to exchange and integrate data resulted in Congress' passing the 1997 Crime Identification Technology Act

(Public Law 105–251). It made more than $1.25 billion available for developing integrated justice systems. The Act called for (1) upgrading criminal history and criminal justice record systems, including systems operated by law enforcement agencies and courts; (2) improving criminal justice identification; and (3) promoting compatibility and integration of national, State, and local systems for criminal justice purposes.

Although many jurisdictions have sought integrated systems, technological and organizational hurdles have proven difficult to overcome. Organizational issues related to collaboration, training, and funding; shortages in technical personnel; and security concerns have thwarted efforts. Nonetheless, by the late 1990s, more than a dozen States were in the process of either developing or implementing plans to allow interagency data exchange and integration. These collaborative efforts took many forms and often involved a diverse set of actors. But the goals were fairly similar: to allow all components of the criminal justice community to share comprehensive case management, incident, and investigative data across organizational boundaries.

The criminal stream

In 1991, DOJ established the Computer Crime Unit (CCU) within the Criminal Division. CCU was given responsibility for prosecuting computer crimes, lobbying for strengthened penalties for computer crime, and encouraging expansion of the Federal computer crime statute. Despite CCU's many responsibilities, the absence of a comprehensive legal framework for computer crime encouraged it to focus more on lobbying than on prosecutorial functions. CCU lobbying goals included (1) focusing on unauthorized use rather than unauthorized access of computer systems (in the legal sense, *use* was broadly defined to include indirect and direct access, whereas *access* was defined by direct access only); (2) criminalizing malicious programming (or the insertion of such programs); (3) legislating the forfeiture of computers used in the commission of crimes; and (4) enacting stricter sentences.

In 1994, the Computer Abuse Amendments Act was expanded to address the transmission of viruses and other harmful code. The Act made it illegal to knowingly transmit a computer program (such as a virus, time-bomb, or worm) that causes damage. And in 1996, the Act was amended, making it illegal to intentionally access a protected computer or cause either reckless damage or a denial of service.

Thus, by the end of the 1990s, Federal computer crime legislation covered (1) interstate and foreign communications; (2) theft or compromise of national defense, foreign relations, atomic energy, or other restricted information; and (3) the intentional transmission of damaging programs. Moreover, legislation prohibited unauthorized access of U.S. Government and most financial institutions' computers. Federal legislation also addressed the unauthorized access of computers in other States or countries. In addition to the State and Federal enactments, every State except Vermont had passed some form of computer crime regulation. Despite the many differences among the statutes of the 49 States, State legislation addressed 6 common categories:

- **Intellectual property**—expanded the idea that computer programs, computer data, and computer services are property or intellectual property.
- **Computer tampering**—made illegal "knowingly or recklessly" degrading or disrupting computer services to the extent that such actions impair the ability of authorized users to obtain full use of their computer system.
- **Computer trespass**—made illegal the unauthorized access of a computer and its contents including using the contents of a computer to aid and abet the commission of a crime.
- **Unlawful duplication/disclosure**—made illegal copying and distributing the contents of a computer without authorization.
- **Defenses**—allowed some defenses to restrict unauthorized access.
- **Venues/sites of offense**—specified the jurisdiction for purposes of prosecuting the theft of computer information.

By the late 1990s, more than 100 million people had access to data networks, and the U.S. financial industry transmitted trillions of dollars of transactions every day over computer networks. The Computer Emergency and Response Team at Carnegie Mellon University found a 498-percent increase in computer crime between 1991 and 1994. In 1994 alone, 40,000 Internet computers were attacked in 2,460 separate incidents.

Eighty-six percent of the States had addressed computer tampering and computer trespass. By 1999, 43 States had passed some form of regulation pertaining to computer tampering and trespass. The next most frequently cited legislative area pertained to the expanded property concept. Sixty-two percent (31 States) had passed legislation extending the property concept to computer technology. Less commonly addressed in the State legislation were unlawful duplication (20 States), jurisdiction of offense issues (16 States), and defenses against unauthorized access (6 States).

By the late 1990s, more than 100 million people had access to data networks, and the U.S. financial industry transmitted trillions of dollars of transactions every day over computer networks. The Computer Emergency and Response Team at Carnegie Mellon University found a 498-percent increase in computer crime between 1991 and 1994. In 1994 alone, 40,000 Internet computers were attacked in 2,460 separate incidents. Yet, according to Attorney General Janet Reno, computer crime has not received the emphasis that other forms of crime have earned (Reno 1997a).

Computers and crime interrelate in three distinct manners: a computer may be the object, subject, or instrument of a crime (Icove, Seger, and VonStorch 1995). First, as objects of crime, processor time, services, hardware, software, or information are often common targets for theft. Second, computers can also be the subject of a crime when the goal is to disable. For example, the transmission of harmful code such as viruses or logic bombs can destroy vital computer data and programs. Finally, computers may be instruments for conducting crimes such as fraud, embezzlement, and child pornography. By the late 1990s, the most common crimes conducted online were network break-ins, espionage, theft (of software, data, or passwords for impersonation), embezzlement, child pornography, and sabotage.

The civil stream

With the 1990s came widespread recognition that information in and of itself was a commodity that could be bought, sold, or bartered. According to Branscomb (1994), information dynamics changed from being an instrument through which we acquire and manage other assets to being a primary asset itself. With information becoming a commodity in and of itself, many called for further elaboration on protection and definition of ownership rights. The increased speed and accuracy of computer data collection and analysis routines also increased the value of information previously seen as unusable. But even as social debates showed the boundaries between public and private information, they were not clearly delineated.

On one hand, companies were encouraged to increase profits by selling data and restricting access. On the other hand, public demand for free access pushed individuals and companies to maximize data access and minimize data restrictions. As a natural consequence of these contradictory pressures, the 1990s saw the beginning of a host of novel questions. While the debate raged, criminal justice agencies wrestled with ambiguous computer and data security issues. The only major legislative act addressing the privacy-access debate was passed in 1997. The No Electronic Theft (NET) Act closed a loophole in the law that allowed people to give away copyrighted material (such as software and data) without legal repercussions.

The civil stream of the 1990s was dominated by debate. Several major pieces of legislation were introduced, but none passed. The underlying philosophical issues spurred debate, speculation, and uncertainty. At the same time, sophisticated computer procedures were evolving. These promoted the economic value of information by establishing sophisticated data-matching techniques and impenetrable data channels. Economic incentives led to complex computer encryption techniques for stopping unauthorized access. The ability to restrict access severely limited criminal justice efforts to identify, deter, and prosecute computer crime.

In sum, operationally, by the close of the 1990s, criminal justice agencies expected much from technological innovations. It was no longer enough to automate simple transactions such as payroll, dispatch, and crime reporting. Many agencies looked to technology to enhance knowledge by providing access to a wealth of previously untapped information. Mapping systems, hot-spot analysis, and object-oriented technologies dominated the decade as researchers sought to define technology solutions capable of enhancing knowledge. If technology was to truly serve the needs of the criminal justice system, then technology had to facilitate the accretion of knowledge that could translate into improved performance and service delivery.

At the same time, criminal and civil issues dominated the IT landscape. The use of technology to perpetrate crimes skyrocketed, but only one-tenth of all computer crimes were reported. The FBI estimated that between 85 and 97 percent of computer intrusions went undetected (Icove, Seger, and VonStorch 1995). The ongoing debate about public rights to access information versus proprietary interests restricting those data offered little to criminal justice professionals in their attempts to protect and serve.

In 1993, recognizing the computer-related difficulties facing the criminal justice community, Vice President Al Gore established the Government Information Technology Services Board. He challenged the Board to establish goals addressing the information technology needs of the criminal justice community. The board identified the following goals: to define the criminal justice community's information requirements, to test the core requirements, to establish a joint Government-private sector Criminal Justice Information Advisory Group, and, by June 1998, to prepare a global criminal justice information network. The Crime Identification Technology Act of 1998 (PL 105–251) provided roughly $1.25 billion for integrated system development efforts to achieve these goals. The following section examines several major challenges that confront the criminal justice system as it enters the new millennium.

IT Challenges Confronting the New Millennium

The criminal justice arena turned to IT to leverage many of the benefits that technology promised. The credo of being able to access "any thing, any time, any place" offered the opportunity to gain significant operational benefits. Yet, with the promise of the technology revolution came unexpected hurdles and challenges. In the last two decades of the 20th century, criminal justice agencies experienced substantial turmoil as the information age gained momentum and they struggled to adapt. The use of technology to improve operations, new mechanisms for crime perpetration, and civil issues pertaining to protection of both privacy and access all stimulated major changes in the criminal justice system.

Sustaining the changes associated with IT innovation has proven difficult for many organizations. The true cost in technological adoption is in the ongoing maintenance that technology demands. Complex training requirements, ongoing funding needs, and system staffing shortages have thwarted many well-intended efforts.

The speed at which IT grew proved particularly challenging to the criminal justice system because few anticipated the speed of these developments and the scope of their impact on criminal justice. Since many of these challenges were unexpected, agencies scrambled to chart new policies and programs with minimal lead time. Although many predicted significant benefits, few understood the corollary costs and disadvantages the criminal justice field would be forced to assume. The discussion below focuses on some of the major IT challenges deriving from the operational, criminal, and civil domains of the criminal justice system. The challenges confronting the criminal justice field fall in the areas of (1) enhancing collaboration and knowledge; (2) sustaining IT change; (3) deterring, investigating, and prosecuting computer crime in a global market; and (4) mediating the privacy-access debate.

Enhancing collaboration and knowledge

The first challenge focuses on collaborating to capture and promote knowledge among staff and officers. In the past, IT equated to automating manual procedures and spewing data—much of which had little relevance to the officer in the field. The link between data and knowledge appeared evasive and fleeting. Although data were cataloged, searched, and analyzed, frustrations grew. Criminal justice professionals complained about the lack of timely, complete, accessible, and accurate data. The need to enhance knowledge by sharing critical data, documents, images, and key transactions among agencies dominated discussions.

Establishing effective partnerships and overcoming the fears associated with information sharing remain challenging. Traditionally, the criminal justice culture has discouraged information sharing, often for good reason. Exposure could compromise an investigation or jeopardize life or property. Developing partnerships and establishing what information can and should be shared does not come easily. Figuring out how to reward data sharing while maintaining security and accountability continues to challenge the criminal justice field as it looks to technology to advance knowledge.

Sustaining IT change

Sustaining the changes associated with IT innovation has proven difficult for many organizations. The true cost in technological adoption is in the ongoing maintenance that technology demands. Complex training requirements, ongoing funding needs, and system staffing shortages have thwarted many well-intended efforts. Although grant opportunities provided funds for system startup, operational budgets have often failed to provide the requisite ongoing support. Ensuring that electronic-based data are maintained in a reliable, documented, and replicable fashion, with a chain of custody, demands procedures for data collection, retention, and distribution. One of the greatest challenges facing any organization is the extent to which it is capable of assimilating the changes that technology brings. Technology often forces changes in work processes and procedures, in training and support, and in policies and communications. It can be a challenge to weather and assimilate the changes while avoiding a detrimental setback in services. Given the rate of IT growth, the procedures and methods for sustaining IT-driven innovations demand constant attention.

Deterring, investigating, and prosecuting computer crime in a global market

The third challenge confronting the criminal justice system is how to deter, investigate, and prosecute crime related to IT in a global marketplace. Computer crime can penetrate political boundaries and override legislative policies with ease. The dimension of the problem was best articulated by Attorney General Reno when she stated that, via computer crime, "You can sit in a kitchen in St. Petersburg, Russia, and steal from a bank in New York" (1997a). As a consequence, controlling computer crime requires sophisticated international treaties. In her desire to address the global vulnerabilities that make deterrence, investigation, and prosecution difficult, Reno proposed an agreement among the P8 countries to combat computer crime. As shown in exhibit 8, the agreement calls for the international criminal justice community to institutionalize 10 major principles for combating computer crime. The extent to which international support can be elicited and maintained will have a significant bearing on the criminal justice system's ability to arrest computer crime.

Exhibit 8. International principles for combating computer crime

1. There must be no safe havens for those who abuse information technologies.
2. Investigation and prosecution of international high-technology crimes must be coordinated among all concerned states, regardless of where harm has occurred.
3. Law enforcement personnel must be trained and equipped to address high-technology crimes.
4. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
5. Legal systems should permit the preservation of, and quick access to, electronic data that are often critical to the successful investigation of crime.
6. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-technology crime.
7. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the state where the data resides.
8. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
9. To the extent practical, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
10. Work in this area should be coordinated with the work of other relevant international agencies to ensure against duplication of efforts.

Source: Reno 1997a.

Mediating the privacy-access debate

The fourth challenge facing criminal justice involves the privacy-access debate. The definition used to determine whether information is public or private is in constant flux (Branscomb 1994; Icove, Seger, and VonStorch 1995; Reno 1997b). Moreover, they suggest that it will continue to be a moving target until we agree on which ethical values to impose and which guiding principles to follow (Branscomb 1994, 176).

According to Reno, encryption techniques can make it impossible for law enforcement agencies to lawfully overhear criminal telephone conversations or gain access to electronically stored evidence. She argues that encryption techniques can seriously jeopardize public safety and national security. She calls for a balanced approach supporting both commercial and privacy interests but also maintaining the ability to investigate and prosecute serious crime.

The use of encryption techniques sits at the center of this debate. These computer capabilities thwart the ability to deter, investigate, and prosecute crime. According to Reno, encryption techniques can make it impossible for law enforcement agencies to lawfully overhear criminal telephone conversations or gain access to electronically stored evidence (1997b). She argues that encryption techniques can seriously jeopardize public safety and national security. She calls for a balanced approach supporting both commercial and privacy interests but also maintaining the ability to investigate and prosecute serious crime. Recognizing that encryption is critical to security, privacy, and commercial interests, Reno calls for a “key” approach to safeguarding information where computer devices incorporate a virtual “lock and key” mechanism. A viable key management infrastructure would promote electronic commerce and enjoy the confidence of encryption users. She also recommended a key management infrastructure permitting law enforcement to obtain court-ordered access, criminalizing the improper use of encryption key recovery information and the use of encryption for criminal purposes, and allowing the Federal Government use of key recovery encryption that is inoperable within the private sector.

The debate between privacy and commercial interests will continue to rage until an effective compromise can be reached among the various interest groups. Unfortunately, as identified by Branscomb, the criminal justice field will continue to wrestle with a legal infrastructure that can best be described as “an impenetrable and irrational thicket of sometimes irrelevant and often unenforceable laws” (1994, 180).

In sum, the past two decades brought the criminal justice system both opportunities and challenges. IT was heralded throughout the business society as a tool for improving operations and stimulating effectiveness and productivity. At the same time, IT also became a critical economic support structure as well as a mechanism for perpetrating crime. In the future, the ways in which international society both employs and controls technology in a global context will have an enormous impact on the criminal justice field and its ability to contain crime and protect domestic safety.

References

Agranoff, Michael. 1991. Controlling the threat to personal privacy. *Journal of Information Systems Management* 8 (3) (Summer): 38–42.

Anthes, G. 1996. IRS project failures cost taxpayers $50 billion annually. *Computerworld* 30 (42): 1–30.

Boettinger, H.M. 1984. Information industry challenges to management and economics. *New Jersey Bell Journal* 7 (1) (Spring): 12–21.

Bowsher, C.A. 1994. Preface to *Executive guide: Improving mission performance through strategic information management and technology: Learning from leading organizations.* Doc. no. GAO/AIMD–94–115. Washington, D.C.: U.S. General Accounting Office.

Boynton, A., G. Jacobs, and R. Zmud. 1992. Whose responsibility is IT management? *Sloan Management Review* (Summer): 32–38.

Branscomb, Anne Wells. 1994. *Who owns information?* New York: Basic Books.

———. 1990. Rogue computer programs and computer rogues: Tailoring the punishment to fit the crime. *Rutgers Computer and Technology Law Journal* 16 (1) (1990): 32–36.

Brown, Mary M., and J.L. Brudney. 1998. A “smarter, better, faster, and cheaper” government? Contracting for Geographic Information Systems. *Public Administration Review* 58 (4): 335–345.

Cats-Baril, W.L., and R.L. Thompson. 1996. *Information technology and management.* New York: Irwin.

Caudle, S.L., D.A. Marchand, S.I. Bretschneider, P.T. Fletcher, and K.M. Thurmaier. 1989. *Managing information resources: New directions in State government.* Syracuse, New York: Syracuse University.

Ciongoli, A.G., J.A. DeMarrais, and J. Wehner. 1994. Computer-related crimes. *American Criminal Law Review* 31(2): 425–453.

Cleveland, Harlan. 1989. *The knowledge executive: Leadership in an information society.* New York: Dutton.

Colton, Kent W. 1979. *Police and computer technology: A decade of experience since the Crime Commission—Summary.* Grant no. 76–NI–99–0043, NCJ 60551. U.S. Department of Justice, Law Enforcement Assistance Administration.

———. 1975. Computers and the police: Police departments and the new information technology. *The Municipal Year Book 1975.* Washington, D.C.: International City Management Association.

Colton, Kent, Margaret Brandeau, and James Tien. 1983. *A national assessment of police command, control, and communications systems.* Grant no. 78–NI–AX–0144, NCJ 87679. U.S. Department of Justice, National Institute of Justice.

Davenport, Thomas. 1993. *Process innovation: Reengineering work through information technology.* Boston: Harvard Business School Press.

Davenport, T.H., R.G. Eccles, and L. Prusak. 1992. Information politics. *Sloan Management Review* (Fall): 53–65.

Davis, G.B., A.L. Lee, K.R. Nickles, S. Chatterjee, R. Hartung, and Y. Wu. 1992. SOS: Diagnosis of an information system failure. *Information and Management* 23: 293–318.

Dawes, S., K. Kelly, D. Andersen, P. Bloniarz, A. Cresswell, and T. Galvin. 1996. *Making smart IT choices: A handbook.* Albany, New York: Center for Technology in Government.

DeFrances, C.J., and G.W. Steadman. 1998. *Prosecutors in State courts, 1996*. Bulletin, NCJ 170092. U.S. Department of Justice, Bureau of Justice Statistics.

DeFrances, C.J., S. Smith, and L. van der Does. 1996. *Prosecutors in State courts, 1994.* Bulletin, NCJ 151656. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

DeSeve, E., A.M. Pesachowitz, and L.K. Johnson. 1997. *Best IT practices in the Federal Government.* Report published by the Chief Information Officers Council and the Industry Advisory Council. Washington, D.C.: Chief Information Officers Council.

Drucker, Peter. 1995. *Managing in a time of great change.* New York: Truman Talley Books/Dutton.

———. 1990. *The new realities.* New York: Harper & Row.

———. 1969. *The age of discontinuity: Guidelines to our changing society.* New York: Harper & Row.

Feldman, M.S., and J.G. March. 1981. Information in organizations as signal and symbol. *Administrative Science Quarterly* 26 (2): 173.

Fletcher, P., S. Bretschneider, D. Marchand, H. Rosenbaum, and J.C. Bertot. 1992. *Managing information: The county study.* Syracuse, New York: Syracuse University.

Flowers, Stephen. 1996. *Software failure: Management failure: Amazing stories and cautionary tales.* New York: John Wiley & Sons.

G2 Research. 1997. Public sector forecasts. Retrieved June 1998 from the World Wide Web: http://206.184.213.145/slg/slg1.htm.

Gallagher, B.P., C.J. Alberts, and R.E. Barbour. 1997. *Software acquisition risk management key process area.* Doc. no. CMU/SEI–97–HB–002. Pittsburgh: Carnegie Mellon University, Software Engineering Institute.

Geller, William. 1997. Suppose we were really serious about police departments becoming "learning organizations"? *National of Institute Justice Journal* 234 (December): 2–8.

Goldstein, Herman. 1990. *Problem-oriented policing.* New York: McGraw-Hill.

Gurwitt, R., 1996. The new data czars. *Governing* (December): 52–56.

Hammitt, Harry. 1998a. Constitutional right of informational privacy. *Government Technology* (June): 22.

———. 1998b. Privacy marches on. Retrieved 16 February 2000 from the World Wide Web: http://www.govtech.net/publications/gt/1998/July/access/access.shtm.

———. 1998c. Privacy versus access tug of war. *Government Technology* (February): 28–29.

Higuera, R.P., A.J. Dorofee, J.A. Walker, and R.C. Williams. 1994. *Team risk management: A new model for customer supplier relationships.* Doc. no. CMU/SEI–94–SR–005. Pittsburgh: Carnegie Mellon University, Software Engineering Institute.

IBM Corporation. Assuring access for all and protecting privacy and security. Living in the Information Society Series. Retrieved 11 January 2000 from the World Wide Web: http://www.ibm.com/ibm/publicaffairs.

Icove, D., K. Seger, and W. VonStorch. 1995. *Computer crime: A crimefighter's handbook.* Sebastopol, California: O'Reilly and Associates.

Johnson, E.C. 1998. Court automation and integration: Issues and technologies. *SEARCH Technical Bulletin.*

Johnson, Jeffrey R., and John A. Ford. 1999. The challenge for global electronic commerce: Building trust on a solid foundation of security and privacy. Retrieved 27 January 2000 from the World Wide Web: http://www.equifaxsecure.com/pdfs/whitepaper.pdf.

Kalbfleisch, J.D., and R.L. Prentice. 1980. *The statistical analysis of failure time data.* New York: John Wiley & Sons.

Kavanaugh, J. 1997a. Child support system in trouble. *Government Technology* 10 (7): 8.

———. 1997b. LAPD technology office proposed. *Government Technology* 10 (3): 10.

Keen, Peter. 1991. *Shaping the future.* Boston: Harvard Business School Press.

———. 1986. *Competing in time.* Cambridge, Massachusetts: Ballinger.

Keider, S.P. 1984. Why system development projects fail. *Journal of Information Systems Management* 1 (3): 33–38.

Keil, M. 1995. Pulling the plug: Software project management and the problem of escalation. *MIS Quarterly* (December): 421–447.

Kerzner, H. 1998. *Project management: A systems approach to planning, scheduling, and controlling.* New York: Van Nostrand Reinhold.

Kichen, C., J. Murphy, and R.B. Levinson. 1993. Correctional technology: A user's guide. Grant no. 91P07GHM9, NCJ 149015. Washington, D.C.: U.S. Department of Justice, National Institute of Corrections.

Lacity, M.C., L.P. Willcocks, and D.F. Feeny. 1996. The value of selective IT sourcing. *Sloan Management Review* 37 (3): 13–25.

Laudon, Kenneth, and Jane Laudon. 1996. *Management information systems.* Upper Saddle River, New Jersey: Prentice Hall.

Lederer, A.L., and V. Sethi. 1996. Key prescriptions for strategic information systems planning. *Journal of Management Information Systems* 13 (1): 35–62.

Lederer, F.I. 1997. An introduction to technologically augmented litigation. Retrieved 14 January 2000 from the World Wide Web: http://courtroom21.net/auglit.html.

Lederer, F.I., and S.H. Solomon. 1997. Courtroom technology—An introduction to the onrushing future. Article submitted for the Fifth National Court Technology Conference (CTC5), National Center for State Courts. Retrieved 13 January 2000 from the World Wide Web: www.ncsc.dni.us/ncsc/tis/ctc5/103.htm.

LIS, Inc. 1995. Technology issues in corrections agencies: Results of a 1995 survey. Report submitted to the National Institute of Corrections, Washington, D.C.

Lively, G.M. 1996. Thinking globally to act locally: NIJ improves worldwide access to criminal justice information. *National Institute of Justice Journal* 230: 2–8.

Loundy, D. 1998. E–LAW 4: Computer information systems law and system operator liability. *Seattle University Law Review* 21 (4).

Lucas, H.C., Jr. 1975. *Why information systems fail.* New York: Columbia University Press.

Maltz, M. 1984. *Recidivism.* Orlando, Florida: Academic Press.

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

Martin, James. 1995. *The great transition.* New York: American Management Association.

Mason, R.O., F.M. Mason, and M.J. Culnan. 1995. *Ethics of information management.* Thousand Oaks, California: Sage Publications.

Matthews, J.R., W.H. Dutton, and K. Kraemer. 1976. *The County Information Systems directory 1975.* Irvine: University of California, Public Policy Research Organization.

Matthews, J.R., K. Kraemer, L. Hackathorn, and W.H. Dutton. 1976. *The Municipal Information Systems directory 1975.* Irvine: University of California, Public Policy Research Organization.

McFarlan, F.W., and R.L. Nolan. 1995. How to manage an IT outsource alliance. *Sloan Management Review* 36 (2): 9–23.

McLeod, Graham, and Derek Smith. 1996. *Managing information technology projects.* Danvers, Massachusetts: Boyd & Fraser Publishing Company.

Mechling, J., and T. Fletcher. 1996. *Information technology and government: The need for new leadership.* Cambridge: Harvard University Press.

National Information Infrastructure Task Force. 1997. Options for promoting privacy on the national information infrastructure. Retrieved 12 January 2000 from the World Wide Web: http://www.iitf.nist.gov/ipc/privacy.htm.

Northrop, A., K. L. Kraemer, and J. L. King. 1995. Police use of computers. *Journal of Criminal Justice* 23 (3): 259–275.

Northrop, A., K.L. Kraemer, D. Dunkle, and J.L. King. 1990. Payoffs from computerization: Lessons over time. *Public Administration Review* 50 (5): 505–514.

Polansky, Larry. 1996. The long and winding road. *Court Technology Bulletin* 8:2.

Information Infrastructure Task Force. 1995. Privacy and the national information infrastructure: Principles for providing and using personal information. Retrieved 12 January 2000 from the World Wide Web: http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html.

Quinn, J.B., and F.G. Hilmer. 1994. Strategic outsourcing. *Sloan Management Review* 37 (4): 43–55.

Reaves, B., and P. Smith. 1995. *Law enforcement management and administrative statistics, 1993: Data for individual State and local agencies with 100 or more officers.* NCJ 148825. U.S. Department of Justice, Bureau of Justice Statistics.

Regan, E.A., and B.N. O'Connor. 1994. *End-user information systems.* New York: Macmillan.

Reno, Janet. 1997a. Keynote address by U.S. Attorney General Janet Reno on high tech and computer crime. Presented at the Meeting of the P8 Senior Experts' Group on Transnational Organized Crime, 21 January, Chantilly, Virginia. Retrieved 12 January 2000 from the World Wide Web: http://www.usdoj.gov/criminal/cybercrime/agfranc.htm.

———. 1997b. Letter to members of Congress regarding law enforcement's concerns related to encryption, 18 July. Retrieved 12 January 2000 from the World Wide Web: http://www.usdoj.gov/criminal/cybercrime/crypto.html#IVc.

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

Roberts, D.J. 1998. *Integrated justice information systems for State and local jurisdictions: An overview of planning activities for the Office of Justice Programs.* Sacramento, California: SEARCH.

Schmidt, P., and A.D. Witte. 1989. Predicting criminal recidivism using "split population" survival time models. *Journal of Econometrica* 40:141–159.

———. 1984. *An economic analysis of crime and justice: Theory, methods, and applications.* Orlando, Florida: Academic Press.

Scoggins, J., T.H. Tidrick, and J. Auerback. 1986. Computer use in local government. *The municipal year book 1986.* Washington, D.C.: International City Management Association.

SEARCH. 1997. *Survey of State criminal history information systems, 1995.* Cooperative agreement no. 95–RU–RX–K001, NCJ 163918. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

———. 1993. *Survey of criminal history information systems, 1993.* Grant no. 92–BJ–CX–K012. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

SEASKATE, Inc. 1998. *The evolution and development of police technology.* Technical report prepared for the National Committee on Criminal Justice Technology. Grant no. 95–IJ–CX–K001 (S-3), NCJ 173179. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Sparrow, Malcolm K. 1994. *Imposing duties: Government's changing approach to compliance.* Westport, Connecticut: Praeger.

———. 1993. *Information systems and the development of policing.* Perspectives on Policing, NCJ 139306. Washington, D.C.: U.S. Department of Justice, National Institute of Justice, and Harvard University, John F. Kennedy School of Government.

———. 1991. Information systems: A help or hindrance in the evolution of policing? *Police Chief* 58 (4): 26–44.

———. 1988. *Implementing community policing.* Perspectives on Policing, NCJ 114217. Washington, D.C.: U.S. Department of Justice, National Institute of Justice, and Harvard University, John F. Kennedy School of Government.

Sparrow, M.K., M.H. Moore, and D.M. Kennedy. 1990. *Beyond 911: A new era for policing.* New York: Basic Books.

Standish Group. 1996. Unfinished voyages. Retrieved 13 January 2000 from the World Wide Web: http://www.standishgroup.com/voyages.html

———. 1995. Chaos. Retrieved 13 January 2000 from the World Wide Web: http://www.standishgroup.com/chaos.html

State Justice Institute. 1997. *Improving the quality of American justice 1987–1997.* Alexandria, Virginia: State Justice Institute.

Tapscott, Don, and Art Caston. 1993. *Paradigm shift.* New York: McGraw-Hill.

Thayer, R.H., A. Pyster, and R.C. Wood. 1982. Validating solutions to major problems in software engineering project management. *Computer* 15 (8): 65–77.

Travis, J. 1997. Technology in criminal justice: Creating the tools for transformation. Opening address to the Academy of Criminal Justice Sciences, 13 March. Retrieved 13 January 2000 from the World Wide Web: www.ojp.usdoj.gov/nij/speeches/acjs.htm.

Trojanowicz, R., and B. Bucqueroux. 1990. *Community policing: A contemporary perspective.* Cincinnati: Anderson Publishing Company.

Turban, E., E. McLean, and J. Wetherbe. 1999. *Information technology for management.* New York: John Wiley & Sons.

Turner, J.A. 1982. Observations on the use of behavioral models in information systems research and practice. *Information and Management* 5:207–213.

U.S. Department of Commerce, Office of Technology Policy. 1997. *America's new deficit: The shortage of information technology workers.* Retrieved 12 January 2000 from the World Wide Web: http://www.ta.doc.gov.

U.S. Department of Justice, Association of State Correctional Administrators, Corrections Program Office, Bureau of Justice Statistics, and National Institute of Justice. 1998. *State and Federal corrections information systems: An inventory of data elements and an assessment of reporting capabilities.* NCJ 170016. Washington, D.C.

U.S. Department of Justice, Bureau of Justice Assistance. 1996. *System integration: Issues surrounding integration of county-level justice information systems.* Monograph, NCJ 156841. Washington, D.C.

U.S. Department of Justice, Bureau of Justice Assistance. 1994. *Understanding community policing: A framework for action.* Monograph, NCJ 148457. Washington, D.C.

U.S. Department of Justice, National Institute of Corrections. 1995. *Survey of corrections technology.* Washington, D.C.

U.S. Department of Justice, National Institute of Justice. 1998. *Building knowledge about crime and justice: The 1999 research prospectus of the National Institute of Justice.* NCJ 172883. Washington, D.C.

U.S. Department of Justice, National Institute of Justice. 1994. National Institute of Justice announces opening of the National Law Enforcement Technology Center. *Technology Beat* (October): 1–2.

U.S. General Accounting Office. 1997a. *High risk areas: Actions needed to solve pressing management problems.* Doc. no. GAO/AIMD/GGD–97–60. Washington, D.C.

———. 1997b. *Managing technology: Best practices can improve performance and produce results.* Doc. no. GAO/T–AIMD–97–38. Washington, D.C.

———. 1996. *Information technology investment: Agencies can improve performance, reduce costs, and minimize risks.* Doc. no. GAO/AIMD–96–64. Washington, D.C.

———. 1994. *Executive guide: Improving mission performance through strategic information management technology: Learning from leading organizations.* Doc. no. GAO/AIMD–94–115. Washington, D.C.

U.S. House. 1997a. *Computer Security Enhancement Act of 1997.* 105th Cong., 1st sess., H.R. 1903. Retrieved 27 January 2000 from the World Wide Web: http://thomas.loc.gov/cgi-bin/query/z?c105:h.r.1903.

———. 1997b. *Data Privacy Act of 1997.* 105th Cong., 1st sess., H.R. 2368. Retrieved 27 January 2000 from the World Wide Web: http://thomas.loc.gov/cgi-bin/bdquery/z?105:h.r.2368.

Walker, J.D. 1995. The challenging voyage to statewide court automation. *Court Technology Bulletin* 7 (2): 9.

Walker, L. 1996. Court technology information trends. *Court Technology Bulletin* 8 (2): 7.