Chapter Eight
Agency Systems

Learning Objectives

• The student will understand the reasons that good record keeping is critical to law enforcement.
• The student will understand the concept of operator security, including the concepts of right to know and need to know.
• The student will understand the purpose of record management systems (RMSs), jail management systems (JMSs) and evidence management systems (EMSs) and how they generally work.
• The student will understand the impact of concepts like the Freedom of Information Act on police records.
• The student will be introduced to the concept of digital images in law enforcement.

Introduction

In the first chapter we developed the idea that police work is primarily about the gathering, analysis, retention, and use of information. State and local police agencies collect a vast and varied amount of information. For instance, we saw in the previous chapter that most computer-aided dispatch (CAD) programs retain information about calls for service. Consider that the millions of calls each year received by a public safety answering point (PSAP) become millions of individual records. Moreover, each of those records could have subpieces of information like the location, disposition, and officer(s) handling the call, etc. A police record system is how that and other information is retained and organized.

The information retained by police agencies runs the spectrum from crime reports to personnel records. Because of the type of information the police collect, the information needs to be readily available, kept for a long time, and held confidentially. Arrest reports are good examples of documents that must be available yet confidential. Presume that an arrest ultimately leads to a conviction. Even though the person has been convicted, there is always the possibility that something will occur and the original arrest report will be needed for review. For instance, say ten years after someone’s conviction, evidence comes to light that may tend to prove his or her innocence. What if the police can’t find the original report? What if the court file is incomplete or missing? Do we just say we are sorry?

Many individual law enforcement agencies have very sophisticated records systems capable of producing the full range of statistics on their own activities. However, a 2000 Bureau of Justice Statistics report indicated that less than half of all local police agencies maintained computerized files on warrants. Think back to our traffic violator from the first chapter, if the violator had been wanted by an agency that did not keep computerized files on warrants, how would the police officer issuing the citation ever find out that the traffic violator was wanted?

In reality, the situation on warrants and police records isn’t all that dismal. A closer look at the BJS report shows that although only 43 percent of the agencies have computerized files on warrants, when you look at state and local agencies that have a service population of more than ten thousand, the majority of the
agencies have computerized files on warrants, alarms, traffic stops, and criminal histories. That means that most police officers in the country have access to computerized records. The problem of a lack of record automation becomes more acute as one examines the very small police agency. The problem of fragmentation is probably most acute in the area of police records.

A little later in the chapter, when we take a look at the benefits of record automation, we will see that even small police agencies and the communities they serve can reap huge benefits from records automation. Of course, the people working in the small agencies have already discovered this, and their efforts to join the information age have somewhat added to the problem of fragmentation. If you are ever in a position to make decisions about systems design, purchase, or implementation you will learn about first tier and second tier manufacturers.

If you were designing a system for a large agency and you had great pots of money, you would probably contract with a first tier manufacturer. One of the primary reasons for this is that when government is spending a lot of money, it has a cumbersome procurement procedure that requires a bidder to complete often very complex and lengthy bid forms. In Chapter Twenty, Implementing and Managing Technology, we will go into this in a little more depth. For now, realize that there is a direct relationship between the amount of money government is going to spend with one provider and the amount of paperwork, approval cycles, and politics connected to the purchase.

Any manufacturer that wants to bid on a large project is going to have to spend a considerable sum of money just to bid. Moreover, large projects tend to be complex and users from large state and local police agencies tend to want their systems custom designed. So first tier manufacturers (of both hardware and software) are large companies. Those large companies are set up to produce quality, custom-designed software and hardware configurations. Because of the large amount of money first tier companies have spent on just getting in the door and

Figure 8.1 Both digital data and voice pass through radio equipment like this trunk-mounted radio transceiver.
Photograph provided by Havis-Shields Equipment Corporation.
maintaining their own internal infrastructure to design large systems, there is little or no profit for them to make with the small agencies. This does not mean that small agencies don’t purchase equipment from large companies—they do have vehicles, computers, and software from major firms—but generally, when they do purchase from major firms, they purchase off the shelf and not custom designed (Figure 8.2). This is more true with hardware than software.

If you were a large firm that spent millions of dollars developing a sophisticated software application designed to automate police records, and you could sell the product to large agencies and make a profit, would you sell the product for less to a smaller agency because they were small? Return for a moment to the hamburger stand. When you purchase a hamburger, does the hamburger stand ask you how much money you have? Would they sell it to you for less because you had less than the person in line behind you? The analogy may become more clear if you think of a fancy restaurant and a hamburger stand. In both you get food. In the more expensive restaurant, you get personal service, there is a wider variety on the menu, and it is cooked to your exact tastes, etc. In the hamburger stand, even though they tell you they will cook it the way you want it, there are only so many variations to a five-minute hamburger. The fancy restaurant is first tier; the hamburger stand is second tier. Both are filling, but the experiences are different.

Figure 8.2 In the last chapter, we looked at CAD and 9-1-1 as a means for civilians to contact the police. However, CAD and 9-1-1 can be used for the police to contact the community. One of the relatively inexpensive tools they can purchase is a telephone notification system that, through their dispatch center, has the capability identifying and telephoning thousands of people with emergency instructions. Using GIS and CAD, an area is selected, numbers are dialed, and a prerecorded message is delivered. It can be used for neighborhood crime alerts, evacuation instructions, and neighborhood watch notifications. This system might be simpler for a small- to medium-sized local agency than a large local or state agency to implement. Source: “Evolution and Development of Police Technology,” 113.
Many second tier products are very good, but when you talk to second tier manufacturers, they will tell you that small agencies struggle to purchase even from a second tier manufacturer. In one conversation I had with a second tier manufacturer, they told me a story of a small agency that held a bake sale to purchase the manufacturer’s product. So as the small agencies struggle to implement second tier products, the large agencies have different struggles with first tier products. The result is that many of these systems are incompatible, and the smaller agencies do not gain the expertise that the larger agencies have; the problem of fragmentation and the resulting effects continue to grow.

We are not the first ones to struggle with fragmentation. The problem has been long recognized. Realizing the importance of local police records and the problems with fragmentation, between 1995 and 1999, the United States Office of Criminal Justice Programs (OCJP) granted more than $265 million dollars to state and local governments for the purposes of upgrading their criminal records. Moreover, the literature is replete with information and case studies on local law enforcement agencies that have used grants from state and federal authorities for the purpose of upgrading their records systems. The growing attention paid to state and local law enforcement records management is because of the value of the information gathered by police agencies.

Much of the focus today is on criminal justice information systems. It is important to realize that there is a difference between criminal justice information systems and police records management. Criminal justice information includes every piece of information gathered in and used by the criminal justice system. It might be court transcripts of testimony, parole or probation records, state drivers’ licenses records, privately gathered information, or police calls for service. It is information used for decision making at every level and stage of the criminal justice process. On the other hand, when we refer to police records management, we are primarily concerned with information gathered, retained, and organized solely by the police. However, a fully integrated police records management system is going to have access to all of the other records maintained by different criminal justice organizations.

The primary purpose of retaining and organizing information is so we can make better decisions. In criminal justice, good information is critical in good decision making. At the most basic level, police records have two basic roles. The first is to supply information, so good decisions can be made about offenders. The second purpose is to supply information for management decisions. Information about offenders might be crime reports, evidence, and their location in a jail. Management information might be crime data used for tactical and strategic planning, calls for service data to be used for resource allocation, or personnel records for use in personnel decision making.

It should be fairly clear that criminal justice organizations, including the police, operate on information. In addition to the need for good information, that information needs to be accessible and timely. Recall our traffic violator—if the police officer doesn’t know the offender is wanted, the police officer cannot take action on the warrant. The police officer might not know because his agency’s system is incompatible with the agency that holds the warrant. The information simply is not accessible to the police officer. The agency responsible for updating a database that contains warrants might not do so in a timely manner, so the police officer in the field lacks the information. Accessibility and timeliness are two of the motivating factors behind the need to automate police records.

There are many benefits to record automation—detectives can track gangs, ensure the chain of custody of evidence, and coordinate the recovery of stolen property.
Police officers in the field are safer because they have better information. Police managers can make better decisions about resource allocation. Moreover, automation generally means less paper and can reduce staff costs (Figure 8.3). Police officers can access policy and reference manuals in searchable, online databases. References and referrals as sources of solving neighborhood problems become more available. Simply put, ready access to good data can improve decision making.

As we look at agency systems, the importance of total information resource management cannot be overemphasized. In addition to automation, there are security and privacy issues that are important for a state or local law enforcement agency to consider. The information has to be accessible, but only to those who are authorized.

Information Security and Accuracy

Before we begin to look at agency systems, we need to understand the concept of operator security. In Chapter Four, we briefly looked at encryption as a means to prevent unauthorized access to transmissions. What we learned was that if encrypted data was intercepted by an unauthorized party, the likelihood that the data could be understood was reduced, and different levels of encryption provided different levels of protection. However, what we find in law enforcement is when information is compromised, authorized users primarily do it...
intentionally. It is far easier to protect the system from being compromised by technology than it is to protect the system from being compromised by our own. Generally, information collected by law enforcement and to which law enforcement users have access is considered privileged information. That means that the information is for official use only. There are a variety of reasons that information is privileged or confidential. Perhaps the general dissemination of the information would compromise an investigation. For instance, let’s say that you are investigating a murder. You, as the investigator, are privy to all information and evidence about the crime scene, and as you may find out as an investigator, not all information is introduced in a trial. There are a variety of reasons that evidence won’t be introduced or that the defense lawyer will successfully suppress the evidence. That means that the jury should only hear the evidence that is lawfully presented. If the details of your crime scene become public knowledge, there is a possibility that the jurors will hear evidence that will not be admitted in the trial. The result could be that the suspect does not receive a fair trial. If the information is damaging enough, it might mean that the suspect who actually did the murder will not be punished.

Law enforcement personnel also have general access to a wide variety of information about the average person that is confidential and protected by law. For instance, recall our traffic violator from the first chapter. Our officer could have accessed the state driving records in order to determine if the traffic violator’s license was valid (Figure 8.4). At the same time, the police officer would have obtained the traffic violator’s home address. The information contained in the driving record is confidential because the information could be used to harm the traffic violator. Prior to stricter regulations in California, driver’s license infor-

**Figure 8.4** The ASTRO Saber™ digital radio is an example of a state-of-the-art portable radio designed to work in both a digital and analog environment. Police officers in the field who do not have access to an in-car computer often use portable radios to request information about traffic violators. *Photograph provided by Motorola.*
information that was released to a private party resulted in someone stalking and killing an aspiring actress.\(^7\)

The idea of operator security introduces two concepts with regard to police access to information, whether a document or an information database: the **right to know** and the **need to know**. In the first chapter, when our police officer stopped the traffic violator for speeding, the police officer had the right to know information about the violator's driving records. As a part of the police officer's job, he has the right to know information that will further an investigation. So the right to know is derived from the police officer's occupation. Police officers have the right to know certain privileged information.

The second part of the concept on operator security is the need to know. The need to know is derived from the situation. In the instance of the traffic violator, the officer had the right to know based upon his occupation and the need to know based upon the traffic violation. What if the police officer was off duty, and his next-door neighbor wanted to know if her long lost Aunt Sally was still alive. Put yourself in that situation—all your neighbor wants to know is the home address of her Aunt Sally. Do you have the right to know that information? Yes. You are a police officer. Do you have the need to know that information? No. What if Aunt Sally doesn’t want to be found by your neighbor? She is not going to be happy you gave out the information. Indeed if you passed the information to your neighbor, you probably committed an illegal act. The circumstances of your neighbor's request were an insufficient reason for you to need to know.

Information that police officers seek to further an investigation can have an additional layer of protection for the individual. Sometimes a police officer needs a search warrant to obtain information. Information that generally requires a search warrant or court order includes telephone company records (the numbers called from and incoming to a telephone), live conversations of any electronic medium, and certain commercial credit information, just to name a few. In Chapter Nine we will look at some external sources of information that require a search warrant. We will find that there is a tremendous amount of commercial information that does not require a warrant. Moreover, in Chapters Fourteen and Fifteen, when we look at the technology involved in covert operations, we will see that sometimes a search warrant is required and sometimes not. For now, think of a search warrant as the judicial review of a police officer's right to know and need to know. That is the simplest definition of the probable cause necessary to gain a search warrant or court order.

So the first protection for the security of police data is training people to realize their ethical responsibilities with confidential information. But as we know, networks and computer systems have some vulnerabilities of which we should be aware. Although we touched on many of these network and systems security issues in Chapter Four, looking at them in the context of their practical uses will give us a greater understanding of their value. For instance, one of the best attributes of twenty-first century information technology (IT) is its size and portability. Computers on desks, in vehicles, and held in users' hands are networked together and provide the ability to access information just about anywhere. We have seen that if our mythical police officers had access to information about a traffic violator, he or she could make better decisions. But in addition to being accessible and portable, these systems are at risk because they are small enough to be easily lost or stolen. One research paper on e-government found that 80 percent of security breaches in wireless government networks occurred because someone's device was lost or stolen.\(^8\)
Security breaches via lost or stolen equipment can be minimized by educating employees, having clear rules and regulations concerning the field use of equipment (like locking the police vehicle doors when away from the vehicle), and using passwords. As we know from Chapter Four, passwords are a valuable method of keeping unauthorized users out of databases. In addition to passwords, networks and databases are usually designed to keep a log of use. In other words, each time a user accesses a database via a network, the database records the node that requested the information, the time of the request, the user who was signed on, and the nature of the request or data that was provided. Data logs provide managers with a means to audit information databases for unauthorized use. Moreover, a good database will monitor use and make notifications to the managing authority when users make an unusual number of inquiries, or in some cases certain records are flagged if the information is accessed.

In addition to needing a password for access, some password systems provide for different levels of access to databases. Most police officers have access to agency information, but they cannot add, change, or delete information. A password scheme that provides levels of access ensures database integrity. It is protected from unauthorized tampering. One last security measure that is similar to passwords is the process of authentication. Authentication occurs when a user enters a password and the password is checked by the database. More sophisticated authentication procedures may include the database checking to make sure that the node requesting the information is an authorized node. So when you access a database using authentication, your computer is examined by the computer managing the database to ensure your node is a registered and authentic requestor.

One of the primary reasons that database security is critically important for state and local law enforcement agencies is the type of information those databases contain. Police databases are capable of storing a tremendous amount of information, and most of that information is about people. Whenever information about individuals is stored, questions concerning their privacy need to be considered and respected. Privacy can be defined as information that, if exposed, could create a sense of nakedness for the person the information concerns. There are lots of things about us that are not bad, but if other people knew them, we would feel exposed. Those things are private matters. One of the most common issues for law enforcement is divulging information about victims, witnesses, and offenders to the news media.

The name of a victim of sexual assault is routinely protected from being divulged to the public. There are a variety of state laws that require that law enforcement agencies do not release the names of victims of sexual assault. Moreover, failure to protect the victims’ privacy can result in civil litigation. In one instance, an agency accidentally released the name of a victim of sexual assault. The victim’s name was subsequently published in a newspaper, along with a variety of details regarding the assault. The law enforcement agency settled out of court for $2,500; the newspaper lost the trial, and the jury awarded the victim $100,000. Subsequent to the trial, the state appeals court upheld the award, but the United States Supreme Court eventually overturned the decision.

For state and local law enforcement agencies, there are four areas of concern regarding the data they collect. First, information about someone can be considered their personal property. If information is property, it could be subject to the restrictions of police seizure as outlined in the Fourth Amendment of the United States Constitution. Second, when state and local agencies collect information about victims, as in the case of sexual assault victims, the victim trusts that the
agency will not reveal the information. Third, if the person’s information is revealed, it could cause the person to suffer, as in defamation. Finally, using a person’s likeness, as in a booking photograph, raises issues of ownership.  

There are so many uses for information that can improve state and local police efficiency and effectiveness, information collection is very likely to increase. A possible opposite view is that the mass of information collected by state and local police agencies is tantamount to an invasion of privacy. It could be that just as incident-driven policing drove a wedge between the community and the police, twenty-first century information gathering may cause the community to lose confidence in police agencies. The goal of state and local law enforcement agencies is to seek a balance between privacy and the use of information.

One of the ways that public confidence in police information gathering can be balanced is to provide mechanisms whereby people can access the information about them. There are a large number of cases where the United States Supreme Court has addressed the right to know information about oneself. When these cases are examined in total, they provide three situations where a private person has the right to know what information the government has collected about her. The first situations simply are the times in which state and local law enforcement agencies are prevented from intercepting communications by private citizens. Situations that fall under the first category are the Fourth Amendment–related subjects we will examine later. The next situation is where the government must fulfill a citizen’s demand to know what information the government has obtained. This obligation is commonly referred to as the Freedom of Information Act (FOIA). The FOIA relates specifically to the federal government. However, many states have similar disclosure laws. The final requirement that the government balance information with privacy involves situations wherein there is a necessity to

### A Look Ahead

In Chapters Fourteen and Fifteen, when we look at the various technological means of surveillance, we will explore the constitutional restrictions on data gathering in more depth.

One option for an agency to consider when developing a policy to balance data and privacy is to adopt the Code of Fair Information Practices, which was the central contribution of the HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems, established in 1972.

The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person’s consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

requirement that the government take affirmative acts to inform people of information. Again, in Chapter Fourteen we will see an example of this when we look at wire intercepts. For now, remember these three situations.

16 The last thing that should be reemphasized is that data systems must be backed up very often. 17 By keeping a backup in a different location than the main system, data security is enhanced.

Turning Data into Information

When organizations first started to collect information, a number of systems were created to organize this information so that it could be recalled and used. One of these schemes was referred to as indexing. There are some police agencies that still use this scheme. An example of indexing can occur when someone comes into police custody. The original report about the arrest is sent to a records person. That person creates a three-by-five card, which has the offender’s name and other identifying information. The card is assigned a master number, and the number of the arrest report is recorded on the card. If the person is arrested again, the card is pulled and the number of the new arrest report is recorded; the police reports themselves are then filed separately. If you were an investigator and wanted to know about an offender’s prior criminal history, you would go to the index file, pull the card, and write down the numbers of the previous arrest reports. With those numbers, you could go to the original report file, pull the reports, and gain your information. This type of indexing has been done with offenders, victims, witnesses, evidence, and just about all police data. Of course, now we have indexes in databases and looking up information is simpler.

In Chapter Two we briefly looked at relational databases. One of the primary things to remember is that relational databases consist of records that are broken down into fields. 18 The relationships between records depends on the accuracy and dependability of the information entered into the fields. 19 The relational database is the foundation of modern police records management systems (RMSs). 20 As with Chapter Seven, we are presuming the agency we are examining is fully integrated and, therefore, all other software and systems eventually report data to and obtain data from our RMS. Moreover, an RMS can be the agency’s

---

**Selected Portion of Freedom of Information Act**

Title 5, U.S. Code Part I, Chapter 4, Subchapter II, Section 522: “This Section does not apply to records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigation or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.”
Unfortunately, many local law enforcement agencies have existing records management systems that are unable to report the new National Incident-Based Reporting System (NIBRS). Sometimes they cannot comply with new federal standards because they continue to follow an old, hierarchy-based reporting system, or their systems are simply antiquated and unable to be updated. In Chapter Nine on external systems, we will explore NIBRS and the importance of an incident-based reporting system will become clearer. In that chapter we will also take a much closer look at the National Crime Information Center. Moreover, in Chapter Twelve, when we look at crime analysis, you will see how a fully integrated, incident-based reporting system has the potential to significantly increase state and local law enforcement agencies’ efforts in problem solving.


How we choose to initially organize a relational database will greatly affect its future usefulness. Remember in Chapter Seven when we looked at computer-aided dispatch (CAD), we saw that CAD automatically creates an incident number. In most police agencies, that incident number is different from any crime or arrest report number. So a relational database would have to cross-reference those numbers in order to obtain all the information about a particular incident. If the agency is fully integrated and the CAD-created incident number is also the crime, arrest, or incident report number, then a query of the relational database by incident number would give you all the information available.

The importance of field description in a relational database cannot be overemphasized. Let’s presume that you want to query a relational database about all of the activities of a particular officer. Would you query by name? Badge number? Employee number? All of the queries could be successful, but if you query by name, especially in a large agency with an in-depth historical database, you would need a full name and probably date of birth, and chances are you would come up with more than one record. If you queried by badge number, you would find that badge numbers are often reissued. If a police officer gets promoted to sergeant, he gets a new badge—most likely with a different number. If you query by employee number, that number should be the only one ever issued—like your social security number. A query by employee number would give you full name, date of birth, all badge numbers, and all incident numbers involving that employee.

So in most instances when we ask a database a question, we have to define the parameters of our search. A parameter is simply a value that we send to the computer. Say you want to find out about police reports at 123 North Main Street. If you queried a relational database, it would return all reports at that location. In a large agency, that could be dozens of reports. So you refine your search by asking the database to tell you about all of the reports that occurred in the past thirty days. You would send the values of “123,” “North,” “Main,” “Street,” and your inclusive dates. Depending on the program, your computer could give you just the specific information you asked for So no reports that did not have all of those values would return to you. What if the person who entered the data forgot to include North, or confused North with South. The point is, when working with databases, you must consider the programming (will it only answer what I ask?) and the data entry.
In a fully integrated agency, the record management system is likely to consist of several smaller systems (like CAD and GIS) that exchange information with a master server. However, when you ask questions, you may also only ask questions of a specific database within the agency. For instance, if you were a police officer in the field, and you were checking a traffic violator for warrants, you would only be interested in querying your agency’s warrant file and perhaps a regional database and the national database. When parameters of a search are defined, often the first decision is which database to turn to. Luckily for us, those decisions are made by programmers before we have to use systems. In other words, if you want to know about warrants, an agency system probably has predefined query fields that only check the warrant system (Figure 8.5).

Return to our traffic violator for a moment. In many instances, when the police have contact with someone, that person does not have identification, or the police officer has reason to suspect the identification. This means the people are often checked for traffic warrants based upon information they provide—and people can be misleading, both intentionally and unintentionally. An unintentional way that people provide misleading information can be their weight. Presume our traffic violator doesn’t have any identification and when he reports his weight to the police officer, he gives his current weight. Unbeknownst to our police officer, the violator’s current weight is correct, but it doesn’t reflect the fifty pounds he lost while in prison. There could be a warrant for the violator that reports the preprison weight. Software designed to circumvent this problem searches for things like height and weight within predefined parameters. It asks the database something like, “give me all wanted persons between the weights of 150 and 170.”

Of course, then there are people who intentionally mislead. Sometimes an offender who believes she is wanted will give a different spelling of her name. For instance, a person named “Walker” might give the name “Wacher.” Her hope is that by providing a derivative of her name she can both remember her lie and escape detection. Some want and warrant software employs a search technique not specifically designed to uncover falsehoods, but to handle the many different spellings of words that sound the same.

Names and words that are misspelled can be a problem for database designers. Names can have different spellings, and they are not unique. Some names have a diversity of ethnic origins, which give us similar pronunciation but different spelling. This problem is solved by phonetic algorithms that can find similar-sounding terms and names. These algorithms are often called SoundExes. They are named after the original patent design created by Margaret O’Dell and Robert C.

---

**Try This**

People provide police officers with misleading information in many situations. However, they try to make up information about themselves that they can remember—like using a relative’s name instead of their own. However, dates of birth are tricky for offenders. Police officers check date of birth information during a field interview by asking confirming questions at different points in an interview. For instance, the year of a date of birth can be verified by asking someone’s age. If he tells you he is 40 but born in 1959, something is amiss. The month of his birth can be verified by asking the confirming question, “What is your Zodiac sign?” If someone tells you he was born in October, but his sign is Aquarius, something is wrong. The important point is the technology is much more effective when the users are better trained in getting good data for inquiry. Try these interview techniques on someone.
Russel in 1918. Most variations of the software work in a relatively similar manner. They convert the name into a code, or key, consisting of the first letter, followed by several numbers that are assigned based upon a predetermined grouping of consonants. The result is the ability to search a database that contains words that sound the same but are spelled differently.

In addition to allowing us to obtain information on individual offenders, relational databases can be used for a number of strategic purposes such as deployment and crime analysis. Two types of inquiries are often made when working on strategic matters. The first is a conditional query—find all white males who were victims of crimes. The second is considered an ad hoc query—find all radio calls at 123 North Main Street, before October 1, 2002.

The final aspect of relational databases is their ability to populate other related documents. Take, for instance, our radio call from the previous chapter. Once the dispatcher entered the information about the call into CAD, that information could be used to populate the fields of subsequent systems. For instance, if our police officers in the field arrested someone, some information from CAD could populate the police officer’s laptop in her vehicle. During the booking process, once the CAD incident number was accessed, information about the radio call could be automatically put into the other systems, such as jail management or evidence management. This transference of information is handled by the agency’s record management system.

In a fully integrated agency, RMS data is imported to and from a central server. There are as many configurations of networks, systems, databases, and computers as there are agencies who set them up. The important thing to
remember is that RMS is the software umbrella to and from which all other database systems report.\textsuperscript{28}

**Police Hardware and Software**

Most police employees don’t directly access the agency’s RMS. Under some configurations, a police clerk might update records or data directly in the RMS, but generally speaking, state and local police officers access and update information through a variety of subsystems. Many of those systems are increasingly accessible to the police officer in the field through what is being referred to as the mobile office (Figure 8.6).\textsuperscript{29}

The field police officer’s mobile officer consists of the vehicle, the mobile radio system, and increasingly a mobile data computer (MDC). An MDC is a microcomputer, either much like a laptop or a laptop, installed in the vehicle. Using the MDC, a police officer can access driver’s license, local, state, and national wanted persons databases and databases concerning stolen vehicles (Figure 8.7). Moreover, an MDC can receive calls for service and allow the police officer to exchange e-mail-like transmission with the dispatcher.\textsuperscript{30} A few police agencies are beginning to test systems that will dramatically expand the capabilities of the mobile officer. In addition to receiving dispatch information and having the ability to make system inquires, new systems allow the officers to access mugshots, fingerprints, GIS maps, and even aerial photographs. All of these functions have the

**Figure 8.6** This photograph shows a typical arrangement inside a police vehicle. Both the police radio and the dash-mounted laptop computer are visible. Photograph provided by Havis-Shields Equipment Corporation.
In 1983 the Institute of Police Technology and Management, University of Florida, established a computer section. The IPTM computer staff develops a variety of software products for use in the criminal justice field. One GUI-based software application developed by IPTM is Police Trak Mobile, a wireless communications system. Using CDPD, GPS, or radio frequency data communications equipment, Police Trak Mobile gives the officer in the field the ability to query state and national crime information systems, run vehicle registration checks, run driver’s license checks, run wanted person checks, and much more. The system also combines an interface for CallTrak, IPTM’s CAD system, whereby officers can be dispatched at the touch of a button. Officers in the field can see current activity of all other officers in real time, check out calls and traffic stops, request case numbers, query both the CallTrak and Police Trak systems, and communicate with others on the system via instant messaging and e-mail. The text to speech capabilities minimize distractions while driving.

Permission for screen capture provided by the Institute of Police Technology and Management.

potential for enhancing officer safety and efficiency. It has been estimated that the mobile office concept can reduce the time a police officer spends in the station on paperwork by 37 percent. However, as we know from our earlier chapters, one of the challenges for these new, powerful systems is going to be bandwidth. Transfers of files containing images are going to have the potential for clogging the bandwidth and slowing the system. In the next chapter, when we look at external systems, we will see how these new mobile offices will allow officers to take full advantage of NIBERS and NCIC 2000.

If our police officer in the field took the traffic violator into custody, once at the station the police officer would interact with other software, such as a jail management system. Most local agencies do not house offenders for long periods of time, but they do house offenders while they are awaiting arraignment in court. During these two- or three-day stays, an agency assumes responsibility for
the care and well-being of the offender. This means meals, medical care, and visitors. Failure to properly administer this responsibility can lead to expensive litigation. Recall the Livescan fingerprinting device from Chapter Six, one integrated booking and jail management technology combines Livescan fingerprinting, automated fingerprint identification, and digital photography. Once the offender has been booked into the jail, the police officer then must complete the reports and secure any evidence. Again there is a software technology, connected to the RMS relational database that can ensure evidence is properly secured and documented (Figure 8.9).

**Image Processing**

A picture is said to be worth a thousand words. For the field police officer, having the ability to take photographs of offenders, traffic collisions, and crime scenes can be valuable years later when testifying in court. Look at your old family photographs, especially ones where you were present during the event. I am sure that they will bring back memories, and often by looking at a photograph...
closely you will remember long-forgotten details. Photographs used as evidence in court can have the same impact on witnesses (Figure 8.10).

Image processing systems are part of police technology. Documents, photos, fingerprints, and crime scene photographs can be scanned, digitized, and stored in the agency’s database. In the field, police officers can take photographs of suspects and crime scenes with digital cameras. With a digital camera, a picture is transferred to a color monitor and appears as an electronic image. One of the advantages of a digital camera is that the police officer can decide when the best possible picture is on the screen and then instruct the camera to capture that evidence. When the cost of film and developing is taken into account, digital photography can also be less expensive than regular photography. Moreover, because the image is a data file, it can be stored as part of an agency’s RMS, available for recall from a variety of subsystems. Initially, there was some reluctance to use digital photographs because digital photographs can be manipulated. We have all probably received an e-mail where someone has taken a celebrity or political figure and placed his or her face on some unflattering body. However, digital cameras have mechanisms that can make the file unalterable. More and more, these photographs are being accepted in court as valid representations of evidence.

Figure 8.9 While most local agencies do not hold prisoners for long periods of time, they may house an arrested offender until the offender can be transported to court or to the jurisdiction responsible for long-term custody. Nevertheless, during the period that an offender is housed by an agency, they have a number of responsibilities to fulfill. Medical care and feeding are two obvious functions. Depending on local laws and policy, they may have to allow visitation. Moreover, since offenders are often repeat customers of the system, any jail management system should be fully integrated into the agency’s overall record management system.

Permission for screen capture provided by Crimestar Corporation.
Chapter Summary

In this chapter we examined a number of aspects of police record keeping. While there are technical challenges to implementing an integrated record management system, there are other issues that are equally important. Among those issues are the concepts of operator security, the right to know, and the need to know. Essentially, the purposes of those concepts are to maintain data security and individual privacy in government databases. We spent a considerable amount of time talking about privacy and describing some of the ways users and policy makers should consider privacy.

A state or local law enforcement agency’s record management system is an umbrella system that allows the capture of information from multiple sources, bridges the agency to outside sources of information, and allows for different types of information queries. By and large, police data systems are relational databases. By placing information in tabular fields, agency employees can use the same data for multiple purposes. Data might be used for a single investigation, to
In Chapter Three, when we looked at wireless systems, we saw that the number of state and local law enforcement agencies that are using in-field computers is increasing, becoming fairly commonplace. In addition to police officers using the computers to make inquiries into databases (we will look at external databases like the National Crime Information Center and State Motor Vehicle information in the next chapter), they can prepare reports and log their activities. Among the information a police officer might log would be calls for service, self-initiated activities, and arrests. But computer logs can also be used to record information on the hours a police officer worked, the status of their police vehicle, and supervisory approval.

Permission for screen capture provided by Crimestar Corporation.

speed the booking process of a multiple offender, to do crime analysis, or for an analysis of workload and deployment. All of these different purposes are possible because of the way in which police data is captured, organized, and retained.

**Discussion Questions**

1. What other circumstances can you think of where a police officer may have the right to know information but not the need to know the information?
2. Visit your local police department or campus security office. Evaluate their record management system. What stage of record management development are they in? Are they paper driven? Do they rely on nonnetworked personal computers? Do they have an integrated internal network? Is their record management system integrated with the wider criminal justice system?
3. If the victims of sexual assaults should have their names kept confidential, how about the victims of other crimes? For example, what about a man who fell prey to an Internet financial scam or a woman whose home was burglarized? Should these people receive privacy protection similar to victims of sexual assault? If so, why? If not, why?
4. What other relational databases can you identify? Does the local college use one?
5. On the Web, go to ftp.rootsweb.com/pub/usgenweb/mo/andrew/census/1860/indexjeff.txt. This is the 1860 census report of Andrew County, Missouri. On your Web browser, click Edit, Find on this page, and enter “Robert.” How many did you find? That is very similar to the actions your computer takes when it searches a flat file. Go to the Bureau of Justice Statistics online database at www.ojp.usdoj.gov/bjs/ddt.htm. Click on the online statistics. Here you can compare a large number of variables on crime in the United States. Try your hand at it. This is an example of the ability of a relational database.

**Key Terms**

<table>
<thead>
<tr>
<th>Criminal Justice Information Systems</th>
<th>Freedom of Information Act</th>
<th>Record Management System (RMS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence Management System</td>
<td>Jail Management System</td>
<td>Right to Know</td>
</tr>
<tr>
<td>First Tier</td>
<td>Need to Know</td>
<td>Second Tier</td>
</tr>
<tr>
<td>Flagging Records</td>
<td>Operator Security</td>
<td>SoundExes</td>
</tr>
<tr>
<td></td>
<td>Privacy</td>
<td></td>
</tr>
</tbody>
</table>

**Endnotes**

1. “Overview of NIBRS”
2. Pastore and Maguire, eds. *Sourcebook of Criminal Justice Statistics*.
4. Ibid.
7. In 1989 Rebecca Schaeffer, a twenty-one-year-old actress, was murdered by Robert Bardo, a mentally ill man who stalked her. Bardo obtained Schaeffer’s home address for $250 from a private investigator. At the time of the murder, anyone with one dollar could get the Department of Motor Vehicle (DMV) records on any other person. Since that time, the law has been changed in California, so that DMV records are not so readily obtainable. However, there are still other methods using commercial databases that home addresses can be found (refer to Chapter Nine in this text). More information about Schaeffer’s murder can be found at crimemagazine.com/stalkers.htm. You can find a review of measures the California DMV has taken to protect individual privacy at www.dmv.ca.gov/dl/authority.htm#protects.
12. See note 10 above.
15. Ibid., 628.
19. See note 17 above.
20. Ibid., Appendix.
22. Ibid.
25. See note 21 above.
28. See note 21 above.
29. Ibid.
32. See note 8 above.