Chapter Twenty-one
Emerging and Future Technologies

Learning Objectives

- The student will understand the importance of looking at possible future technologies.
- The student will be exposed to a variety of new and potential technological applications in law enforcement.

Introduction

A large portion of this book was devoted to looking at how scientific discoveries and technical innovations have led to technological progress in law enforcement. For instance, we started with a look at binary digits and radio waves so we could understand practical technologies like cellular digit packet data (CDPD). Our understanding of past developments made the digestion of what is going on in the present more understandable.

Our look at the present was also often a look at possible futures. Consider that in many instances we looked at fully integrated systems, but we know that these are the exception and not the rule. For a variety of reasons, the implementation of technology in law enforcement has been significantly fragmented. Some agencies are very advanced, some are advanced in certain areas, but most are using technology that was available twenty or thirty years ago. Our view of past and present technologies should make us a better user of present technologies and a better decision maker about future implementations. Now we are at the point where we know enough about police technology to begin to think about possible futures.

Today you are likely to find major companies and government organizations employing consultants as futurists. These consultants forecast possible futures using a variety of quantitative and qualitative means. Their job is to provide information to organizations so they can chart their strategic course. While the title “futurist” is relatively new, the concept is very old. For instance, when human beings started to turn from hunter/gathers to farmers, they planted crops based upon their experiences with the fairly predictable cycle of the weather. You planted; it rained; you harvested. As things became more complex, humans looked at per-acre crop yields, transportation to market, transportation of water to increase yield, etc. We observed, recorded, and planned ahead. Our experience has been that most of the time, our predictions about the future when based upon the past are fairly good.

There are a number of techniques people use to predict the future. They may be qualitative such as Delphi surveys, questionnaires, and polls that use individuals with specialized or generalized knowledge. Based upon the results of these qualitative measurements, the people looking at the future try to reach a consensus among those surveyed or who participated regarding the possible future. We have also seen in our chapter on crime analysis that there are statistical methods such as extrapolation, probability, variance, regression, and correlation techniques. Other people looking at the future look for analogies with existing systems. They use the development of the existing systems to explore the potential for new systems. Still others use role-playing and simulation games in an effort to make predictions about possible futures. Simply stated, there are many ways that we can look at the past and present in an effort to predict the future.
Thinking about the future is your job. In this chapter you will be provided with a number of brief descriptions or vignettes of technologies that are being field tested for law enforcement, have some potential for use in law enforcement, or are being discussed as potential law enforcement technologies. These technologies are on the horizon. They are in the near future and decisions about their use will have to be made by people like you and me. Looking at the future, we may be able to see how decisions on use and implementation today will affect state and local police agencies in the future.²

Finding Us

Since 1982, during emergency situations, aviators and mariners have made use of emergency location transmitters (ELTs) and emergency position indicating radio beacons (EPIRBs). In that time, these technologies have reportedly been used in more than fourteen thousand emergencies.³ Recall in Chapter Five, on geographic information systems (GISs), we looked at how satellite technology was being used in automatic vehicle locator (AVL) devices. The ELT and EPIRB technologies are also satellite based. However, they are not true GPS devices. They do not use the GPS satellite constellation; instead they use a satellite constellation maintained by the National Oceanic and Atmospheric Administration (NOAA) called Search and Rescue Satellite-Aided Tracking System (SARSAT). The location determined by SARSAT is not as exact as the one that is generated by GPS satellites. When SARSAT receives a distress signal, the general geographic location of the signal is determined, and the appropriate search and rescue center is notified. Generally, this would be a United States Coast Guard (USCG) base. Aircraft and search vessels are then sent into the area where the signal is being transmitted. The signals generated by ELT and EPIRB can be monitored and triangulated by search and rescue aircraft and vessels. They home in on the signal and locate the beacon.

On July 1, 2003, the Federal Communications Commission (FCC) authorized the use of ELT and EPIRB technologies in the form of a personal locator beacon (PLB) for the general public. This type of technology will probably be useful for hikers, backpackers, and off-road vehicle users. When a PLB is activated, the SARSAT control center in Suitland, Maryland, notifies a designated contact point in the state wherein the PLB was activated.⁴

In the previous chapters we looked at AVL technology and we also briefly visited some of the commercial versions of AVL. It is likely that in the future commercial AVL systems, like the ones purchased for new cars, will include automatic collision notification (ACN) systems. These systems automatically contact Public Safety Answering Points (PSAP) if a privately owned vehicle equipped with ACN is involved in a traffic collision. Currently, some commercial AVL technology reports the activation of the airbag, but these new systems are likely to provide information about the collision. They would transmit not only the location of the traffic collision, but also information concerning the severity of the incident. With information concerning the severity of traffic collisions, the likely injuries could be extrapolated and the correct public safety response predetermined.⁵

Today if you walk through a department store, you will see that many of the high-value items within the store are tagged with a relatively large, often white, inventory control tag. Moreover, many preboxed items have a similar white tag that has a barcode (Figure 21.1), and inside the tag there is also an electronic inventory control device. If you walk past the threshold of the store without having the tag removed or demagnetized, a tone or disembodied voice directs you to return to the cash register. In the very near future, manufacturers are going to use
much smaller electronic tags embedded directly into the merchandise. Recall that
your cellular telephone constantly broadcasts an electronic serial number (ESN).
In the near future, nearly everything we purchase will contain a small microchip
and RF transceiver that will broadcast the product’s ESN.

This process is referred to as “chipping goods.” The transceiver located in
the very small and inexpensive tag (there are estimates that the tags will cost less
than four-tenths of a cent) does not contain a power source. It picks up energy
from the scanner that is used to detect it and sends back its ESN, using the energy
from the scanning device. Currently, these scanners can activate and detect the
ESN from about five feet. For the store, this will enhance inventory control and loss prevention. For state and local law enforcement agencies, the potential and
problems with these devices are vast.

What if a database of stolen tagged property was constructed? Every time a re-
tailer or manufacturer suffered a theft, they could report the theft and the ESN.
This information could be easily entered into a database. State and local police of-
ficers equipped with scanners could simply scan you and your vehicle during a
traffic stop or at any other time you walked by a police officer. Is this a search? As
these tags become commonplace and ridiculously inexpensive, will manufactur-
ers tag every can of soda? In many states theft of an object with a value of less
than $400 is a petty theft or a misdemeanor. However, possession of stolen prop-
erty is often a felony. What if you buy something, like a lamp, at a garage sale, and
it is stolen or at least reported stolen?

Another application of similar RF chips is embedding them into handguns. In
2001 5 percent of the police officers killed by firearms nationwide were killed
with their own handguns. The NIJ is sponsoring a project designed to protect police officers from being killed by their own weapons. One of the ideas is to modify handguns so that they can be fired only by their owners. There are a number of schemes under consideration, such as the police officer wearing a ring that must come into contact with the weapon or, alternatively, a ring that must be in close proximity to the weapon.

Much like the personal locator beacons we looked at earlier, specific location devices are under development for police officers. One such idea is to have a transmitter worn in or around the collar of a police uniform. The transmitter would constantly provide information on the police officer’s location and allow the police officer continuous communications contact with his or her dispatch center. In the future, you may see police officers using some derivative of the remote control information system (RCIS) which was originally developed for medics in the military. The RCIS is a highly compact communications system that provides video feed, two-way communications, and vital signs monitoring, and has a GPS feature. With a system like this, the communications dispatch center would see and hear some of what the field police officer sees. More important, by having a real-time feed, it would be possible for the police officer to access real-time advice on field situations.

Our Homes as Prisons

As of 2003, more than two million people were in prison and federal, state, and local governments spent $40 billion dollars a year on corrections. A technological solution to the cost of the number of people in custody is being tested. It is estimated that approximately 20 percent, or four hundred thousand offenders, could qualify for some type of house arrest arrangement. Currently, an offender who is under house arrest wears a bracelet with a transponder. At random intervals, the corrections agency calls the offender’s home. The transponder responds to these telephone calls, and if the offender is not at home, he is in big trouble. It has been suggested that this transponder be replaced with technology similar to AVL technology. By incorporating GPS and a computer monitoring station, if the offender leaves his home, the corrections agency would be immediately notified. It is not too much of a jump to see the potential state and local law enforcement applications. First, if this arrangement were used and an offender violated the terms of his house arrest, the corrections agency could notify the local police jurisdiction.

But there are other potential applications. While there are a lot of people in jail, there are many more people on probation and parole. A condition of probation or parole could be the wearing of this AVL-like technology. In the future, a police officer may be driving down the street and be automatically alerted that he or she is in close proximity to someone who is on either parole or probation. With relational databases, GPS, AVL, and in-car computer technology, the police officer could receive the offender’s photograph, physical description, and the terms of the parole or probation—in the car. Most offenders on parole and probation have surrendered their Fourth Amendment rights. They can be detained and searched without probable cause. Once alerted, a police officer might decide to stop and search the offender.

This technology also has potential applications for crime analysis and crime prevention. Since most crime is committed by repeat offenders, if offenders on parole or probation were wearing AVL technology, it could have a deterrent effect. Moreover, someday crime analysts might find themselves running comparisons between AVL-monitored offenders and crime patterns.
Scanning Us

There are a number of new scanning technologies that allow for very precise scanning for metallic objects and contraband on people. Two of these are magnetic gradient measuring and passive millimeter wave (MMW) imaging.\(^8\) Fluxgate magnetometers measure changes in the Earth’s magnetic field caused by metallic objects. As people walk through a portal, or gateway, they are scanned and the results of the scan are compared against a database that contains the magnetic disruption of the Earth’s field by a certain weapon. This technology would be used to replace the large metal detectors that you must pass through on your way into many public buildings. It is predicted that this technology will be more reliable and accurate, speeding entry and reducing the number of false alarms. So unless your car keys meet the exact magnetic disruption of a handgun or knife, you walk on through.

Passive Millimeter Wave can see through your clothing. Fortunately, it cannot see your anatomical details, but it can detect weapons, plastic explosives, and other types of contraband. The technology uses the natural emissions from objects and, therefore, does not require that you be scanned. The NIJ is working on a project to mount MMW technology on a police vehicle for field use. This technology is probably a decade or so off, but think about the search and seizure issues involved. In addition to MMW, there are experiments underway to combine radar and ultrasound technology to allow for remote searching of people.

Using a video camera, an infrared light source, and optical character recognition (OCR) software, the text from a vehicle license plate can be read by a computer. The OCR software converts the text to a binary code and that code can be compared against many different relational databases. Although this can currently be done in real time, it has some limitations. The license plate on your car is made of a highly reflective material and is very good at reflecting infrared light. Of course, infrared is out of our visible light spectrum, so we never know when someone is shining an infrared light on us. The infrared image returns to the camera, and using an OCR-like algorithm, the license plate number of a vehicle is converted into computer code and can be stored and compared. These systems are being used in private industry for access control to parking structures, by quasi-governmental agencies for toll booths and at some border checkpoints. Currently, this technology has not been developed to the point where it can be installed in a police vehicle, but that is not far off. In the future, police officers will be alerted by their optical license plate reading (OLPR) system that the car in front of them is stolen or unregistered or the driver is wanted.

Dataveillance

Throughout the text we looked at a wide assortment of databases. We saw that the federal government alone has some two thousand databases, but so does your grocery store for their discount card, the bank for the ATM, the library, and the hospital. Just about every organization is creating relational databases. Dataveillance is the term coined to describe the use of data in the investigation and the monitoring of us.\(^9\) It is watching us not by camera, not in person, but through our transactions.\(^10\) As databases become more interconnected and cross-referenced, greater questions about personal privacy need to be asked. Think about combining any of the technologies in this chapter with dataveillance. For instance, when you go to the store, your discount card records your purchase and the chipped goods report exactly what you have purchased. You
are driving down the street and OCR technology records your license plate as you travel. The potential and danger of any technology is increased by a relational database.

**Using the Us of Us**

**Biometrics** is the science of using technology to automatically identify an individual based on physical, biological, and behavioral characteristics. We have talked about a biometric science many times in this textbook. Think back to what made fingerprint evidence both strategic and tactical information. Fingerprints became tactical when it was possible to take a scan of a fingerprint, convert the fingerprint to binary code, and check the fingerprint against a database. That is the essence of biometrics—automatically identifying an individual based on characteristics.

There are two classifications of biometric information. First, there are physiological characteristics like your fingerprint, DNA, facial features, eye pattern, and **hand geometry**. Second, there are behavioral characteristics that are unique to people, such as voice and handwriting. Biometric information has the capacity to go even further. There is the way you walk, or your gait; your personal thermal pattern; and your personal magnetic resonance. Anything about us that is unique and can be converted to a digital format can be used to differentiate us from others automatically.

Currently, there are two broad categories of use for biometric information: access control and remote identification. Access control is used to prevent unauthorized individuals from gaining access to a location or to information. You probably don’t know it, but you partially participate in biometric access control every day. Strict access control is a combination of three factors: what you are (biometrics), what you have (your ATM card), and what you know (your personal identification number, or PIN). Every time you use your ATM card, you gain access to your money by showing what you have (your ATM card) and telling what you know (your PIN). If you use a credit card, you show what you have (the card) and what you are (your signature), and often present picture identification (what you are) to gain access to your credit. The only reason a credit card is not a biometric transaction (yet), is because your picture or signature are not verified by comparing them to a relational database. However, there are many government locations and some private industry locations that may be accessed only through the use of biometric information. This happens when employees present identification (what they have), enter an access code (what they know), and verify their identities by fingerprint, retina scan, or hand geometry (what they are).

The other use of biometric information is to ascertain identity for purposes other than access control. The use of livescan devices by police officers is a prime example of using biometrics for a purpose other than access control. Although fingerprints have been known to be unique for more than a hundred years, the first biometric applications were with hand geometry. More than twenty years ago, the first biometric device was installed on Wall Street for timekeeping purposes. That device measured the length of the human fingers. Today, by taking a number of measurements, the hand geometry device can be found as an access control measure in a number of venues. For instance, hand geometry was used as identification equipment during the 1996 Olympics in Atlanta.

In addition to hand geometry and fingerprints, iris and retinal measurements are used to uniquely identify individuals. A retinal scan consists of a low-intensity beam of light directed into the individual’s eyeball. The pattern of veins in the eyeball are recorded, converted to a digital format and then compared against a relational database. An iris eye measurement photographs the iris in the front of
the eye. Retinal vein patterns can change over time, but the iris does not change and, like fingerprints, is unique to the individual.\textsuperscript{11}

One of the most controversial biometric applications is \textbf{facial recognition technology (FRT)}. With FRT, a digital photograph of an individual’s face is used to take measurements between nodal points, which are locations on every human face. For instance, the centers of the eyes, the tip of the nose, and the corners of the mouth are nodal points. While there are about eighty different nodal points, an FRT software algorithm requires only between fourteen and twenty-two of these points for comparison. Recall our examination of fingerprint technology in Chapter Six; FRT measurements and the subsequent conversion to a searchable database are somewhat similar. Facial recognition technology is being used in some jail management systems as a means of identifying people during the booking process and while they are in custody. This technology seems to work well as a supplement to the normal booking procedure. Although this software has been deployed at public events such as concerts with closed-circuit television cameras, there remains a considerable amount of technical and policy aspects that still need to be worked out.\textsuperscript{12}

But of all the new biometric technologies, facial probably has the most promise and probably the most controversy. In Chapter Fifteen we found that you can’t go anywhere without being videotaped. Moreover, you probably have seen a video on the news of a robbery or burglary where the offender is unidentified and the police are asking for assistance. In Pinellas County, Florida, and Los Angeles County, California, digital photographs are taken of offenders as they are being booked. Between these two agencies there are nearly one million photographs. If facial recognition algorithms and relational databases can be improved to the point where a million photographs can be filed and searchable by FRT, this biometric application may become a valuable investigative tool.

With improved FRT, once a first responder seizes a video as evidence, that video could go to a lab and the photographs of the offender can be compared against a database of known offenders. Since most are repeat offenders, there would be matches. Eventually, many offenders whose crimes were videotaped would be identified very quickly. Sometime in the future, when FTR algorithms, databases, and bandwidth issues mature further, we will probably see the in-car camera of a police vehicle being used for OCR of license plates and FRT for wanted offenders. Imagine a police officer driving down the street, his superintelligent police car scans for offenders on parole and probation with AVL, and his in-car camera scans back and forth, capturing license plates and the faces of people on the street. His supervisor is receiving real-time feed of the in-car camera and the camera and audio installed on the police officer’s person. Of course, dispatch tracks the police officer’s progress with AVL. It may be that some day the police officer will just ride in the car and it is preprogrammed to drive where and when the next crime is to be committed. You have seen all of this technology; it isn’t far off.

Although a unique identifier, DNA is not yet fully under the biometric umbrella because of the way it must be collected and analyzed. However, consider that fingerprint evidence remained a nonbiometric science for more than a hundred years after its first use in law enforcement. As science and technology matures, it is quite likely that some day, perhaps decades off, DNA samples will be routinely “sniffed” from the air (recall we drop DNA everywhere) and like fingerprints, the police officer will know the offender’s identity.

Voice recognition and handwriting are considered behavioral biometric sciences. Their applications in law enforcement are limited because of issues concerning conclusiveness. However, voice recognition biometrics probably could be used during wiretaps to provide insight into the identity of a caller.
Satellite Technology

If you asked most law enforcement managers what the potential use of satellite technology was for law enforcement, they would probably answer, “communications.” Although it is not practical or economical to use satellite technology in law enforcement, the potential to relieve some of the problems associated with dead spots in communication exists. Our look at satellite technology centered on its GPS capabilities, but there are other types of satellites—communications satellites probably being the most common. But what about using satellites for observations?

By combining infrared, visible light, and radar technology, a satellite can look down and see relatively small objects, very clearly. Who really knows how good the optics are on a military satellite? What if one were used to look down on an American city. Consider a real-time feed from a satellite to the communications dispatch center. When a burglary or robbery call comes in, the dispatcher could instruct the satellite to focus on the location. Currently, in many large cities, law enforcement uses helicopters for speedy response to emergencies. Helicopters have caught offenders leaving the scene of the crime many, many times, but helicopters make a lot of noise (warning offenders), and they, too, have a response time. But what if response was nearly immediate? What if the satellites fed information to ground stations and computers continually monitored for environmental changes, like sudden heat plumes. Could the fire department be dispatched before anyone even realized there was a fire? Perhaps the satellite relays images to a computer, and in the middle of the night, the computer continually looks for environmental changes, such as a thermal signature of burglars on the roof of a business? All of the technology exists, just not in this combination. However, what would be the public’s reaction to this type of monitoring?

Pursuit Technology

As we saw in a previous chapter, the only means of pursuit termination are currently mechanical. One recent improvement has been the development of spiked barrier strips which have retractable and remotely operated spikes. Now the strip can be placed down even if other motorists are nearby, and only activated as the offender’s vehicle passes over. There have been some interesting suggestions for technology: a small radio transmitter that is deployed to the offender’s vehicle with a handheld launching device; a low-power radio transmitter that allows the police to talk to the offender; spiked balls on a chain to be shot across the roadway; and a giant parachute that would be launched as a package from an aircraft and once it attaches to the vehicle, it causes slowing by increased drag. I didn’t make any of those up.

One electric solution that has been suggested is the use of a very strong electromagnetic pulse directed at the offender’s vehicle. The pulse would burn out the computer chips that run the car, causing it to stop. There might be a problem with offender’s braking and steering the vehicle after it shuts down in such a manner, and issues abound concerning accidentally hitting another vehicle with the pulse. One promising solution is the use of a laser device that allows police to specifically target a vehicle, if that vehicle has a preinstalled computer chip. When the laser strikes the vehicle, the chip slows the vehicle to fifteen miles per hour and eventually shuts off by restricting the flow of gasoline. Another similar technology proposes that a chip be preinstalled that allows police officers to shut the vehicle off after it has been reported stolen. For either of these technologies to work, they would have to be legislatively mandated into new vehicle construction.
That solution probably isn’t far from what will eventually happen. Manufacturers are increasingly including GPS systems that enable AVL. There isn’t much to engineering the remote shutoff chip. While commercial AVL is a consumer choice, a mandated product would not only help to reduce police pursuits, it would probably decrease new car theft, or at least minimize damage to newer cars because the AVL would allow the police to track down the stolen cars. Of course, there are privacy issues.

With the difficulties associated with driving during a high-speed pursuit, it is unlikely that we are going to see a device actually deployed from the chasing vehicle. If anything, like the spike strips, police officers may be able to anticipate the offender’s route and deploy some electrical device. Deployment of external charges or pulses from a helicopter seem unlikely, because of aiming and the potential effects it might have on the helicopter. In reality, the only viable near-term solution seems to be the internally installed chips.

**AVL**

As AVL technology in police vehicles becomes more commonplace, we are likely to see a continued integration of AVL into any number of other systems. One suggestion has been combining AVL with traffic management systems. So if you are a police officer and you activate your emergency equipment, AVL gives you the route to your call and gives you green traffic lights all the way there. This has applications for all of public safety. It would likely speed up police, fire, and emergency medical services response in urban areas.\(^5\)

**Less-Lethal Use of Force**

Through the National Institute for Justice, the Oak Ridge National Laboratory in Tennessee is involved in the research and development of less-lethal force devices. They are looking at a variety of exotic tools that can cause temporary physiological responses like nausea. They are investigating how the human body responds to sound, light, and different types of electromagnetic waves. What they are looking for is a less-lethal force device that incapacitates the offender without causing injury. One of the things they have experimented with is using RF energy to raise the body temperature of an offender. This RF energy, or thermal, gun would cause an offender to become disorientated. They have also experimented with using electromagnetic energy to produce a seizure in the offender, another energy beam weapon that causes the offender to “see stars.”

**Getting Smaller**

One of the operational strategies often associated with community-oriented policing is the deployment of police officers on foot or bicycle patrol. Police officers assigned to these duties can carry only a limited amount of equipment. Unlike most police officers assigned to vehicle patrol, these police officers did not have ready access to databases via a computer. With the introduction of personal digital assistants (PDAs) police officers assigned any detail have computer access to databases from motor vehicle departments and the National Crime Information Center.\(^6\) Recall from Chapter Two, a PDA is a handheld personal computer (Figure 21.2).
Chapter Summary

Some of the technologies mentioned in this chapter are very far from deployment in the field and others are examples of interesting but not quite useful ideas. An underlying theme of this chapter is how different technologies are being combined to make them more effective or to be used for a completely different purpose.

New technologies also bring new questions about policy. As was stated in the beginning, most of police work is about gathering information. Therefore, it is not surprising that most of the technology being introduced into law enforcement enables the collection, organization, and analysis of information. Moreover, since the police and technology are focused on information, the primary community concerns usually center around issues of privacy and the Fourth Amendment.

Technology is making police work more complex. Certainly, in some instances it is making police work efficient, but technology adds to the information a police officer must know. A police officer must still know how to communicate with a wide variety of people often under stressful circumstances; a police officer still must exercise basic tactical skills like standing with the gun leg back; a police officer must still know how to use their traditional tools like the radio, vehicle, baton, and firearm. Added on top of the basics is new technology—a computer in the car, AVL, and two thousand federal databases.

Discussion Questions

1. If you were in charge of nationwide development of new police technologies, which of the new technologies or areas of technological development would you emphasize? Why?
2. Which of the emerging and future technologies do you think will have the most difficulty with community acceptance? Why?
3. Based on what you’ve read, what combinations of technology do you think
would be useful for police officers?
4. Based on all of the technology you’ve read about, how can technology enable
or enhance community-oriented policing?

**Key Terms**

- Automatic Collision Notification (ACN)
- Biometrics
- Chipping Goods
- Dataveillance
- Facial Recognition Technology (FRT)
- Hand Geometry
- Magnetic Gradient Measuring
- Passive Millimeter Wave Imaging (MMW)
- Personal Locator Beacon (PLB)
- Remote Control Information System (RCIS)
- Transponder
- Universal Product Code (UPC) Barcodes

**End Notes**

4. In California, the contact point for PLB alerts will be the Governor’s Office of Emergency Services Warning Center.
7. Ibid., 3.
9. Clarke, “Information Technology and Dataveillance.”
12. See note 6 above.
15. See note 5 above.