9 TECHNOLOGY AND COMMUNICATION

A New Frontier

> *When I started my career in law enforcement nearly 35 years ago, the only "technology" we needed was the police radio and the location of the nearest pay phone. Today police radios scan 30 channels and officers typically have in-car video cameras, traffic monitoring radar units, in-car computer data terminals with Internet access, body cameras, a department issued cellphone and, of course, personal cellphones. With all this technology in the cruisers, it's a wonder we don't have more officer-involved crashes than we do.*[1]
>
> —Brian Cain and Michael Bostic, *Police Magazine*

The criminal justice field has made tremendous strides in the last 40 years, with the most notable developments being in the area of law enforcement and corrections. The process of prosecution or the application of law has undergone societal changes; and court decisions have altered some of the protections afforded offenders and, in some cases, hindered law enforcement. Technological advances in the area of crime detection, investigation, incarceration, and communication have made the greatest impact.

When I began my career in policing, sidearms, nightsticks, and car radios were all the tools required of a patrol officer. The first portable radios were low band frequency, limited range, heavy, and awkward. Communication was limited to the individual officer's local dispatch center. Communication between agencies required phone calls among the various entities, a time-consuming and difficult process. The scenario that follows demonstrates how communication between agencies (interagency communication) was handled in the 1970s and 1980s.

LEARNING OBJECTIVES

After students have completed this chapter, they will be able to do the following:

1. Identify and explain how criminal justice agencies are using technology to improve communication, investigation, prosecution, and incarceration
2. Identify types of social media, and explain how criminal justice agencies are employing social media in their communities and beyond
3. Identify alert systems, and explain their purposes for criminal justice agencies
4. Describe ways in which the use of smartphones and other tools has impacted criminal justice agencies
5. Explain cybercrime, and identify the types of cybercrimes
6. Identify and explain how virtual platforms are impacting training and meetings within criminal justice agencies

> A city patrol officer needs information about a possible warrant or summons for an individual in another jurisdiction (county). The officer must contact the city dispatcher, explaining what he or she needs from the county officer. The city dispatcher contacts the county's dispatcher by phone and relays the question. The county's dispatcher contacts his or her officer to confirm possession of a warrant or summons, if such exists. After receiving a response from the officer, the county dispatcher calls the city dispatcher and provides the requested information. The city dispatcher then contacts the patrol officer by radio, advising him or her of the answer to the warrant or summons question.

Today's criminal justice professionals have instantaneous access to information from a variety of sources—local, state, and federal. Vehicles today still use radios, but they are high band frequency, expanded range, light, and easily carried. Most of the technological advances have been positive; however, a few have created potential opportunities for new types of crimes to proliferate, particularly social media programs that have made coordination of terrorist and gang activities easier and more difficult to police. Other technological concerns center on mobile applications on smartphones and tablets that allow users to identify current locations of law enforcement officers (e.g., Waze, a traffic-tracking tool). If people can pinpoint the exact location of a police officer using this type of mobile application, that officer's safety is jeopardized—particularly if an individual is intent on doing harm to members of the law enforcement community.[2]

According to a 2016 Rand study, "The future might be so saturated with data and information that police agencies will need new ways to tag, sort, and share what they know."[3] Thus, how do criminal justice agencies decide what technologies are useful, and how do they balance the cost of purchase and maintenance against the safety of the public and the privacy of the citizens they protect?

TECHNOLOGY AND TODAY'S CRIMINAL JUSTICE AGENCY

As mentioned earlier, technology has changed and provided new opportunities for today's criminal justice agencies to be more proactive and to solve crimes with a higher percentage of accuracy. Some of these technologies are surveillance based while others are designed to provide additional protections for law enforcement officers.[4]

Aviation technology—including both planes and helicopters—aids officers on the ground in locating and apprehending suspects, locating lost children or older citizens who have wandered away from home, and providing an additional layer of safety for officers.

Detection and surveillance technology allows officials to monitor specific individuals for criminal or dangerous behavior and to keep officers and innocent citizens safe. Detection and surveillance technology includes cameras with night vision capability to record in low-light situations, which aids in the identification of offenders and serves as undisputable proof in the prosecution of criminal cases.

Vehicle and body cameras are common in law enforcement agencies. Vehicle and body cameras can be both an aid and a detriment to an officer. These devices provide visual evidence in cases such as driving under the influence (DUI) or driving while intoxicated (DWI), vehicle pursuits, or officer-involved shootings. However, in some instances, these videos reveal improper conduct on the part of the officer or, in the severest cases, unlawful behavior of an officer.

- In 2017, an Orlando, Florida, police officer was captured on video taunting a participant involved in a family dispute and threatening to beat him and take him to jail.[5]
- An example of severe misconduct occurred in 2017 when a Balch Springs, Texas, officer fired at a vehicle fleeing from a party. His shots struck a 15-year-old passenger in the head and resulted in the individual's death.[6] The officer testified that the vehicle was driving toward him at a high rate of speed and posed an imminent threat to his life. The police chief fired the officer on May 2, 2017, for violating policy, although the chief did not specify what policy.[7]

Body armor, once expensive, heavy, and uncomfortable, has become standard issue for most departments. With the advent of Kevlar and other advanced fibers, body armor has become less expensive, lighter, and cooler to wear.

Less lethal technologies, such as pepper spray, Tasers, beanbag rounds, rubber bullets, tear gas, and stun grenades, allow officers to use alternatives to methods that may involve greater risk for harm to the suspect and the officer. These tools are utilized in situations that involve escalating violence. Each tool is designed to be used in a specific order but may be taken out of sequence in the event of imminent danger to life or limb. While these technologies serve a valuable purpose, the first step—or first line of defense—in any situation is for the officer to use the *command voice* to inform citizens of the action you want them to take and how to comply with your commands. If the command voice does not achieve desired results, you move forward with the use of these less lethal technologies.

Crime mapping (software) and **predictive analysis** is another area where the use of statistics provides criminal justice agencies with a more cost-efficient use of resources to increase the likelihood of crime prevention and suspect apprehension. Crime mapping is a software that was created to allow criminal justice agencies to track crimes—types, dates, times, and geographical locations of crimes.

Biometrics has a variety of uses: confirmation of an individual's identity through voice and/or facial features and expedited capture of personal physical features (fingerprints, facial recognition, and retinal scans).

Communication technologies have expanded greatly. Consider the following:

- While vehicle radios are still used, most officers prefer mobile technologies. Thus, smartphones are used to receive photographs, fingerprints, criminal histories, and messages from other individuals involved in an investigation, as well as general messages.
- Message boards over the interstates and major roadways alert motorists to accidents or road hazards.
- **Amber Alerts** or **Silver Alerts** are broadcast on local television and radio stations, as well as via weather alert radios, to notify citizens of missing or kidnapped children or a missing older person.

- Twitter, Snapchat, Instagram, and Facebook all play a role in the process of modern criminal justice communication (and will be covered later in this chapter).
- Mobile phones, smartphones, or cell phones and tablets have also expanded the options for communication within and among criminal justice agencies and among personnel. Cell phones allow agency personnel to make calls; send text messages; take and receive photographs of suspects, victims, and witnesses; and take and receive criminal histories, photo lineups, and GPS (Global Positioning System) locations. Tablets may be used as a supplement to cell phones if a larger screen or added software applications are required.

> Most recently, texting and driving (also known as distracted driving) has become a significant problem and has resulted in an increasing number of traffic accidents. In 2016, approximately 40,000 traffic fatalities occurred nationwide, an increase of 6%.[8] Despite the fact that 46 states have laws prohibiting texting while driving, and 14 ban the use of handheld devices while driving, a number of the fatalities that occurred were the result of distractions due to smartphones.[9]

In response to this issue, lawmakers in New York and a number of states are considering ways to make obtaining phone records easier for law enforcement. At present, without probable cause to obtain a warrant, law enforcement officers (and other members of criminal justice agencies) cannot check personal smartphones. Due to the advent of a new roadside technology developed by Cellebrite, called the Textalyzer, however, agencies may be able to determine what drivers were doing at the time of an accident using a process similar to that employed with the breathalyzer.

New York is considering the first-of-its-kind legislation to require drivers involved in accidents to submit their phones to roadside testing via the Textalyzer. The proposed law is meeting with resistance based on privacy issues. However, Cellebrite engineer Lee Papathanasiou has explained that the Textalyzer would capture only taps and swipes to determine if a driver was using the phone, that it would not download content, and that it would merely display a summary of what apps on the phone were open and in use.[10] According to the Centers for Disease Control and Prevention, in the United States, more than 1,153 people are injured and 9 people die each day due to distracted-driving accidents.[11]

While not widely recognized as a specific form of technology, **technology assistance** serves as an invaluable asset for agencies that do not possess the budget to purchase new technology or the expertise to use it successfully or to train individuals in its use. State resources (e.g., the Tennessee Bureau of Investigation [TBI]) or federal resources (e.g., the Federal Bureau of Investigation [FBI]) serve as points of information and scientific analysis. These agencies provide the professional analysis and, when necessary, the professional testimony to interpret the information collected from crime scenes to aid jurisdictions in the prosecution of a suspect.

The Intranet (Organizational Network)

One of the most significant advances in criminal justice technology centers on the use of organizational networks, often referred to in the private sector as intranets.

An **intranet** is a group of connected computers and servers that exchange information and share equipment within a specific organization. Prior to the advent of network typologies, criminal justice agencies relied on clerks, secretaries, or office personnel to retrieve information or data from extensive file cabinets and records centers. This method of maintaining and retrieving data was extremely time-consuming, labor-intensive, and costly.

In the corrections area, the use of intranets offers options that facilitate the manner in which inmates are admitted to the institution and tracked during their incarceration. Again, prior to the implementation of intranets, inmate files were stored in a secure records facility and retrieval involved lengthy and arduous procedures. From a computer offering access to the organizational network, records can be reviewed by authorized correctional personnel in order to confirm identities, to determine the appropriate classification and assignment of inmates, to track inmates' disciplinary problems, to review credit for "good time," and to complete any other administrative functions.

Mobile Data Terminals (MDTs)

The establishment of an organizational intranet allows authorized personnel to access information from a variety of locations. Officers in patrol cars have access to database information via the use of a **mobile data terminal (MDT)**. The mobile data terminal is a screen and keyboard that connects the patrol car to the central computer or server and allows the officer to stay in contact with the dispatch center. The use of the MDT not only enhances the officer's ability to access information but also reduces the need to use the police radio. Furthermore, the use of the MDT provides an additional measure of security because the communication cannot be accessed by the general public, unlike radio communication that is frequently monitored by civilians who possess police scanners.

MDTs allow officers to be dispatched on calls for service without the utilization of the police radio. When a call is received, the MDT makes a noise, either a beep or a buzz. This sound notifies the officer that an incoming call will be received on the terminal. As the call is received, the officer reviews the nature of the call and the address and strikes a function key, which notifies dispatch that the call has been received and that the unit is en route. When the officer arrives at the designated address, another function key is struck to notify dispatch that the officer is on the scene and out of service. In some of the more advanced MDT units, a follow-up tone will notify the dispatcher that the unit is still out of service and may require assistance. This innovation was designed to ensure that dispatchers check on the safety of officers who have been marked out of service for a specified period of time.

Once the officer has handled the call, he or she returns to the unit and prepares an initial offense report. At one point, offense or incident reports had to be prepared by hand and delivered to a supervisor, who reviewed and approved the document. The reports were disseminated to the proper divisions for investigation or storage in records. However, with the development of appropriate software, reports may be generated by utilizing the MDT keyboard to type and send them to a supervisor for review. One caveat, nonetheless: Even though you prepare your reports using the MDT, you still need to adhere to the rules of report writing discussed in earlier chapters.

Once the report is completed and forwarded to the appropriate supervisor, the officer again strikes a function key on the MDT to notify the dispatcher that the unit has cleared from that address and is in service or able to receive a call.

Another vital aspect of the MDT is the ability of the officer to retrieve information while in the field. Frequently officers see suspicious vehicles and want to know to whom the vehicle is registered. By utilizing the MDT, an officer may access the State Division of Motor Vehicle (DMV) records and determine the owner of the vehicle. Additionally, officers may verify the license status of a driver by accessing the DMV records to determine if the driver has a valid operator's license or if his or her privilege to drive has been suspended or revoked.

Officers frequently come in contact with a wide variety of individuals during the course of their patrol activities and will routinely run what is referred to as a "wants and warrants check." The MDT allows them to obtain the status of these individuals locally, statewide, and nationally. Officers can seek information from the Federal Bureau of Investigation's National Crime Information Center (NCIC) through a link from their MDT. They also have the capability of retrieving data from their state system (e.g., Virginia's VCIN [Virginia Crime Information Network]).

Department or Bureau Computers

Much like their MDT counterparts, these computers allow authorized personnel access to a variety of information. The only significant difference is that these computers are located on the desks of officers or supervisors or in a central location that is easily accessible to qualified personnel. Generally, these computers are used to prepare supplemental offense reports (discussed elsewhere in this text). However, they may be used to transcribe the notes from victim, witness, or suspect statements.

Department or bureau computers have expanded capability or access to information unavailable to their MDT counterparts. Access to sensitive information, however, may be limited to certain individuals by issuing passwords for specific levels. An example of sensitive information may be a list of informants or suspected drug dealers that would be contained within the narcotics or vice bureau. An administrative example of sensitive information would be the department budget or salary structure for the department.

Typically, networked computers require users to log on with a username and a password. This username and password are considered to be of an extremely sensitive nature and, therefore, should be kept confidential. Only select administrative personnel should have access to departmental personnel's usernames and passwords.

Electronic Mail (E-Mail)

E-mail, or electronic mail, is a means by which a message, a bulletin, or other information may be distributed to an individual or a group of individuals from a single source. E-mail is the electronic equivalent of the U.S. Postal Service. However, unlike the postal service and the confidentiality assumed in the delivery of a letter, e-mail can and is frequently monitored by other individuals. These individuals may be supervisors or hackers. Either way, you should always be aware that e-mail is not generally secure.

E-mail may be a particularly effective means of disseminating information that needs to be shared with a large group of people immediately, such as changes in the warrant status of current offenders, changes in the current status of search warrants, or any modifications to departmental policy. Additionally, e-mail may be utilized to handle the more mundane aspects of organizational operation, such as the date for change from summer to fall uniforms, shopping vehicles for maintenance, or extra duty assignments. E-mail could also be utilized to submit routine information, such as the number of officers on sick leave, the number of officers on vacation, or the number of officers on special assignment.

If e-mail is adopted as the official channel of intradepartmental or interdepartmental communication, then it holds the same authority and status as any written document containing the same information. The same rules of composition (including grammar and punctuation) that are used to create a written document also apply to e-mail.

Etiquette Guidelines for E-Mail

The use of e-mail as an official communication channel requires a basic understanding of the rules of etiquette for its use.

- Use e-mail only when it is the most efficient channel for communication. Remember that e-mail has permanence. Even deleted e-mails can be retrieved, and lawyers can subpoena e-mails to use as evidence in court. Choose e-mail for short, informal messages that need to be written and read.
- Do not key your e-mail messages in ALL CAPS, as the use of all capital letters is viewed as shouting. If you need to call attention to a word or words, you can enclose it in asterisks (i.e., *all caps*).
- Always include a relevant subject line; change the subject line when the purpose of the message changes; make sure the subject line reflects the purpose of your message and that the subject line is specific (i.e., avoid using "Information," "Question," or "Need Help" as subjects because they are too vague and do not offer your reader the necessary information as to the specific purpose of your message).
- Do not leave the subject line blank. If you want to be effective at e-mail, you need to use subject lines in the same fashion as newspapers use headlines. Your subject line is actually an advertisement for the attention of your recipient. Busy people require specifics in the subject line. If you are requesting some kind of action, tell the reader in the subject line. If you are providing an update, summarize the information in the subject line by using the 140-character Twitter postings as an example. However, you should state your subject in about half of a tweet posting—70 characters or less.
- Address your recipient in a salutation (Dear Skip or Dear Dr. Grubb) or in the opening sentence. Do not use openings such as Hi, Skip; Hello, Skip; or Hey, Skip. Follow simple rules of courtesy in your opening; if you

have been given permission to address someone by his or her first name, then do so. If you are writing to people you do not know, address them as Mr., Ms., Rev., or Dr.

- Remember that without facial expressions, some comments may be misinterpreted. Choose your words carefully when writing your e-mails.
- Keep your e-mails to one topic only. Your recipient should not need to focus on more than one purpose for your message, so do not confuse the reader.
- Keep your e-mails short; an e-mail message should cover no more than one screen. If you have to scroll down to read the entirety of the e-mail, your message is too long. You might want to consider preparing your message in a Word format and sending it as an attachment to an e-mail. You would ensure a higher percentage of your e-mail messages get read in their entirety by recipients if you follow the writing guidelines for all messages: Keep them concise, complete, clear, and correct.
- Consider the purpose of your message. Is the purpose to deliver bad news, criticize, or share confidential information? If so, you need to step away from the keyboard and pick up your phone to schedule a face-to-face meeting. You want to think about the response of the recipients. If they will be angry, upset, hurt, or disappointed, you need to select another channel by which to communicate with these individuals. Certainly, the use of e-mail is fast and efficient; but in situations where the information is difficult to share in person, you just want to use e-mail to distance yourself from people. That approach is unacceptable. Electronic messages diminish the impact of a message. So choose carefully what type of messages you are willing to send via electronic means.
- Follow the proper guidelines for creating your message. Analyze your audience (who will be reading my message), write your message, and then proofread and revise your message. Do not hit the "Send" button until you complete all three of these steps, especially the proofreading and revising one. Check your grammar, spelling, and punctuation. Make sure that what you have written is reflective of what you intended to say. Communication is not effective unless the recipient of the communication understands the message the way that you intended it. (Chapter 1 of this text covered this important information.) If you have run-on sentences, sentence fragments, subject–verb disagreement, misplaced modifiers, or other grammatical issues, your message can be confusing to your recipient.
- Avoid using abbreviations or brief forms in your professional messages or texts. You certainly might use "u" or "gr8" in a message or text to your friends; but for work-related messages, stick with the tried and true, and spell out your words; you are not in middle school.
- Verify the e-mail address for your recipient, and ensure that you are sending carbon copies to only those individuals who should receive them. Do not "cc" (carbon copy) everyone. If you are sending sensitive information, you

want to ensure that your message goes only to those individuals who are allowed access to that information.

- Create an electronic signature for your e-mail messages. Think of the electronic signature as a substitute for department or agency letterhead (stationery), so include your full name, position, agency or department name, address, phone number, and e-mail information—anything relevant to you and your position.
- If you are angry, do not send an e-mail message (known as flaming). Rather than tempt fate, go to Word and type everything you want to say—in whatever form you want to say it. Type a message that is as lengthy as you need it to be in order to fully vent your anger or frustration. The good news is that since you are in Word and not your e-mail account, you cannot press send once you complete your angry diatribe. After you have finished keying your message, move on to another project. Give yourself a minimum of 2 hours before returning to your message. After you have completed that reasonable waiting period, if you still feel you need to send a message, read what you have written. Select parts of the message you deem to be pertinent. Copy and paste those selected parts of your message into your e-mail. Be forewarned, however: E-mail is nothing more than words on a screen, and no nonverbal communication, such as facial expressions or voice inflections, are present to help defray the impact of those words on the screen. So your recipient may react in a like fashion—angry. The rule of thumb is to exercise caution. If you can avoid angry messages, do so.
- Sarcastic messages follow the same guidelines as angry messages. Avoid them whenever possible. Sarcasm does not translate well to words only. You need the accompanying facial expressions, gestures, and voice qualities to ensure a positive response.
- When responding to an e-mail message that is asking you for information (such as answers to a series of questions), include pertinent parts of the original message in your response. For example, copy and paste the list of questions from the original e-mail message into your response, and key your answers beneath each question. You will remind the recipient of the questions he or she wanted you to answer without the necessity of having to open the original e-mail message to view them.
- Respond to all e-mail messages in a timely fashion. Send a reply as soon as possible but no later than 24 hours after receipt of the message, even if you simply state that you have received the e-mail message and will follow up. If you plan to be away from your workplace and your e-mail program has the capability of an automatic response, then you should set up a response that automatically acknowledges receipt of messages and explains when you will return.
- Keep personal e-mail messages out of your workplace e-mail account.[12]

While e-mail is the most frequently used communication channel, it is not the only technology designed for such use.

Texting

Because of its convenience and the speed at which messages can be sent and received, texting is gaining in popularity. E-mail requires you to log in to your agency or department system. Texting requires only the use of your smartphone.

The downside to texting, however, is that you are limited in what you can send (i.e., no attached documents), and you cannot easily print text messages. With e-mail, you can maintain a record of communication, a trail of correspondence that you can use for legal purposes or simply for departmental or agency records. In addition, you can easily print your e-mail messages from a computer or directly from your smartphone if you are using a departmental or agency network with a wireless printer.

Etiquette Guidelines for Texting

If your agency or department approves the use of texting, you will need to follow a set of etiquette guidelines to ensure appropriate responses.

- Texting is faster than e-mail because of the shorthand (abbreviations) that can be used, but you have to make sure that the recipient has an understanding of all abbreviations in your message. If not, your abbreviations may lead to misunderstandings or cause wasted time while the recipient attempts to translate the message.
- Texting offers greater privacy, especially in agencies and departments where open work spaces are used. You should not default to texting just because it is quieter, however. Some situations call for a phone call or a face-to-face meeting.
- Text messages are not easily tracked or recorded. So if you need a record of this information for future reference, texting is not the best option. E-mail will provide you with that option.
- Do not allow your text messages to cross the line into unprofessional conversations.
- Do not allow yourself to become distracted while texting. Text only in safe locations.
- Do not text while driving. Some states have enacted laws against texting while operating a moving vehicle. Whether your state has enacted such laws or not, you should never text and drive.
- If your agency or department has established an acceptable cell phone use policy, you may find that you are restricted to certain times of the day or certain locations when and where you may text. You may be required to sign an agreement that you will adhere to the organization's policy. Follow the policy guidelines.

Remember that your agency or department establishes the guidelines for the technology you are allowed to employ in your daily work activities. If texting is allowed only among members of your agency or department, you should adhere to that guideline.

TECHNOLOGY IN THE COURTROOM AND IN CORRECTIONS

While many of the technologies previously discussed are used by law enforcement agencies, some of these technologies—and others yet to be discussed—have applications to criminal justice agencies aside from law enforcement. The following section discusses these new and emerging technologies and their applicability to corrections and the courts.

New Technologies in the Courtroom

Nothing is more dramatic than the positive identification of the suspect by an eyewitness in the courtroom. However, this type of identification is frequently exploited and dismissed by defense attorneys. Research has shown that human memory is fallible, and positive eyewitness identification is not always an asset. Historically, suspects have been identified through a variety of means, including the sketch artist. Victims or witnesses would come to police headquarters and provide an artist with details from which a sketch or composite would be created. In some instances, these sketches or composites were remarkably accurate. Unfortunately, in some instances, these sketches or composites were remarkably inaccurate. In cases where DNA was collected, 70% of eyewitness testimony was proven false.[13] Herman E. Kimsey offered the following explanation for why creating a sketch of a suspect from human memory using common language is difficult, if not totally impossible.

> One of the most difficult problems in human communication is that of exactly duplicating in another mind the visual image one has in one's own. Language is not adequate to the job: the range of variant concepts corresponding to each descriptive word, not to mention their inevitable emotional and imaginative colorings, create inaccuracies, distortions, and downright false impressions. Man has therefore had to resort to comparing such an image or its elements with accepted common physical standards, which reach their ultimate precision in the standard units of measurement. This procedure leaves no room for the vagaries of individual interpretation.[14]

Since sketch artists are few in number and not readily available, several attempts were made to create a library of different facial characteristics. Generically, these attempts were marketed as *Identi-Kits*. Initially, these Identi-Kits provided investigators with a means of developing a visual representation of a suspect without having any particular expertise or specialized training in sketching. Original Identi-Kits were transparencies that overlaid each other in order to develop a facial reconstruction of a suspect.[15] The investigator began with a facial shape such as round, oval, or square, and from that point proceeded to the shape of the eyes. Then the shape of the nose and the mouth and the hairline and its relationship to the ears were developed until ultimately a visual representation of the suspect was created.

An improvement on the Identi-Kit came when facial composite sketch software was created. Identi-Kit is a graphics-based application that is available to criminal justice agencies via cloud-based delivery. This tool was designed to be used by investigators, not computer programmers, so it is intuitive to use. A facial reproduction may be electronically created, stored, and printed within a matter of minutes. Furthermore, this image may be distributed very rapidly to local, state, or national authorities to assist in the apprehension or detention of a suspect.[16]

The facial composite sketch software is not the only tool of technology available to the prosecutor in the courtroom. The axiom "A picture is worth a thousand words" is never more true than in a courtroom setting when the prosecutor is trying to describe a crime scene and the relationship that may exist between pieces of evidence. **ScenePD**[17] and **CAD Zone**[18] are two examples of computer software that aid an evidence technician in diagraming a crime scene. Crime scenes presented in court are the result of a scaled final product prepared by a law enforcement evidence technician. Upon arrival at the crime scene, an evidence technician prepares a rough draft of the scene that includes the position of the victim, any evidence, and the layout or design of the area. These technicians formulate a sketch by utilizing a variety of methods, but three of the most prominent are the **grid**, **triangulation**, or **cross-projection**. These methods allow technicians to accurately draw the crime scene and to ensure the relationship between pieces of evidence is factual. Once this diagram is completed, a scaled drawing is constructed by the technician for display in court. ScenePD and CAD Zone allow these technicians to more efficiently and effectively create diagrams of the crime scene.

Other design technologies similar to ScenePD and CAD Zone are utilized in the re-creation of crime scenes and traffic accidents. However, the use of these technologies for court purposes has been limited. Generally, these technologies have found more success in civil proceedings than in criminal trials.

Furthermore, with the increasing availability of body cameras and the proliferation of smartphones, recording of crime scenes has become widespread—for both the good and the bad. A distinct advantage to recording crime scenes is the addition of color and the clarity with which the scene may be presented. Jurors and judges are impressed with being able to view the entirety of a crime scene and the relationship that exists between the evidence and its relative position in a specific location. Recording could eliminate the necessity of transporting the judge and/or jury to the actual crime scene, thereby saving time and money for the local jurisdiction, an important factor to consider given today's high cost of prosecution.

In-car camera systems (also called dash cameras) are being used in law enforcement vehicles to monitor the officer's safety and to serve as a visual confirmation of the officer's observations and the suspect's actions. In many instances, defendants who are charged with driving under the influence plead guilty once they or their attorneys have viewed the officer's recording of the traffic stop. In other cases, suspects have been found guilty by a judge or jury as a result of having viewed the recording. In extreme cases where officers are injured or killed, in addition to serving as evidence in the trial of the suspect, these recordings serve as a graphic training reminder for new officers and seasoned veterans to remain vigilant.

In 2011, a five-county judicial circuit in Missouri deployed a Skype-like system to help judges remotely preside over motions, arraignments, and other legal proceedings without the need to drive across the state to do so. The system selected for the 4th Judicial Circuit included a large-screen, high-definition television and top-mounted video camera for each of the five counties. Cameras were arranged so that one focused on the judge and the other camera on the defendant.[19]

Additionally, videoconferencing is being employed as a means for out-of-state witnesses or experts to offer testimony in civil trials. However, in criminal cases, the Confrontation Clause of the Sixth Amendment of the Constitution still holds sway in the realm of testimony. One case in point is *New Mexico v. Truett Thomas*. Thomas is alleged to have bludgeoned to death a woman named Guadalupe Ashford. State forensic analysts collected DNA samples from her body and the murder weapon (a brick) and found them to match Truett Thomas. The state tried and convicted Thomas for first-degree murder and kidnapping. The issue with this case, however, was that of the testimony of the forensic analyst who matched the DNA samples. The analyst moved out of New Mexico during the time preceding Thomas's trial and did not wish to physically return to the state to testify. The court allowed the testimony via Skype.

As New Mexico's entire case against Thomas hinged on the DNA analyst's work, her testimony was the mainstay of the trial. Without the analyst's work, the state had no case. The New Mexico Supreme Court consequently ruled that courts cannot use Skype to circumvent the Sixth Amendment to the Constitution. Defendants have the right to confront all witnesses against them.[20]

As far as the use of Skype and whether personal sessions are admissible in court—or can be subpoenaed for introduction in a courtroom—the answer is no to recordings of videoconference sessions but yes to certain other information. In 2007, Skype created a Law Enforcement Relations Management (LERM) Team to handle records requests. Skype can provide only the following information via subpoena:

- Registration information provided at the time of account registration
- E-mail address
- IP address at the time of registration
- Financial transactions conducted with Skype in the past year (only billing provider used regarding credit cards is available—e.g., Bitbit and PayPal)
- Destination telephone numbers for any calls placed to the public-switched telephone network (PSTN)
- All services and account information, including any billing address(es) provided, IP address (at each transaction), and complete transactional information[21]

Twice each year, Skype publishes the number of legal demands for customer data it receives from law enforcement agencies from around the globe.[22] These data can be filtered by country and time frame.

Videoconferencing has definitely gained a foothold in criminal justice. Whether using a video camera and specific programs designed for a corrections or court setting or simply employing Skype, criminal justice agencies have seen the benefits of real-time communication that does not require travel or an investment of time beyond the actual virtual meeting or interview. While videoconferencing occasionally experiences issues in connectivity and streaming capability, these problems are small in comparison to the advantages this technology provides. Prior to the use of this technology, communication with experts, witnesses, victims, family members, colleagues, attorneys, mental health staff, and others required scheduling face-to-face meetings in the office, bureau, department, prison, or judge's chamber.

New Technologies in Corrections

Booking suspects in the docket historically involved fingerprinting and photographing. While a visual representation of the suspect was captured, these pictures were not always the best quality. Differences in skin tone, light facial hair, or facial scars were not always discernible. Now, digital cameras and editing software ensure that photographs of suspects are more realistic and representative of the individual. Digital cameras allow a suspect to be photographed from at least three different angles and for this information to be stored in the local computer database. Those facial anomalies previously undetectable can be enhanced to provide a better photograph or description of the subject. Furthermore, these photographs may be altered by means of new software to reflect the addition or removal of mustaches, beards, toupees, glasses, and other features. Since these photographs are stored electronically or digitally, agencies no longer have to budget for costs associated with purchasing, developing, and storing traditional film.

In addition to the digital camera, certain departments are using a **live scan fingerprinting process**. These two new technologies not only improve the processing of incoming suspects but also reduce the possibility that violent or repeat offenders will be released or lost in the system.

In 2003, rural counties in West Virginia experimented with an innovative approach to arraigning suspects. This new approach involved **synchronous transmission** of information. Synchronous transmission of data or information is "real-time" transmission or reception of video images and audio. A suspect in the local jail was taken to an interview room that contained a microphone, video camera, and monitor. The suspect was able to hear, as well as to see, the local magistrate or judge, who advised him or her of the charge and the determination of bail. Local law enforcement agencies were pleased with this adaptation of existing technology because it eliminated the need to transport prisoners over long distances and reduced the probability of an escape attempt. Deputies were reassigned to other duties or placed in the field rather than used for transport details.

Spring forward a decade, and you will see that arraignments are being handled in a variety of ways involving technology. For example, Skype or other virtual platforms for videoconferencing are being employed to cut down on transportation issues and costs, as well as to handle arraignments quickly and more efficiently.

In December 2011, the Niagara County Jail in Lockport, New York, began using a web-based videoconferencing system. This system was implemented to reduce the number of physical visitors the jail must accommodate, such as attorneys, mental health staff, and probation officers. These individuals could engage in online meetings with prisoners without the necessity of traveling to the facility.[23]

In 2013, the Yellowstone County Detention Facility in Montana implemented a remote visitation system for inmates. This visitation system was the first of its kind in Montana and allowed inmates to have 30-minute scheduled visits via webcam with family and friends. The system chosen by the Yellowstone County Detention Facility was not Skype but one offered by Telmate. This system allowed family and friends to link to an inmate through a web browser. The system the inmate uses in the detention facility resembles a pay phone with a screen and is equipped with a camera and telephone for communication. Family and friends must pay $10.50 per session to visit with an inmate. The facility commander explained that this system was beneficial for family and friends because no travel was required, and it was beneficial to the inmates, as the profits from these virtual visit charges went toward the facility's GED program, anger management classes, and other inmate activities.[24]

MOBILE DEVICE APPS

What is an app? **App** is merely an abbreviation for the word *application*. In the world of smartphones and tablets, mobile apps are those programs downloaded to perform a specific function. A plethora of apps are available for both the iOS (Apple) and Android operating systems; however, these programs must be evaluated carefully before deploying them. Many are useful for short periods of time or for specific activities but have little value over the long term.

A review of published research regarding apps used by law enforcement reveals a minimal number of recommended programs.[25] The following list of applications is not comprehensive. Most of these apps work on both the iOS and Android platforms.

Law Enforcement Apps

- **TBL Universal Reporting.** The Thin Blue Line Reporting app allows law enforcement officers to create reports and sync them to the cloud. CJIS and FIPS compliant.
- **Spanish for Police.** Offers more than 200 simple Spanish commands and questions. Has written and audio translations.
- **Net Transcripts.** Officers who have a Net Transcripts account can record and submit dictation and interviews for transcription. This app touts itself as the "nation's leading provider of confidential transcription for law enforcement agencies."
- **NoteM8.** Keeps a local copy of your data, images, and documents. You can also synchronize your local data for sharing with your peers using the NoteM8 Cloud or the Presynct Report Network enterprise server.
- **Video Armor: Police Camera.** Turns your smartphone into a body worn video camera. The app records high-quality video that is automatically tagged with date, time, and GPS location data.
- **Snitch'n.** Allows you to browse police images of wanted criminals, suspects, associates, missing persons, and more.
- **Appriss MobilePatrol.** Improves communication between sheriffs' offices and the communities they serve.
- **PublicEye.** Allows everyone in the department to collaborate from his or her mobile device.

- **U.S. Cop.** Provides resources for street officers, including more than 2,000 pages of accident investigation formulas, training articles, a pill identifier, case law resources, and more.
- **Camera Canvas Tracker.** Addresses difficult tasks associated with canvassing for surveillance cameras.
- **Crashdocs.org.** Designed to be used by officers responding to an accident scene. The responding officer can use a smartphone or cell phone to scan the vehicles' identification numbers and input information about the collision. The officer provides a card to the individuals involved in the accident that contains the web address for access to the accident report (http://www.crashdocs.org). The driver seeking a copy of the accident report must still pay the same fee as that required for "in-person" requests. However, the use of this app and corresponding website provides more convenience for the drivers. According to CarFax, the company behind the app and website, accident reports are normally available on crashdocs.org within 5 to 7 business days after the accident. CarFax sends all monies collected for the accident reports to the corresponding law enforcement agency.[26]

Corrections Apps

Very few applications are available for corrections officers themselves. Those available have a fitness focus rather than anything related to the job.

Some states have deployed mobile applications that track probation and community corrections officers as an overall safety and accountability measure. In addition, a smartphone-based GPS monitoring solution has recently been released that will assist case managers in monitoring offenders. This Telemate Guardian app provides real-time monitoring, reports, and check-in controls, as well as voice and facial detection, and is compatible with both iOS and Android smartphones.[27]

Private Security Apps

Most of the applications available for private security are geared toward corporate staff or security companies themselves. Some of the apps recommended for law enforcement in the previous section would be helpful to private security officers, however, especially Spanish for Police.

An important point to remember about mobile applications is that they are continually evolving. If you do not find one of these apps in your app store, you should not despair, as another one has most likely taken its place in the list of importance.

The next section of this chapter discusses social media. Social media applications are also mobile apps (e.g., Facebook, Twitter, LinkedIn, Instagram, and Snapchat). However, we did not wish to include them in the section on mobile apps, as their importance extends beyond the ease of access via smartphone and tablets.

SOCIAL MEDIA: CRIMINAL JUSTICE'S NEWEST WEAPON

No technology has opened the closed doors of criminal justice agencies to the public more than social media. The advent of Facebook, Twitter, and Instagram has led to opportunities for agencies to become more transparent and community friendly. While many criminal justice agencies have embraced this new technology, still others have failed to recognize its potential to create a bond with the communities they serve.

What is social media? **Social media** is defined as “forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos).”[28] Facebook, Twitter, Instagram, LinkedIn, and Snapchat are examples of social media. Facebook and Twitter are the two dominant social media programs used by criminal justice agencies.

In 2016, the International Association of Chiefs of Police and the Urban Institute created a Social Media Survey designed to gain information about how law enforcement agencies are using social media technology. The survey was distributed to law enforcement officials who manage their agencies’ social media accounts in the United States. Demographic data from the survey indicated that 539 law enforcement agencies representing 48 states and the District of Columbia participated in the study. Responses revealed that participating law enforcement agencies use social media for a variety of purposes:

- 91% to notify the public of safety concerns
- 81% for community outreach
- 86% for public relations and reputation management
- 59% for obtaining information to use as evidence[29]

When asked how long their agencies had used social media, 5% of responding law enforcement departments indicated using social media for over a decade; 5% revealed they had adopted it within the last year.

Not all agencies use social media in the same fashion. When asked about management of social media sites, 80% of the responding agencies reported that they have written social media policies that detail how officers use the technology. Still others have policies in the development phase (11%). Also, a majority of respondents (25%) indicated that a public information officer is the person responsible for managing their agency’s social media accounts. Use of a public information officer is considered the best option, as this individual serves as a central point of contact for releasing information, for presenting a positive and consistent message to the public, and for serving as an intermediary between the public and the chief administrative officer. The public information officer does not have to be responsible for every communication sent from or posted to agency sites. Rather, he or she can be charged with oversight of social media and agency websites and the personnel who manage them.

The public information officer need not be a sworn member of the agency. He or she could be a civilian with experience in mass communication and the media. Individuals who have previously worked for local television stations as anchors or reporters and who have effective communication skills typically make the best choices for public information officers since they will be interacting with the media and the local community in a myriad of situations requiring the ability to “think on your feet” while not revealing any confidential information.

When asked about content on social media sites, agencies revealed that most respond to user questions on their social media sites (86%). Only 14% indicated that they do not respond to any questions on social media. Most agencies reported responding to questions or comments on a case-by-case basis—both positive and negative questions and comments.

An interesting finding regarding differing tones and strategies used to engage community members was that 29% of responding agencies stated they always or almost always use an informal tone while 26% said they never use or almost never use an informal tone. However, 85% of responding agencies reported using humor at least some of the time while posting.

In many instances, social media is taking the place of community policing—the cop on the beat—by initiating conversations with new generations of technology-savvy individuals while engendering trust and providing vital information to the people these agencies have sworn to serve and protect. In addition, the use of social media helps humanize police departments and shows that the officers are also members of the community they serve. Social media can be an effective way for agencies to highlight officers' accomplishments, make announcements regarding enforcement campaigns, and provide messages about safety. Agencies can also use social media to ask followers for tips on crimes or to provide important warnings or alerts regarding missing children or suspected criminals who may be on the street or in the community.[30]

Participating agencies (84%) indicated adapting to new online trends to be a challenging issue for them, followed closely by measuring the impact of their social media presence (82%) and training personnel to effectively use social media (81%). In this situation, challenges that law enforcement agencies face are no different than those the average citizen or any business, organization, corporation, or foundation faces, particularly in terms of keeping up with and adapting to new online trends.

When asked how many social media accounts participating departments had, the responses varied by size of department and the community population. Larger departments may require the use of several accounts to reach different segments of the population, such as crime victims, abused spouses, and child advocates. A separate account may be created solely for official statements from the chief administrative officer.

Agencies responding to the survey indicated that they believed training would be beneficial to their agencies. The greatest percentage of responses revealed training that focuses on engaging the community to be of the most value to agencies (28%). However, 26% of respondents indicated that training to improve the use of social media would be most valuable to them. Of note as well, 21% of respondents believe that training to protect agencies from liability issues created by social media would be of the most value.[31]

Writing for Social Media

In earlier chapters of this text, we discussed the need for conciseness in the writing process. Nowhere is this more evident than in the social media world, particularly with Twitter. Twitter limits each post to a maximum of 140 characters. Therefore, if you are going to post something, you must remember a few facts in addition to the character limit:

- Recognize the difference between voice and tone. Voice does not change. Tone, however, should vary based on the situation. If a person had a negative experience (left a negative comment), your response should be more sympathetic and understanding.
- Talk with people, not at them. Reply to any "@ mentions," and address both positive and negative feedback. Twitter is a real-time network, so the sooner you respond, the better.
- Keep your tweets conversational.
- Be professional without being overly formal.
- Avoid jargon when possible. Most laypeople do not understand "police" speech.
- Consider how your content will be consumed by your followers. Would they want to retweet it or pass it along to others?
- When possible, incorporate humor, inspiration, and newsworthy content to draw in followers.

You can post a URL for a specific published newspaper or other article. You can also post a link to your agency's website where you are sharing additional information, photos, or video. In order to maintain the 140-character post, however, you will want to use a tool to shorten your URLs. Several tools are available, including the following: Bitly, Goo.gl, tinyURL.com, Ow.ly, Is.gd, AdF.ly, Bit.do, and Mcaf.ee.

When preparing to write for your Facebook page, you do not have to be constrained by a character limit. However, you do not want to stray too far from your point or add too much extraneous material to your posts, as that will deter your audience from reading them. Consider the following suggestions:

- **Listen.** Before you can talk to a community, you have to understand and embrace how they talk about you. Your community should inform your voice and your content (to an extent). Check to see how people talk about your agency, and use that to inform your writing.
- **Write to one action.** You either want your community to like, share, comment, or click your link. Review your post carefully, and determine what you are trying to get your community to do—what action are you trying to spur? If you have more than one action, you may be confusing your readers. Keep it simple.
- **Do not limit your post to writing only.** The best Facebook writers spruce up pictures and infographics with clever copy. Infographics do not need to be long images riddled with stats and graphics. The busier ones tend to be ignored on Facebook. If your infographic takes too much thought or too much time, people will not review it.

- **Be inspiring first.** If you want your community to post photos, you have to show and ask. Show them the types of photos you want to see on your page, and ask them to do the same.
- **Refrain from making your posts feel forced.** Often when you manage an agency's Facebook page, you will have specific messages that you have to work into your content plan: legal notices, warnings, and reminders. These postings are not always a natural fit with the content you normally push out. If you have to post some of these types of messages, push to make sure that you keep them in line with the agency's voice, tone, and overall approach. When you try to force engagement, your writing will seem or feel inauthentic. Your audience will recognize lapses in authenticity, and your engagement will suffer for it.
- **Standard tenets of good writing still apply.** Just because the people who comment on your page fail to use the proper versions of your/you're and there/their/they're does not mean you can. There is nothing new here, as you have read this information throughout this text.
- **Experiment, measure, and respond.** The more chances you take with your writing on Facebook, the more you can use metrics to understand what type of writing works with your community.
- **You are only as good as your next post.** Any writer should continually strive to improve his or her craft. When it comes to writing for any social platform, you can't rest on your laurels. After every post that falls flat, you should ask, "How can I make this better?" Similarly, after every successful post, you should ask, "How can I make this better?"

To see several examples of agencies that effectively use Facebook and/or Twitter, visit the following sites:[32]

Facebook

- https://www.facebook.com/NYPD
- https://www.facebook.com/RoanokeCountyPolice
- https://www.facebook.com/PlacerSheriff
- https://www.facebook.com/PlanoTexasPoliceDepartment
- https://www.facebook.com/SeattlePolice
- https://www.facebook.com/BostonPoliceDepartment

Twitter

- https://twitter.com/FranklinTNPD
- https://twitter.com/salempolicedept
- https://twitter.com/DallasPD
- https://twitter.com/portlandpolice

- https://twitter.com/columbuspolice
- https://twitter.com/cspdpio

Clearly, law enforcement agencies, in an effort to grow closer with their respective communities, are increasingly moving toward the use of technology. While social media does not replace the interpersonal relationships built between the citizens and their protectors, this tool does help agencies reach a broader audience that is very comfortable communicating in this fashion. What will the future bring with respect to communication and technology? We can only wait and see. Our hope is that the relationships between communities and the agencies that serve them strengthen and that these stronger bonds continue with the emerging citizens of the next generations.

The next section in this chapter discusses what some may believe are outdated technologies: bulletin boards and listservs. However, these tools are still in use.

BULLETIN BOARDS

A bulletin board system (BBS) is often called a chat room, where people with similar interests meet online to discuss issues of importance. **Bulletin boards** exist for political activists, hobbyists of all types, collectors, and law enforcement officers, to name a few.

Many law enforcement agencies maintain bulletin board systems as public relations tools but monitor other BBs for unlawful activity. Some ways law enforcement agencies monitor bulletin boards include the following:

- Social site
- Hidden service
- Semantic
- Marketplace profiling

LISTSERVS

Requiring only an e-mail connection, **listservs** are one of the most cost-effective means for networking among criminal justice professionals worldwide. Individuals join a listserv by e-mail. Most often, you are required to e-mail the listserv address and state your desire to subscribe to that service. The listserv will respond by e-mail to your request and advise you that you are now a subscriber. Shortly thereafter, you will begin to receive e-mail from the listserv.

Some listservs are moderated by a list owner who reviews each message and decides whether or not to send it to the subscribers. The list owner can also edit messages before sending them. Examples of listservs that may be of interest to the criminal justice professional would be as follows:

- **BJS, the Bureau of Justice Statistics.** Provides information on crimes and victims, drugs and crime, criminal offenders, and special topics. To subscribe to the listserv, visit the web address for the Bureau of Justice Statics, www.ojp.usdog.gov/bjs.
- **Justice Information Center.** A service of the National Criminal Justice Reference Service. This site is one of the most extensive sources of information on criminal and juvenile justice in the world. It is a collection

of clearinghouses supporting bureaus of the United States Department of Justice Office of Justice Programs, the National Institute of Justice, and several other government agencies. To subscribe to the listserv for the Justice Information Center, see their web page at www.ncjrs.org.

The following are some examples of other listservs available for membership, depending on your area(s) of interest and specialization:

- **NIC.** This listserv is the United States' National Institution of Corrections' public forum for the discussion of corrections issues and practices and for the exchange of views and information. It is also intended to facilitate communication between the institute and field practitioners, policy makers, and researchers. Available at https://nicic.gov.
- **National Criminal Justice Reference Service.** Sponsored by the United States Department of Justice, Office of Justice Programs, this electronic newsletter service provides the latest criminal justice news and information. Available at https://www.ncjrs.gov.
- **Yale Prison Project.** Yale University hosts this discussion list on prison issues and topics. Available at https://www.yaleundergraduateprisonproject.org.
- **UNIVPD-L.** A discussion list for sworn law enforcement officers, its purpose is to provide a forum for law enforcement officers to discuss issues of campus safety, crime prevention, and law enforcement as they relate to university and college environments. Available at https://www.listserv.buffalo.edu.

ELECTRONIC JOURNALS

Criminal justice administrators will find a variety of information on a plethora of topics located on the Internet. The most useful tool for gathering and examining information on topics of current interest may well be electronic journals. These journals are generally published by leading authorities in the field or in academia. Some examples of available electronic journals are as follows:

- *Journal of Criminal Justice* (https://www.journals.elsevier.com/journal-of-criminal-justice)
    - "Is a scholarly record of research and opinion on the intersection of crime, criminal justice, and popular culture."
- *Police Quarterly* (https://us.sagepub.com/en-us/nam/police-quarterly/journal201421)
    - "Emphasizes policy-oriented research of interest to both practitioners and academics."
- *American Journal of Criminal Justice* (https://link.springer.com/journal/12103)
    - Is "a multidisciplinary journal devoted to the study of criminal and deviant behavior, the social and political response to crime, and other phenomena related to crime and social justice."

- *Probation Journal* (https://us.sagepub.com/en-us/nam/journal/probation-journal)
    - "Provides a national and international forum for sharing good practice, disseminating high quality criminal justice research and developing debate about the theory and practice of work with offenders."
- Law Enforcement Enterprise Portal (LEEP) (https://www.fbi.gov/services/cjis/leep)
    - "A monthly newsletter which provides law enforcement with a digest of the best relevant information for law enforcement on the Internet."
- *NIJ Journal* (https://www.nij.gov/journals/Pages/welcome.aspx)
    - "The major journal on best practice and latest thinking and research in police science and management."

You can conduct a search for topics of interest, and the results will lead you to other publications, as well as those contained in this list.

LAW ENFORCEMENT AND THE INTERNET

According to the Law Enforcement Directory maintained by PoliceOne,[33] more than 11,000 criminal justice agencies have websites. As an example, in northern California, Placer County residents can file complaints, commendations, and crime reports on the sheriff's department's Internet site; in Roanoke County, Virginia, citizens can click on a map to find out about the latest crimes in their communities.

The Internet is a powerful, versatile law enforcement tool because it offers instant communication, and it crosses jurisdictional barriers. Citizens are able to report crimes, ask questions, and obtain information, all instantaneously. Law enforcement officials are also able to receive information, post pictures of wanted criminals, and communicate with local citizens.

Many websites include active links to federal agencies and state police departments. One of the best-known sites is CopNet (www.copnet.org). CopNet touts itself as a free community service without affiliation to any police agency, government body, or special interest group of any kind, unless clearly stated. CopNet maintains links to international agencies, crime prevention, search and rescue, electronic crime, events, firearms, forensics, list servers, missing, most wanted, seminars, security agencies, traffic, training, fitness, standards, and other sites of interest to the police world. The Federal Bureau of Investigation, the United States Department of Justice, and the International Association of Chiefs of Police also maintain Internet sites for public access.

You need only search the web for police sites, and a myriad become available for you to view—just one click away. In addition to the information mentioned previously, these sites carry information on training, where to get training, how much an officer can expect to be paid, physical standards for officers, and job postings—along with links to completing online applications for those jobs. Training academies that specialize in law enforcement preparation use the Internet as an advertising forum for their programs as well.

Access to the Internet provides criminal justice agencies with another tool to serve their communities more effectively. However, as with many other technological tools, the Internet has a dark side. What is beneficial to criminal justice agencies is also beneficial to criminals. The next section of this chapter will briefly review cybercrime and its ramifications for criminal justice.

CYBERCRIME AND CYBERSECURITY

A chapter on technology would be incomplete without a mention of the crime that is affecting every person who uses any technology to access the Internet for personal or business purposes. Due to the increase in use of the Internet for activities other than research and preparation of documentation, criminals have begun to exploit technology to commit crimes and to harm the safety, security, and privacy of everyone.[34] Titled **cybercrime**, this lucrative new venue for criminals is causing a migration of "traditional" crimes from the physical to the online world, as well as spawning a new set of criminal activity that targets computer networks themselves. Criminal justice agencies are facing technical, legal, and operational challenges in their battle with cybercrime. This section of the chapter will focus on some of these issues and the mechanisms by which agencies are addressing them.

Cybersecurity

Cybersecurity might have previously been more appropriately titled computer security since the value of theft was centered on the actual computer itself.[35] However, would-be thieves are more concerned with the data than the actual equipment since the real value lies in the information that can be stolen and used to the benefit of the thief. A more appropriate definition of cybersecurity may be the protection of the data that lie within the technology itself.

What Are You Trying to Protect?

The most readily identifiable target of value is identity theft. Most individuals attempt to protect their personal information, such as account numbers (ATM PINs and credit card account numbers) and the usernames and passwords associated with debit cards and credit cards. Less recognizable but equally important is the proprietary information associated with businesses—client lists, supplier lists, cost structure, and product information (intellectual, patents, and ingredient lists). Even the United States government is not immune from attacks designed to steal data concerning defense, intelligence, and basic infrastructure designs and protocols.

What Is a Hacker?

A hacker is an unauthorized individual who attempts to gain access to a device or network that he or she is not entitled to use.

What Are the Types of Attacks?

The most common attack may be the denial of service (DoS) or the distributed denial of service (DDos) attack, and the goal of these attacks is to prevent a system or service from functioning normally or to deny the use of access to a specific service or system.

The backdoor and trapdoor attacks were originally designed by software developers to ensure that they could gain access to an application or product in the event that they were unable to gain access through the normal methods.

Sniffing is an attack from someone examining network traffic that passes the network interface card (NIC). Another approach is spoofing, which is making data appear to come from a different source. The last and most publicized is referred to as phishing or pharming attacks. Phishing is the use of fraudulent e-mails or instant messages that appear to be genuine but are designed to trick users into opening and responding to them. Pharming is the impersonation of a website in an effort to deceive a user into entering his or her credentials.

Cybercrime

Cybercrime is of increasing concern to criminal justice agencies. Crimes such as threats, child pornography, fraud, gambling, extortion, and theft of intellectual property are migrating to the online world. To reinforce this information, you need only look to the address of former U.S. assistant attorney general Leslie Caldwell from the Cybersecurity + Law Enforcement Symposium in October 2015, where she talked about the increasing problem with cybercrime and cybersecurity:

> It's no secret that cybercrime poses a significant threat to the privacy and economic security of American consumers and businesses.
>
> Every day hackers are trying to steal the financial information of millions of victims from a computer halfway around the world. Cyber criminals are orchestrating massive disruptions of businesses or electronically spiriting away trade secrets on a daily basis. And, of course, every day we have threats from within: the disgruntled IT manager or the soon-to-be ex-employee, who steals, deletes or otherwise compromises company information.
>
> Indeed, this past year alone we saw a series of extraordinarily invasive and damaging data breaches that victimized some of our nation's largest businesses, as well as the federal government itself, with tens of millions of personal and consumer records being stolen or compromised at a time. All types of businesses were victimized, from banks to retailers, to mom and pop financial firms, to entertainment companies, to restaurant chains, to health care providers. Sadly, according to data from a recent report, there will be more than 32,000 additional victims of online crime by the time we're done with my session this afternoon.
>
> Hackers incessantly target us because barriers to entry are so low and because it is so lucrative. One study released last month estimated that cyberattacks have cost the global economy at least $315 billion over the past twelve months. A study from this past week stated that hacking attacks cost the average American firm $15.4 million per year. These figures only continue to grow and are just the financial effects. They do not capture the very real—but unquantifiable—personal harm suffered by victims of online crime, such as identity theft and sextortion.[36]

In December 2015, the Department of Justice created a Cybersecurity Unit and staffed it with Computer Crime and Intellectual Property Section prosecutors with extensive experience in the complexities of legal and policy matters associated with cybercrime. This unit was charged with helping the private sector to safeguard consumer data that have been entrusted to it.

In conclusion, cybercrime and the appearance of cybercriminals has presented a new threat to individuals, businesses, and governments around the world.

Criminal justice agencies worldwide must heed the advice of Assistant Attorney General Caldwell; we must "remain committed to bringing perpetrators to justice wherever they may be, disrupting cyber threats, and forging enduring global partnerships across the public and private sectors to ensure that our data, and our economy, are secure and protected from harm."[37] Twenty years ago, a new police officer was given a gun, a flashlight, and a notepad. When that officer retired, the three items would be returned to the police department, and the only intervening equipment expenses would have been replacement bullets, batteries, and note paper. Today, keeping pace with computer criminals means that law enforcement experts in this field must be properly equipped to fight crime on whatever front it presents itself—on the street or on the Internet.

SUMMARY

Criminal justice professionals in both law enforcement and corrections have long been enamored with technology and its potential applications. This fascination has traditionally been limited to specialized weaponry or equipment used in subduing aggressive violators. Tasers and stun guns are two examples of this technology. However, as the sophistication of criminals and criminal behavior has increased, so has the technology with which to detect and apprehend these individuals. Unmanned drones (aviation technology) are being seen more frequently in areas that police officers cannot access. They provide real-time data to crime analysts and criminal justice agencies so that this information can be used to better plan responses. Drones can also be used to capture real-time commission of crimes via video and other images. This information can be especially pertinent for court proceedings.

The organizational intranet, the Internet, and social media serve as primary means of communication to disseminate information among criminal justice agencies and the communities they serve and to help stem the tide of criminal activity. Furthermore, these communication tools assist corrections personnel in maintaining a complete and accurate record of incarcerated individuals and in ensuring that the guilty pay the fullest measure of their debt to society.

Other criminal justice technology, such as MDTs, the live scan fingerprinting process, and synchronous transmission, not only increases the effectiveness of law enforcement and corrections but also helps ensure the public is provided with the best and most cost-effective means available for maintaining a safe community.

The migration of "traditional" crimes from the physical to the online world is increasing. Cybercrime has become more lucrative to the criminal because of the ability to disguise identities, to reach more victims quickly, and to collaborate with other criminals. As computer technology advances with the identification of fingerprints and DNA, so too does the identification of cybercriminals become ever more important. Agencies are constantly searching for officers with new skills in computer investigation and telecommunications. Additionally, governments need to develop global legal structures that will support detection and successful prosecution of offenders. To keep pace with the cybercriminal of today, criminal justice agencies must be properly equipped with cutting-edge software and hardware and also be confident of laws and statutes governing prosecution of cybercrimes.

KEY TERMS

Amber Alerts 181
App 193
Aviation technology 180
Biometrics 181
Body armor 181
Bulletin boards 199
CAD Zone 190
Communication technologies 181

Crime mapping 181
Cross-projection 190
Cybercrime 202
Cybersecurity 202
Detection and surveillance 180
Grid 190
Intranet 183
Less lethal technologies 181
Listservs 199
Live scan fingerprinting process 192
Mobile data terminals 183
Predictive analysis 181
ScenePD 190
Silver Alerts 181
Social media 195
Synchronous transmission 192
Technology assistance 182
Triangulation 190
Vehicle and body cameras 180

FOR FURTHER REFLECTION AND DISCUSSION

1. Compare and contrast an organizational intranet and the Internet.
2. Evaluate the effectiveness of the mobile data terminal (MDT).
3. Are MDT transmissions superior to police radio transmissions? Why, or why not?
4. Compare and contrast the value of ScenePD and CAD Zone and the traditional methods of grid triangulation and cross-projection.
5. Compare and contrast the use of videorecording a crime scene and the traditional method of sketching.
6. List the advantages and disadvantages of installing cameras in law enforcement vehicles. Explain each statement.
7. List the advantages and disadvantages of having a departmental webpage.
8. What are some uses for criminal justice bulletin boards or listservs? How are they useful?
9. Suggest ways in which technology may enhance the effectiveness and efficiency of law enforcement and correctional agencies.

ETHICAL ISSUE EXERCISES

1. Is videorecording an individual suspected of a crime an invasion of privacy?
2. Who should be responsible for retrieving, reviewing, and storing video from law enforcement vehicles?
3. If an officer is accused of wrongdoing that may be captured on the patrol car video, should it be used in an internal affairs investigation?
4. If an officer is accused of wrongdoing, and it is captured on video that is used by internal affairs for departmental disciplinary procedures, could the same video be used in a criminal prosecution?
5. Should individuals who use the computer and the Internet to enter networks and databases to which they have no authorization be punished? Keep in mind that most young “crackers” enter these sites for the challenge rather than to tamper with or remove information.
6. Most of us know that it is wrong to break into our neighbors’ houses and steal things or damage their property. Is there a correlation between this behavior and computer hacking and virus dissemination? Why, or why not?