Chapter Ten
The Internet and Law Enforcement

Learning Objectives

• The student will have an understanding of the historical development of the Internet.
• The student will have increased skills in navigating the Internet.
• The student will be exposed to how law enforcement organizations have used the Internet.
• The student will understand how the Internet can increase a law enforcement agency’s efficiency and, possibly, effectiveness.
• The student will understand how the Internet can be used as a technological enhancer of the community-oriented policing model.

Introduction

In this chapter we first look at the historical development of the Internet, then begin to build on our skills and knowledge of police technology by exploring different methods of navigating and searching the Internet. In the place of case studies, we will look at a variety of law enforcement agencies’ Web sites as a means of exploring and understanding the potential of the Internet. Throughout this chapter we will be asking these questions. How can the Internet increase a law enforcement agency’s efficiency and effectiveness? How can the Internet be used as a technological enhancer of community-oriented policing?

Recall from Chapter One, technology is seen as an integral part of community policing. However, the part that technology plays is as an enhancer to the core elements of the model. For instance, in this chapter we will examine ways in which the Internet is being used in problem solving, increasing community partnerships, and increasing community participation. In Chapter One, in addition to looking at the COP model, we looked at how state and local law enforcement agencies are developing crime prevention operational strategies that fall into three broad categories. As we examine state and local law enforcement’s use of the Internet, we should be looking for ways that Internet technology has enhanced or can enhance situational crime prevention, community crime prevention, and criminality prevention.

The History of the Internet

In 1994 nearly 94 percent of American homes had telephones and just over 24 percent had computers. Interestingly enough, in 1994 the United States Census Bureau did not even ask Americans about their use of the Internet. By 1997 the percentage of American households with a telephone remained constant, but the presence of a computer in the home had grown to more than 38 percent and nearly 19 percent of Americans had Internet access. By 2000 the presence of a telephone grew slightly, but the personal computer was now in 51 percent of American homes, and Internet access had more than doubled to nearly 42 percent. The growth in access to the Internet has been exceeded only by the growth in what is available on the Internet. In 2003 Internet users had access to more than three billion pages of information, and approximately three million...
As we discussed in Chapter One, there are two broad areas of operational strategies for the implementation of crime prevention. The first involves the identification of specific crime problems and the application of tailored response to those problems. The second is a crime prevention strategy that examines the root causes of crime within a community and the tailored responses to those issues. In this chapter on the Internet we will look at ways the Internet has assisted or can assist with crime prevention; Chapter Twelve, on crime analysis, will delve much deeper into these issues.


A Look Ahead

As we discussed in Chapter One, there are two broad areas of operational strategies for the implementation of crime prevention. The first involves the identification of specific crime problems and the application of tailored response to those problems. The second is a crime prevention strategy that examines the root causes of crime within a community and the tailored responses to those issues. In this chapter on the Internet we will look at ways the Internet has assisted or can assist with crime prevention; Chapter Twelve, on crime analysis, will delve much deeper into these issues.


new web pages are added daily. Although today the Internet is very large, it did not start out that way. The idea was always big, but the actual network started out comparatively small and stayed that way for a relatively long time.

In 1962 J. C. R. Licklider wrote a paper at the Massachusetts Institute of Technology (MIT) entitled “On-Line Man Computer Communication.” In that paper he described the “galactic network,” an idea that in theory operates like our Internet of today. Throughout the early 1960s and into the 1970s, the precursor to the Internet was called the ARPANet, after the Advanced Research Projects Agency within the Department of Defense, which provided the funding for the project. Essentially, the United States government needed a way for the government employees, researchers, and contractors to communicate effectively.

The early development of a worldwide communications network was undertaken for military communications. The “urban legend” that the Internet was designed so that a communications network could survive a nuclear attack does not appear to be the driving force behind development and implementation. However, in the minds of some, it may have eventually had that characteristic, but it does not seem to have been a driving motivator.

The ARPANet was developed by United States government employees and people working in the academic field. In fact, the first communication hookups were between two academic computers linked into the ARPANet. The first two computers were located at the University of California at Los Angeles (UCLA) and Stanford University, California. Among the greatest early technology challenges that ultimately made the Internet successful was the development of data packets. Recall from our earlier chapters we discussed that digital data moves across wireless and hardwired networks in small packages. In 1972 the development of the ARPANet went public when it was premiered at the International Computer Communications Conference. It was also at this conference that e-mail was introduced.

As it developed, the primary foundation of the Internet became that it is an open architecture network. This means the Internet grew from multiple networks of different designs that could be linked together using some basic principles. Today’s Internet is not one big network. Rather, it is many networks that are linked together. In Chapter Three (“Wireless Communications”) we briefly looked at the history of the development of cellular telephones. We mentioned in

In 1984 William Gibson coined the term cyberspace to describe the place where people interact, communicate, and exchange information using the Internet.


200 Part Two Strategic Information Systems and Technologies
Because e-mail has numerous ramifications for both the employer and the employee, we will take a closer look at using e-mail later in the chapter. For now, e-mail was considered the first “killer app.” In the computer technology industry, a killer app (application) is a computer program (recall from Chapter Two that a computer program can be either an operating system or an application) that becomes incredibly useful.

Source: Cunningham, B2B, 179.

that chapter that before 1984, American Telephone and Telegraph was the primary carrier for telephone service in the United States. There was, in essence, one big telephone company. Recall from our chapter on networks, we saw that there were local area networks, wide area networks, and even metropolitan area networks. By using the right protocols, these privately owned networks can become part of the Internet. Any computer or network that has Internet access has become a small part of the huge, global network. The point to remember is that there is no one big company, enterprise, or network that is the Internet. The success of the Internet is that everyone who gains access becomes part of the global network. You and I are the Internet.

Recall in Part One (“Introduction to Theory and Basics”) we discussed packaged data several times. In Chapter Four, on networks, we looked at the Transmission Control Protocol/Internet Protocol (TCP/IP), which is essentially software that divides information into packets and then transmits this information in its divided form. Packaged data and TCP/IP protocols are essentially all that is required for computers on the Internet to communicate. There can be other protocols involved in a network connection—for instance, Serial Line Interface Protocol (SLIP) or Point-to-Point Protocol (PPP) connections.10 Earlier we learned that protocols are the rules and language we must use to complete electronic transactions. We also learned that TCP/IP is the Internet standard. This protocol gave us four principles from which the Internet flows. First, as we have said, each network is its own design. It does not have to comply with some global Internet standard. Second, if your data gets to its destination corrupted (recall error detection coding in data packets from Chapter Three), you, the sender, would retransmit the data. Third, the access points (gates and routers) to the Internet would be only access points; they would not keep information about the data that passed between them. The third point is important. When compared to most of the technology that makes up the Internet (such as servers), the access point technology is relatively simple. It would be significantly more complex if it did much more than foster access. Fourth, there would be no central Internet control point. There is no Big Brother engineered directly into the Internet.

A Look Ahead

Although there is no “Big Brother” engineered directly into the Internet, there are a number of means by which the transfer of data is monitored by the government. Some people have argued that although there is no Big Brother, there is a series of “little brothers.” Our text focuses on state and local governments, and Internet monitoring is done by the Federal Bureau of Investigation (FBI). In Chapter Fourteen, when we look at wiretaps, we will examine how Internet communications can be monitored by the government. Moreover, in Chapter Sixteen on hi-tech crimes, we will look at how the Internet is used to facilitate certain crimes and how law enforcement and private industry are responding to these crimes.
For the next decade or so, the Internet remained primarily as a resource used by the government and increasingly by the academic community. In 1987, there was a significant development in the standardization of software technology that ultimately gave us today’s Internet and World Wide Web. As more and more networks became part of the larger Internet, a new protocol was needed for the management of the access points (routers). Ultimately, the Simple Network Management Protocol (SNMP) was adopted. In addition to TCP/IP, SNMP became standard rules and languages our computers would use to communicate.

Some people use the terms Internet and World Wide Web as if they are interchangeable. In some sense they might be interchangeable, but they are different concepts. The Internet is the system of protocols and architectures that allows the vast number of different networks and, ultimately, different computers to communicate. Because we use telephone lines and direct service lines (DSL) to connect in a wired mode, radio frequencies to connect in a wireless mode, and dedicated lines to connect between networks—the Internet is virtually every means of transmitting digital information around the planet. Because the Internet does use satellite signals and we can view images from other planets, the Internet is arguably solar system—wide. Essentially, the Internet is the information super highway. On the other hand, the World Wide Web is a way in which most of us use the information super highway.¹²

The World Wide Web is based on client/server computing.¹³ In this arrangement, the client is a Web browser that can communicate with any Web server on the Internet. Moreover, the Web server shares resources with all of the Web browsers.¹⁴ Think of a drive-through hamburger stand. As you drive through, you are the client. You place your order into the speaker. At the other end of the speaker, the server is taking your order. At the same time, the server is quite possibly doing other things. For instance, he might be recording your order on a touch screen, filling sodas, making change with the person ahead of you, or passing your order to the cook in the back. Moreover, the speakers and the wires that connect them are the network between you, the client, and the server in the hamburger stand. As more people put demands on the server, your service slows. Our server in the hamburger stand is like a computer in that he can multitask, but as we noted in Chapter Two, a computer can do only one thing at a time, and the appearance of multiple things going on is an illusion of speed. Your Internet client/server relationship is similar. The client (your computer) makes requests to a server through a network of connections. The server is receiving and managing other requests from different clients.

The World Wide Web consists of pages of information that are linked together.¹⁵ These electronic links between pages are called hyperlinks. Hyperlinks make it possible to jump from one document or Web page to another.¹⁶ For instance, you may be on one Web site and see that they provide a link to some document that provides more information on a subject. Many of the endnotes in this text provide you with Web site addresses for additional exploration. If this textbook were a Web page, you could click on those links and would be taken to another Web site. By using a link on a Web site, you are never really sure where you are going. The Web site might be maintained by the person in the house next to yours, or it might be all the way around the world from you. The linkages between the pages are what make them a distinctive web of information.

In 1988 the commercialization of the Internet began to take hold. The people who had been responsible for the development of the Internet up to that point began to hold tradeshows that introduced the technology and concepts they had developed. At this point most private individuals who gained Internet access
probably did so through an access service provider (ASP). Many ASPs provide a variety of other services to their clients like newsgroups and chat rooms.

Throughout the 1990s the Internet began to increase in size and scope as more people joined the Net. Today, the Internet is nearly everywhere. It has grown beyond the early government and academic uses to a tool for all.  

Navigating the Internet

Now that we know how the Internet and World Wide Web were created, we need to learn how to navigate the Net. The Web consists of millions of cyberlocations created by people to exchange information. Some of the Web sites are commercial information—someone is trying to sell you a product or service. Some are governmental, academic, or not-for-profit sites that have a number of purposes. Finally, there are the thousands upon thousands of personal sites dedicated to a hobby, a family, or some personal interest.

Although some of the Web sites consist of a single page, most consist of multiple Web pages. The first page (and occasionally the only page) is considered the Web site’s home page or, as it is increasingly referred to, index page. The Web would not be as we know it today if each of the Web sites’ owners had to have their computer constantly connected to the Web. In other words, if each time you visited a Web page you were actually going to the Web site owner’s computer, there would be far fewer Web sites and the system would be significantly slower. When you visit most Web sites, the physical location you are going to is an internet service provider’s (ISP) Web server. In Chapter Two (“Computer Basics”) we discussed servers. A Web server is a computer dedicated to managing the information flow associated with the Internet. ISPs provide a large variety of services to individual users and organizations. For instance, an ISP might provide Internet access, Web hosting, electronic mail, and e-commerce services. The physical location of the ISP Web server is called the point of presence (POP). Although an ISP can provide many services, many ISPs center on hosting Web sites. In order to be an ISP, one would have to have high-speed access of at least the capability of a T-1 line and a server. Companies like America Online who primarily provide access to the Internet, are referred to as access providers. However, just as an ISP can provide access, an access provider can provide Web hosting.

If you have Web access at home, you are using an ASP. That ASP can be dial-up, cable, an asymmetrical digital subscriber line (DSL), or some direct access scheme. The ASP you use for access probably will also provide you with limited space for a personal Web page.

Today most people are using one of two browsers as a means to explore the Internet—Internet Explorer or Netscape. These browsers are graphical user interface (GUI) software applications that simplify Internet navigation. As we know from Chapter Two, a GUI scheme is one that provides the user with icons to complete certain tasks. The body of the browser is the Web page that the browser has accessed (Figure 10.1). When you connect to the Net using a browser, your browser has a predetermined home page. If you are using an ASP like America Online (AOL), this configuration with your browser is different. We are going to work with an ASP that is unlike AOL, one that only provides you with access to the Web. We are doing this because most law enforcement Internet access is through an ASP that provides access only and not the myriad of services available through an ASP like AOL. Depending on how your Internet service is configured, there may be some type of authentication...
process that allows access to the ISP. If you are using the Internet at school or in a large organization, the Internet is probably accessed by simply clicking the browser icon on your computer screen. However, if you have dial-up service, you may have to enter a user name and password to gain access to the Internet. Additionally, when you first open the browser, if you are using a computer at home, the browser will default to the software manufacturer’s home page. If you buy a computer that is specifically manufactured for you, from Gateway for instance, they may set the browser default to their home page. We, however, have control over this. With Internet Explorer, click Tools, Internet Options, General, and you will see the place where you can change the home page (Figure 10.2).

On the Internet, each Web site that you visit has an address. We are used to accessing an address like www.prentice-hall.com. This address is to the Web site is called a domain name. However, in reality, the domain name, or Web site address, is actually a number. In this instance the actual address for Prentice Hall, the publishers of this textbook, is 192.251.135.15. Recalling a bunch of numbers so that we can access different Web sites would be cumbersome. We would end up keeping an address book nearby so that we could visit our favorite sites. The browser simplifies this by giving us an address line (at the top of the browser in Figure 10.1) that translates the number into the domain names with which we are familiar. This address line software application is called the universal resource locator (URL). You have probably noticed that before the domain name is the URL, there are the letters www—rather obviously, the World Wide Web. Preceding those letters you will find—http, which stands for Hypertext.

Figure 10.1 The opening page of the browser Internet Explorer with the homepage set to Google. Permission to reprint provided by Microsoft Corporation and Google.
The domain name has an extension that generally describes the general function of the organization. The six most common extensions are:

- Commercial organizations (.com)
- Educational institutions (.edu)
- Military (.mil)
- Government (.gov)
- Miscellaneous organizations (.org)
- Networking organizations (.net)

In the United States, an organization called InterNIC is the governing body controlling the issuance and control of Internet domains and addresses. The management of domain names is done through a partnership between the United States government and a private firm, Network Solutions, Inc.

Source: Cunningham, B2B, 100; 179.
You can find out the actual numerical IP address of any Web site at www.networksolutions.com/cgi-bin/whois/whois.

Try This

File Transfer Protocol (FTP) is a protocol used on the Internet to transfer many different types of information in the form of files and data. For instance, were you to create your own Web site, you might use FTP to load your Web site from your computer (where you designed it) to your Web host. Source: Cunningham, B2B, 177.

your computer. Although temporary files have a preset lifespan, you can change the settings on your computer to delete them earlier or you can delete them yourself.

The browser is also translating the program language used to design the Web site into the images on the page you are viewing. The most common Web site programming language is **hypertext markup language (HTML)**. HTML uses programming cues called **tags** to tell our computers what we should see on the screens. It gives the Web site developer the tools to add color, lines, and formatting to his or her Web site. For instance, in order to determine the colors that the Web site is going to be, the tags used are six-digit numbers. The color tags use two-digits to identify distinct shades of the primary colors. By combining the two-digit shades of the primary colors, your computer knows what color the programmer intended you to see. As an example, 999999 is the code for black. Conversely, 000000 is the code for white. All of the colors of the rainbow fall between the codes of 000000 and 999999. The programming language HTML can format the text of a document; create links to Web pages; describe the structure of a Web page; and display different kinds of media like images, video, and sound.

With HTML you can create the perfect Web site. The only problem is your Web site is just a collection of pages in a special file on the Internet. With HTML it is static and unchanging. In order to create more dynamic Web sites, developers use programming that tells a computer to execute a program—to do something. The programs, or scripts as they are called, use a computer’s common gateway interface, or CGI. With special scripts, the CGI can be used to create interactive maps on a Web site.

One of the common scripts used in conjunction with CGI is Java. Java was created in 1995 by Sun Microsystems. Essentially, when you download an HTML file that requires Java, the Java applet (applet is a term for an application that runs a relatively simple program) is downloaded to your computer and it runs the Java program. The use of Java adds to the dynamic nature of Web sites. Since we are not aiming at becoming Web developers (fancy programmers) we will stop here.

With thousands of ISPs hosting millions of Web pages of organizations and individuals, how can we find anything? One way is to rely on private firms that have designed **search engines** to do the hard work for us. One such search engine is Google. A search engine searches the World Wide Web for keywords, keeps an index of the words it finds, and allows users to look through those indexes for words or combinations of words.

A Look Ahead

In the next chapter, on information exchange, we will look at another type of Web programming that is becoming increasingly useful and popular, extensible markup language (XML).
While at your home page, in the upper left-hand part of your browser, click View. A drop-down menu will appear. Click Source. Another window will open up in Notepad. You are looking at the programming language that makes up the Web site you are viewing. Note that in the very top left-hand corner you probably see <html>; this tells you that the primary code used to write this Web site was indeed HTML.

Permission to reprint provided by Microsoft™ Corporation and Google™.

Spam is unsolicited e-mail. In most instances, spam e-mail is very much like junk mail, in that it is sent out in huge batches. Spam is not a known acronym for any technical term. Spam is however, the canned meat product produced by the Hormel company. Some say that the term spam (to denote junk e-mail) comes from a Monty Python skit. If you are so inclined, a quick Internet search for “spam Monty Python” will locate a Web site wherein you can hear Vikings singing the “Spam Song.”

Source: Cunningham, B2B, 183.
Experiment with something like what we older cybernauts used instead of a modern search engine. As we know, before the advent of the Web of today, people used search engines like Veronica, Archie, and Gopher. On your computer, click Start then All Programs. Then select Accessories and Command Prompt or DOS Prompt. Your computer will open a new window that bypasses your GUI and allows you access to the underlying disk operating system (DOS). You will see a flashing cursor. Type “telnet” and hit enter. You now see “Microsoft Telnet.” This is Internet access as it used to be. On the command line, type “o.” If you are connected to the Internet, type “bbs.fament.com” and hit enter. Once at the Family Entertainment site, you are using the Internet, but not the Web, per se. However, you will be in an “old style” bulletin board system (BBS) that was used for Internet access. You probably noticed that it does not have any of the visual characteristics of today’s Net. If you have time (I know that paper on underwater basketweaving is waiting), go into the Tradewars game and compete with the older cybernauts. You will find that it is nothing like the games of today, but we still like it.

Source: Cunningham, B2B, 184.

The spiders, for being so small, are pretty smart. They look at every word except articles. So, the spiders crawl past words like a, an, and the, but they look at every other word and, depending on its location and frequency of use, begin to develop an idea of how to rank the Web site for your search. People who have designed Web sites want the spiders to recognize how applicable they are to your search, so Web site developers use HTML meta tags while writing your Web site (Figure 10.3). If you opened up the source code on your Web site you would see meta tags at the very beginning of the programming. These meta tags are the programmer’s way of helping the spiders decide what the Web site is about.

While spiders like the help from programmers, they don’t trust them. The meta tags are especially helpful to the spiders in making a decision about words on your Web site that many have multiple meanings. But the spiders know that some Web site developers are untrustworthy. The evil programmers (who are
probably part-time employees of the spam kings) sometimes put meta tags in the HTML programming that have nothing to do with the Web site’s actual content. The evil programmers just want you to waste your time looking at their bogus content. Because the spiders are good, they know that sometimes people do not want their Web sites to be crawled over. For instance, if you were running a game server, the spider’s interference might be perceived by the game as a really good player and crash your system. So the spiders recognize programming, or scripts, that tell them to go away.

After the spiders have completed their review of the Web site (they will be back constantly in case the content changes), they go back to the search engine owner and divulge all that they have learned. The search engine programs go to work and index the information so that you and I can search the Web and find what we want. Some of the methods for creating an index are rather complex. For instance, information is given different weights depending on its location in the Web site. For us, it’s just enough to know that the search engine programmers have designed a way for us to reliably search the Net.

There are three kinds of searches users commonly perform on the Internet. Probably the most common is a search using boolean logic. A Boolean search is named after the mathematician George Boole who lived from 1815 until 1864. His mathematical system of logic is not only used for our searches, but also one of the underlying principles of programming that enables mathematical computation by computers. Recall that computers use binary data—off and on. Boolean logic uses the off and on scheme to answer questions as true or false. If you have ever played twenty questions, you know that by answering true or false, or yes or no, you can determine an object. So, our Boolean logic search (by far the most common Internet search), uses Boolean operators like the word and to enhance our search capabilities. If at the search engine we type in the words cars and asteroids, we will only get a search return for Web sites that contain both words. There are six common Boolean operators:

• AND—all words joined by and must appear. For instance, “cars AND asteroids AND cats,” will reveal only Web sites that contain all three words.”

• OR—one of the words is in the Web site. For instance, “cars OR vehicles.”

• NOT—the word following not is not in the Web site. For instance, “cars AND asteroids NOT cats.”

• FOLLOWED BY—one of the words must follow the other. For instance, “cars FOLLOWED BY asteroids.”

• NEAR—the words must be within a certain distance from each other on the Web site. For instance, “cars NEAR asteroids.”

• QUOTATION MARKS—By placing the words in quotation marks, they are treated as a phrase and must be in that order. For instance, “car asteroids.”

Now we know a little bit about the Internet, Web sites, and searching the World Wide Web. The last technical issue we should look at before we start to see
When using most search engines, you can further refine a search by using the symbols + (plus) and − (minus). For instance, if you searched for “technology” you would get around 115,000,000 hits. However, if you added “+ television” (telling the search engine you wanted all Web pages with both the terms television and technology, your search is down to 57,600,000. Still a bunch. If you searched “technology − television,” your search is similarly limited.

how the Internet is being used by law enforcement is cookies. Cookies, like spam, are one of the current hot topics of the Internet. Moreover, cookies, like spiders can be both good and bad. The purpose of cookies is to allow what is called “retaining state information.” Let’s presume that you have set your browser to open at www.msn.com. You are using this as your home page so that you can access your e-mail, newsgroups, and chat rooms. In order for the Web site to recall how you personally configured (set up) this page, it gives your computer a cookie which has a serial number identifying the state of the page you want to retain. Without this cookie, you would have to repeatedly reset how you want the page configured. In essence, a cookie is a very small file that identifies you to the Web site. This cookie is not a program; it cannot do anything on its own. That is the good part—now the bad. Anyone with access to your computer can look at your cookies and see where you have been. You sort of leave a trail of cookie crumbs along the information highway. Moreover, some Internet companies, like Double Click, which provide Web advertising, retain your cookies because they want to develop a shopping profile of you. On your personal PC, you can go to Tools, Internet Options, Privacy and determine when and how you will allow cookies to be placed in your computer.

In addition to storing your personal preferences at certain Web sites, cookies also save information about which sites you visited, when you visited them, if you made a purchase, and any files that you downloaded. There is a second way in which personal information is collected on the Internet. We give it up. Any time we register or complete a commercial transaction on the Web, that information is retained by the firm who owns the Web site. Because Web sites can compile information from our cookies, transactions, and registrations, they can develop a fairly accurate picture of our personal likes and dislikes. Before we look at specific uses, we should take a look at an Internet use that is common to nearly every Internet user—e-mail.

Employee Use of E-mail and Instant Messaging

Electronic mail, or e-mail, is the Internet’s most widely used program. In fact, e-mail is so popular, it has surpassed the United States Postal Service in the number of messages delivered daily. When you send an e-mail, you are creating a file that will be transmitted to a recipient’s electronic mailbox. In addition to the text message, you can transfer files that contain other documents, photographs, and a myriad of other multimedia information.

A Look Ahead

Although legal, cookies and related consumer-tracking technology are forms of intrusion. It is increasingly simple for an individual or corporation to gather information about our Internet habits. In Chapter Sixteen (“Hi-Tech Crime”), we will look at illegal intrusion and some of the defensive methods and investigative techniques.

Source: Moore, Mass Communication Law, 438.
ware and software associated with scanners and printers, just about anything you could send via facsimile, you can send via e-mail.

Electronic mail is also far less expensive than either long-distance telephone calls or facsimile transmissions. Moreover, your e-mail address is portable. If someone wants to send you information, a document, or a photograph, with the telephone, facsimile machine, or regular mail, they have to know where you are going to be when you will receive it. With e-mail, you can send someone information, and they can access it from just about anywhere there is Internet service. There are security, privacy, and legal reasons you should use a communications method other than e-mail, but for most communications, e-mail is becoming the preferred choice.

While the security of e-mail is still a concern, encryption (for further reading on how encryption works, return to Chapter Four on networks) technology is increasingly allaying fears about messages being read by unauthorized persons. There are a variety of commercially available products and services that scramble messages between users. In most instances, all an end user has to remember in order to unscramble an encrypted message is a password or confidential phrase. These products guard e-mail against unauthorized intrusion during both transmission and storage. A second form of electronic communication is real-time conversations between people on the Internet using Internet relay chat (IRC). The Internet capabilities of e-mail and chat bring up interesting questions for employee–employer relationships. If you were at work and you placed a telephone call using your employer’s telephone, would you expect the telephone call to be monitored by an agent of your employer? Would you expect the telephone call to be recorded and potentially monitored from a database of employee telephone calls? What if you were on a break at work and reading a magazine—would you expect your employer to review what you had read? As we know from our earlier chapters on computer basics and networks, it is very possible for an employer to monitor, store, and retrieve e-mail, chat, and Internet activity.

One survey by the American Management Association indicated that 45 percent of firms monitor their employees’ e-mail, voice mail, or Internet use. As we know, hardware and software has become so sophisticated that an employer can monitor or record virtually every electronic word an employee utters. It is a fairly safe assumption that many state and local law enforcement agencies are following the lead of private industry and also monitoring their employees.

Essentially, there are two types of electronic monitoring. The first is interception. Interception occurs when the electronic communication is examined by the employer as it is occurring between the sender and receiver. With e-mail or chat, a copy of the message might be routed to a supervisor’s computer. With a voice communication, a supervisor might listen in on the conversation. The second type of monitoring is auditing. Auditing is primarily concerned with e-mail. However, in some instances, telephone conversations are also routinely recorded by an employer. For instance, as we learned in Chapter Seven, on communications dispatch centers, 9-1-1 calls are routinely recorded. Auditing occurs when the employer examines the message after it has been received, stored, or perhaps even deleted. While some employees have challenged their employer’s right to monitor their electronic communications, the courts have generally said that auditing was like the employer looking in a filing cabinet. The employer owns the filing cabinet, so he can look in it when he wants. The issue of monitoring is much more complex. However, if the employer has an electronic communications policy (like an e-mail policy that warns of potential monitoring) and the monitoring is done in a reasonable manner, the courts have generally upheld the employer’s right to monitor the communications.
Just as the Internet has brought us new ways to communicate, it has brought us new questions in the areas of employee-employer relationships and privacy. The Internet can cause questions about what is appropriate material for you to read or possess at work. The safest position is for employees to realize that the employer’s computer and Internet service is the property of the employer. It is nearly always subject to monitoring and auditing.

**Listservs and CrimeWeb**

A listserv, or a list server, is a program that automatically redistributes e-mail to names on a mailing list. Users can subscribe to a listserv by e-mail, or in some instances, there is a registration process. Once someone has subscribed, the listserv will automatically add her name and distribute future e-mail postings to every subscriber. The programs can be managed by a human being or a computer program. Commonly, people join listservs because they have some common interest with the other subscribers. One of the common hobbies that take advantage of listservs is genealogy. But there are law enforcement applications.

CrimeWeb (Figure 10.5) is a listserv that generates e-mail alerts to subscribers when a public safety agency makes notification of a missing child, missing adult, major crime, homeland security issue, school information alert, or community information alert. Any member of the public can go to their Web site and register. You enter the ZIP codes for which you are interested in alerts, and if a public safety agency posts an alert pertinent to your ZIP code, you receive an e-mail.

![CrimeWeb](image-url)
The Internet and Law Enforcement

In previous chapters we have seen how the Internet and Internet protocols have been used to supplement state and local law enforcement communication schemes. From this point forward, we are going to look at how law enforcement agencies have used Web sites on the Internet. The law enforcement–related Web sites listed in the text box on pages 214 and 215 provide information that gives you an idea of what other people are doing, and they can provide statistical and research information so that you can make better decisions or explore other aspects of law enforcement. Although the listing of law enforcement–related Web sites is by no means totally inclusive of what is available, it should be fairly representative. Furthermore, in order to completely understand the potential of the World Wide Web, it must be explored in a hands-on fashion. You will get a lot more out of navigating the Web than you will by reading my descriptions of the Web.

A comprehensive examination of the police function will reveal that there are many police and police-related functions that can be conducted via Web site, or supplemented by an agency’s Web site. Much of the research for this chapter was provided from examples of private firms exploring the commercial potential of the Web. That is because the success of some e-commerce firms has directly impacted the development of e-government. Many police departments are beginning to take cues from commercial firms that have been successful in e-commerce. The first job of a police department Web site is to get users to the Web site and attract them back again. Whether we like it or not, at first it is all about marketing. While it is unlikely that police department Web sites will attract new users to the Internet, they should be designed to attract those people in the community who are users. People visit a Web site because there is something at the Web site they want to see, know, or buy. Furthermore, in many instances, people visit a Web site because they were referred by another Web site.

At first, law enforcement Web sites resembled e-magazines. They were online publications that looked like newsletters or magazines. They sought to tell the reader what was unique about the particular police department that had published the Web site. Today many agencies still use the Web as a means to provide this type of one-way communication to the public. Those Web sites, which are probably the majority, are essentially static. While the information they contain might change on a fairly regular basis, they are static because they remain a one-way form of communication. One-way forms of communication with the public are trademarks of the professional policing model.

With one-way communications, the police are telling the public what they have done and what they are going to do. For community-based policing to be successful, the police must have two-way communications with the public. There must be an exchange of ideas about what is important to the community, and the community must be involved in solving the problems. Now, most police department Web sites have some form for feedback. Generally, there is a method to either submit an electronic feedback form or submit an e-mail to the police department’s Webmaster or perhaps to some police department employee designated to handle requests via e-mail. This is certainly a step toward two-way communication.

Recall from Chapter One that in the community-oriented policing model, technology is an enhancer. We have certainly seen that technology has enhanced traditional police functions. There are numerous examples of technology increasing police efficiency, and in later chapters we will see how technology has increased the effectiveness in traditional roles. The question remains, how can the technology of the World Wide Web enhance community-oriented policing? The

E-commerce is the completion of a commercial transaction via the World Wide Web. Essentially, a business sells something that you buy via the Internet. Source: Cunningham, B2B, 176.
It is likely that you will gain more from this chapter by actually exploring law enforcement on the Internet. The following nine Web sites are a collection of government, not-for-profit, and commercial firms that provide law enforcement-related information. While most of the Web sites listed below contain information that is available to anyone with Internet access, some sites, like the Federal Bureau of Investigation, maintain portions of their Web sites that can be accessed only by law enforcement personnel. As we saw in Chapter Nine, on external sources of information, there is information available via the Internet that law enforcement personnel can access with the proper passwords and secure linkages.

- **The Source Book of Criminal Justice Statistics**
  [www.albany.edu/sourcebook/index.html](http://www.albany.edu/sourcebook/index.html)
  This site annually compiles criminal justice statistics from more than one hundred sources. The information is presented in more than six hundred tables. The information is searchable and available for review and downloads in Adobe Acrobat format.

- **National Criminal Justice Reference Service (NCJRS)**
  [www.ncjrs.org/](http://www.ncjrs.org/)
  This Web site searches the NCJRS Web site and the Web sites of the U.S. Department of Justice, Office of Justice Programs (OJP) (OJP includes five separate bureaus: the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Bureau of Justice Statistics, the Bureau of Justice Assistance, and the Office for Victims of Crime), and the White House Office of National Drug Control Policy. Additionally, this Web site has the capacity to search the NCJRS Abstract Database, which contains more than 160 thousand criminal justice publications. There are a large variety of text documents available in both a plain text format and Adobe Acrobat format.

- **United States Department of Justice, Community-Oriented Policing Services (COPS)**
  [www.cops.usdoj.gov/](http://www.cops.usdoj.gov/)
  This Web site provides a good overview of community-oriented policing and funding opportunities, and it publishes problem-solving guides for police agencies. There are currently nineteen problem-solving guides that offer information and advice on subjects ranging from rave parties to the use and abuse of 9-1-1.

- **The Federal Bureau of Investigation**
  [www.fbi.gov/](http://www.fbi.gov/)
  The FBI Web site offers a reference library on a variety of police subjects. There are also links to a variety of programs the FBI is conducting in conjunction with state and local law enforcement agencies.

- **The Bureau of Justice Statistics**
  [www.ojp.usdoj.gov/bjs/](http://www.ojp.usdoj.gov/bjs/)
  The BJS is responsible for the collection, retention, analysis, and dissemination of statistics related to criminal justice. It is an outstanding source for statistical information. Many of the links from other Web sites on statistics actually take you to the BJS.

- **National Institute for Justice**
  [www.ojp.usdoj.gov/nij/](http://www.ojp.usdoj.gov/nij/)
  The NIJ is the research, development, and evaluation agency of the United States Department of Justice. It was created in 1994 as a component of the NIJ’s Office of Science and Technology, the National Law Enforcement and Corrections Technology Center (NLECTC). The NIJ serves as the “honest broker” offering support, research findings, and technological expertise for state and local law enforcement and corrections personnel. The NIJ includes regional centers around the United States that are available to assist criminal justice personnel with technology problems. Moreover, the NIJ sponsors research and development when it otherwise will not occur.*

- **International Association of Chiefs of Police (IACP)—Technology Clearinghouse**
  [www.iacptechology.org/](http://www.iacptechology.org/)
  The IACP link will take you to their Technology Clearinghouse. It has a wide variety of resources available, including a searchable library.

---

*“Evolution and Development of Police Technology,” vii.*
an archive of “Tech Talk” articles that appeared in past issues in their magazine, and links to police technology practitioners.

- The Terrorism Research Center  
  **www.terrorism.com**  
The Terrorism Research Center (TRC) conducts research into terrorism and terrorism-related subjects. In addition to analysis of terrorism trends and counter-terrorism efforts, the TRC, through its Web site, offers information on information warfare and infrastructure protection. It includes a searchable knowledge database on articles, policy analysis, and reference materials.

- The Society of Police Futurists International (PFI)  
  **www.policefuturists.org/index.htm**  
The Society of Police Futurists International (PFI) is an organization of law enforcement practitioners, educators, researchers, private security specialists, technology experts, and other professionals dedicated to improving criminal and social justice through the professionalization of policing. Futures research (long-range planning and forecasting) is the pivotal discipline that constitutes the philosophical underpinnings of PFI. The tools and techniques of this field are applied in order to more accurately anticipate and prepare for the evolution of law enforcement ten, twenty, and even fifty years into the future. Futures research offers both philosophical and methodological tools to analyze, forecast, and plan in ways rarely seen in policing in the past. The strength of PFI lies in the participation of its members as we engage in dialogue and collaborate on research on the future of the policing profession.

The answer is fairly straightforward—a police department’s Web site should be designed to attract users and increase the two-way communications between the community user and the police.

One move in the direction of creating two-way communication and partnerships might be in community participation in Web site design. Consider that a static Web site is fairly simple and not very expensive. Hosting services for a 350 MB site that includes fifty e-mail addresses is less than $60 a month. Moreover, fairly comprehensive Web development software costs less than $200. The primary stumbling block is development and content.

Even a static Web site can be made more attractive by constantly updating and changing the content. The question for the manager of the agency is, where do we find the talent necessary for site development and management? A Web site can become a technological enhancer for community policing if the community is involved in the development of the site. Even with differing community values and standards, there is little direct community input into the day-to-day operations of a local police agency. Police agencies are restrained and directed in what they can do and what they must do by the Constitution, federal law, state law, case law, etc. In other words, any time a police agency has the opportunity to solicit community input and involvement in decision making, it is a special occasion. A Web site gives an agency that opportunity. A Web site can foster community participation and input if the community is given a strong hand in site development and content. What do they want on their Web site? How should their Web site look?

Following the lead of e-commerce, how can police agencies increase Web traffic? I have not referred you to police department Web sites that are static and dull; you can find those on your own. The point is that you were unlikely to have visited those Web sites without a referral, one of the most basic things a police department can do to increase Web traffic. Referrals come from links with other agency’s Web sites, or e-partnerships (Figure 10.6).

One of the tenets of community-oriented policing is partnership with the community. This is not just partnership with individual community members.
Figure 10.6 In Chapter Eleven, when we look at information exchange, we will explore the value of regional systems. One regional system is the Automated Regional Justice Information System (ARJIS) in the San Diego area of California. Regional information systems not only increase the technological efficiency and effectiveness of the participating agencies by reaping the benefits of economies of scale, but the combined agency resources have the capacity to increase the use of technology for information exchange with the public. The San Diego Police Department, in conjunction with ARJIS, has produced a very interactive Web site (www.sannet.gov/police/). Through the Web site, the community can view interactive crime, traffic, and sexual offender maps; they can obtain information about the San Diego Police Department and other service organizations; and they can submit crime clues and other information online. Go to www.sannet.gov/police/prevention/index.shtml. You will find that the San Diego Police Department provide hyperlinks to a variety of community resources, broken down by police beats. Permission to reprint provided by the San Diego Police Department.

This is also partnership with other community service organizations. We know that community-oriented policing is about solving problems, and we know, primarily from experience, that the police cannot solve most community problems. Yet as one of the most visible members of the service community, the police are often called upon to solve problems far outside their area of expertise. If you want a test of whether or not a police department is practicing community policing, you need only ask a few basic questions about the operation of that department. Does that police department recognize that many of the root causes of crime, fear, and disorder are outside their area of expertise? Does that police department work to solve those problems by seeking partnerships with the people and organizations who have the expertise to address the root causes? If you can answer yes to both questions, some level of community-oriented policing is occurring.
Many of the organizations that police departments work with to solve problems have their own Web sites. Creating Web linkages with agencies a police department works with to solve problems is a means of strengthening those partnerships and increasing Web traffic. This can be as simple as modifying the way in which police departments post press releases on their Web sites. Instead of a static press release that tells the public what happened, the press releases should be dynamic and have links to the participating agencies. Conversely, when those agencies post their version of the press release, they should have a link to the police department Web site. Both agencies benefit by having their particular audience jump back and forth between the Web sites.

These types of linkages are very common in e-commerce. Commercial firms whose products are complementary but not competitive often link among each other in an effort to increase market share. That is the essence of partnership; we are complementary and not competitive. While most police service is not a commercial transaction, individual commercial transactions are conducted between the police and some community members.

Generally, police service is a public good that we all pay for in advance through taxes; whether or not we use it, we pay for it. However, there are some transactions for which the police are going to charge a fee to an individual. For instance, let’s say that you are unfortunate enough to have your cellular telephone stolen out of your parked car, but you were smart enough to purchase loss insurance when you obtained the telephone. However, the insurance carrier wants a copy of the police report in order to process your claim. Your local police department is probably going to charge you a fee for a copy of the completed report (Figure 10.7).
Term Definition:
E-commerce is a term generally associated with commercial enterprises. Simply put, it is the act of buying or selling goods electronically, primarily over the Internet. However, as the presence of public organizations expands on the Internet, e-commerce, or e-government, is the process of conducting transactions between the public and the government, over the Internet. A developing concept is m-commerce, which is the ability to purchase goods and services anytime and anywhere through a wireless Internet-enabled device. Source: Clarke, “Emerging Value,” 133.

Presume that in addition to being savvy with your cellular telephone, you are an Internet wizard. You have learned to purchase all kinds of merchandise via the Internet. So would you rather go to the police station, stand in line, and pay for the report that they will mail to you in seven to ten days, or would you rather go online, pay for the report, and have it mailed to you in three to five days. This is exactly what is happening in many police departments across the nation. They are beginning to use e-commerce to facilitate commercial transactions with individuals. For the Omaha Police Department, e-commerce is becoming more significant as a business-to-business transaction, especially in the realm of traffic collision reports, which are used primarily by automobile insurance companies.

There are several benefits to government-based e-commerce. First, it gets the user to the Web site. That user is likely to look at other services available at the Web site. E-commerce increases Web traffic. Second, e-commerce improves public satisfaction. If the transaction is not quick and simple, there will be no users. If there are users, they are likely to be satisfied because the service was quick and simple. Moreover, think about your perceptions of the police department. If you order the report online, your expectations are fulfilled. However, if you go to the station and stand in line with the collection of people who find themselves in the lobby of a police station and you have to deal with a desk officer or clerk who is handling the telephones and all of the people in the lobby, no matter how efficient that person at the desk is, it is very likely that your perceptions of the experience are going to be less favorable than had you ordered online.52

Figure 10.8 A frequently asked questions (FAQ) page is a good way for new and returning users to look at questions that are regularly asked. Source: Cunningham, B2B, 176.
Permission to reprint provided by the Arlington County Police Department.
In addition to improving your experience with the police department, e-commerce has the advantage of allowing the police department to more effectively use their personnel’s time. Police departments, like all organizations, experience peak staffing times. No matter how much a police manager tries to deploy personnel in order to even out the workload, there are always going to be unexpected peaks, employee absences, and unexpected lulls. Some agencies fill the lulls by having employees complete e-commerce transactions during lulls in the workload.\footnote{In 2003, the Omaha Police Department began posting their weekly crime reports to the Web.}

Let’s stop for a moment and consider a question about efficiency and e-government. One study on e-government looked at the annual purchases of federal, state, and local governments. It found that our government purchases goods and services totaling $568 billion annually. Now private industry has found that by putting services online, it can cut costs by as much as 20 to 25 percent. Well, if we use the business model, it looks like our government could save more than a hundred billion dollars a year by going online.\footnote{Source: A study by the University of Chicago Business School and Chicago Booth School of Business.}

Sounds like we ought to wire up the government now, right? Well, maybe not. Strict comparisons between business models and government often lead to serious disappointment. First, the government is responsible for doing things that are by their very nature inefficient. If there were an efficient way to provide a service that people would pay for, a private firm would probably do it. Second, the more complex e-government becomes, the more people and resources (read as money) are going to be needed to support the operation. So there might be some gain in efficiency by going online (as with the Omaha Police Department reports), but we must carefully examine the resources that were shifted away from one area to support e-government. We might find that there was little or no gain in how we spent the public money. Finally, shifting money to support online resources creates questions of equity (at the end of the chapter, one of the discussion questions is designed to help you consider the issue of equity).

It is probably fairly clear to you that the main problem with Web sites is the development and maintenance of content. Content is what the Web site says or does. The actual programming, structure, and issues related to hosting are relatively simple when compared with the problems associated with the content. Many law enforcement agencies underestimate the cost of content, especially the need to change content.\footnote{In 2004, the San Diego Police Department spent over $1 million on a new Web site, only to have it be outdated by the time it was completed.}

If it is not interesting or useful, people are not going to come back.

Between links (partnerships) and e-commerce, a police department can probably significantly increase the traffic to their Web site. Now the task is to increase the

\begin{center}
\textbf{A Look Ahead}
\end{center}

In Chapter Twenty (“Implementing and Managing Technology”) we are going to examine some of the difficulties in planning, implementing, and managing a technology project like a Web site. One common, recurring theme in all law enforcement technology is how well-trained personnel are often lost to the private sector. For instance, if a police agency develops in-house talent for the construction and maintenance of their Web site, they can find themselves in the position of losing good people. A stellar Web site means the agency has a stellar developer or Webmaster, and the better someone is, the greater the lure of private industry. Of course when someone leaves an agency, the agency can find itself in the position of no one knowing how to update their Web site.

Go to the National Law Enforcement and Corrections Technology Center (NLECTC), Justice Technology Information Network (JUSTNET) at www.nlectc.org/justnet.html and subscribe to their weekly News Summary. It is a service for criminal justice practitioners that provides weekly abstracts of articles from major national newspapers, business magazines, Web sites, national and international wire services, and other periodicals focusing on law enforcement and corrections technology. The summary is delivered to your e-mail address. You will find the link to subscribe at the bottom right-hand corner of the Web page.

Try This

A portal literally means a gateway into something. Portals started out as search engines. They grew from an index to a center that could provide information on a variety of related subjects. For e-government, a portal is a gateway to all of the services offered by the particular jurisdiction. 


number of times that users return to the Web site. There are a number of ways to increase return visits. The most obvious is to develop a dynamic and well-thought-out Web site. Additionally, people return to a Web site when they are reminded that there is something useful for them to view at the site. Again, taking a cue from commercial e-commerce, police departments are developing the means to alert users when new and useful information has been posted to the Web site. Many organizations are taking advantage of the listserv concept much like CrimeWeb. As we saw with CrimeWeb, the e-mail notification could take on a variety of forms. It could be an actual newsletter or news digest of some sort, or it could an e-mail that provides you with a link to the Web page with new information.

In addition to e-mail notifications or alerts, Web traffic is increased when the information available at the Web site is likely to change frequently. The more real time the information, the more frequently users are likely to access the information (Figure 10.8). If you return to the San Diego Police Department Web site, you will see that they post nearly real-time crime information (taken from the type of relational database we discussed in Chapters Two, Seven, Eight, and Nine). Moreover, the maps are interactive and the view and data can be changed depending on the user’s needs.

E-government

Police agencies are not the only government entities that can benefit from Web sites; the term e-government is inclusive of all services. Some political jurisdictions, particularly the larger ones, are using the parent jurisdiction Web site (the municipality is the parent of the police department, the county might be the parent to the sheriff’s department, and so on) as a portal to all government services.

The portal concept is gaining ground at the federal level where there are reported to be more than twelve hundred different e-government projects in progress.\footnote{56} We will probably find that as e-government matures, technology is going to force us to reorganize our government structure to meet demands. Linkages within portals should allow the community one-stop access to government services. As we know, many community problems cannot be solved by the police themselves. The portal concept relies on hyperlinks to other resources and other organization’s resources in a manner that complements the problem solving process. For instance, Web-based mapping like the type you can view at the San Diego Police Department site supports a wide variety of applications, such as resource management, crime prevention, urban planning, education, and community participation.\footnote{57} However, this is going to require redesigning service delivery and significant coordination. Just getting different departments within a jurisdiction
As technologies mature and begin to converge, the challenges and opportunities for creative law enforcement increase. For instance, one of the emerging business models concerns the convergence of cellular and Internet technologies. In the private sector, this convergence is providing customers alert notifications to business transactions such as auctions and stock price changes. We are not very far from the day when the CrimeWeb concept could be combined with cellular technology. In the business model, the combination of the Internet-based CrimeWeb service and cellular technology is thought of as location-based marketing. Note that subscribers to CrimeWeb identify the alerts they are interested in by ZIP code. Recall from Chapter Three, one of the defining features of cellular telephone service is the network's ability to keep track of the cellular telephone and hand off service among cell sites. A true convergence of the CrimeWeb technology and cellular technology would entail the subscribers getting notifications based upon which cell site they were currently using.

Source: Clarke, “Emerging Value,” 133.

to share the same standards and systems so that everything fits together and offers users the same look and feel is a huge task.\(^58\)

So far we have seen how law enforcement agencies can use the Internet to increase two-way communications with the community, form and strengthen partnerships, and facilitate problem solving. The Internet also has the capability to facilitate situational crime prevention. Recall that situational crime prevention can be defined as reducing the opportunities for a criminal offender. If we can make it more difficult to commit a crime, thereby increasing the effort an offender must expend, crime may be prevented. Typically, we think of this as ‘hardening the target.’\(^59\) By using the listserv concept; providing crime prevention information on their Web site; and through nearly real-time, interactive mapping, police agencies can provide the community with information necessary to protect themselves.

Chapter Summary

We have seen that in the beginning the Internet was a big idea that actually started out relatively small. From government efforts to improve communications between defense contractors, employees, and researchers, the idea of a global communications network grew. The two key ideas that finally launched the Internet were determining standard protocols that allowed different networks to communicate and the concept of sending information in data packets. From the Internet, the World Wide Web evolved as people used hyperlinks to create connections to information they determined was consistent and complementary to their information. Essentially, the information highway (the Internet) enabled the creativity that has become the World Wide Web.

The technology of the Internet and the creativity of the World Wide Web spawned the explosion of commercialization. As e-commerce became possible and profitable, government organizations began to look for ways to use the Internet as a means of providing information, communication, and individual transactions. Somewhat slowly, e-government is learning from e-commerce that the power of the Internet is to deliver the content to the community that the community wants. For law enforcement agencies, the content the community wants is Web sites that enhance the community-oriented policing model—two-way communications, partnerships, and problem solving.

As we have seen, a static Web site resembles the professional model of policing in that it is primarily a one-way form of communication. Therefore, law enforcement agencies are increasingly turning to the use of dynamic Web applications...
that allow them to increase two-way communications, partnerships, and problem solving. Some of these applications are:

- Multimedia applications that enhance text, graphics, audio, and video.
- Relational databases that allow nearly real-time information in the form of text, tables, and maps.
- Multiple means of communications including listserv capabilities, feedback forms, and e-mail to specific officers.
- Hyperlinks to other service organizations and resources.

Although the Web can enhance an agency’s community policing efforts, there are challenges. With a finite budget, police executives must make tough decisions about where to spend public money. Dynamic Web sites can be costly to develop and maintain. The shifting of public funds to Web sites brings tough questions about efficiency and equity. The money comes from somewhere. Does it create more public value when it is applied to Web development and maintenance?

In the next chapter, when we look at information exchange, we will build on our knowledge of the previous chapters while looking at some of the problems associated with information exchange in a fragmented environment. We will explore some of the consequences of the inability to communicate on a tactical level and the inability to exchange information about offenders.

Discussion Questions

1. A 1999 study by the National Telecommunications and Information Administration (NTIA) found that a rural, low-income household has a less than one in thirty chance of having Internet access in the home.60 Because law enforcement agencies have limited budgets, when funds are used to develop a Web site, they can reduce funding to other areas of the department or the parent agency. Because the people who arguably need police services the most have less access to e-police services, do law enforcement agencies unintentionally create service inequities? If so, what do you think a law enforcement agency, or the parent organization, should do to minimize the inequity?

2. It is estimated that the number of people who have Internet access via a mobile communications device, such as a cellular telephone, increased more than 700 percent between 1999 and 2003 (from 7.4 million to 61.5 million).61 Traditionally, most law enforcement Web sites have targeted the citizens who live in their jurisdiction and have Internet access. Given that mobile Internet users may just be passing through a jurisdiction, are there content or configuration changes law enforcement agencies should consider in order to capitalize on the number of people with mobile Internet access?

3. Surf the Web and find several state and local law enforcement agencies’ Web sites. There are some common questions we ask about Web sites in an effort to determine what, if any, standards the organization developed.62
   A. Is the site accessible? What meta tags did they use? Are they linked to other organizations?
   B. Is the site easy to use?
   C. Is the site well maintained; do there appear to be constant updates?
   D. Is it interactive?
   E. Is the presentation attractive and effective?
   F. Does it have any e-commerce attributes?
4. If you were building a law enforcement Web site, what would you include and why?

**Key Terms**

<table>
<thead>
<tr>
<th>Access Service Provider (ASP)</th>
<th>Hypertext Transfer Protocol</th>
<th>Meta Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing</td>
<td>Index Page</td>
<td>POP (Point of Presence)</td>
</tr>
<tr>
<td>Boolean Logic</td>
<td>Interception</td>
<td>Portal</td>
</tr>
<tr>
<td>Browsers</td>
<td>Internet</td>
<td>Search Engines</td>
</tr>
<tr>
<td>Cookies</td>
<td>Internet Protocol (IP)</td>
<td>Spam</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Internet Relay Chat (IRC)</td>
<td>Spiders</td>
</tr>
<tr>
<td>E-commerce</td>
<td>Internet Service Provider (ISP)</td>
<td>Tags</td>
</tr>
<tr>
<td>E-government</td>
<td>Listserv</td>
<td>Webmaster</td>
</tr>
<tr>
<td>Home Page</td>
<td>M-commerce</td>
<td>World Wide Web</td>
</tr>
</tbody>
</table>

**End Notes**

2. Ibid., 100.
4. Ibid.
5. On July 27, 2003, the Search Engine Google reported that it was searching 3,083,324,652 Web pages.
7. The Internet Society (ISOC) is an organization composed of private individuals, government agencies, commercial companies, and foundations that are a primary force in the past and current development of the Internet. The members of the society also comprise several other organizations such as the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). For a view on the development of the Internet from people who were involved in its creation, a look at current standards, and a glimpse of the future, visit their Web site at [www.isoc.org/](http://www.isoc.org/).
9. Ibid., 7.
10. Ibid., 178.
11. Ibid., 174.
12. Ibid., 185.
15. Ibid.
19. Ibid., 185.
20. Ibid., 178.
21. Ibid., 181.
22. Ibid., 171.
23. Ibid., 172.
24. Ibid., 172.
25. Ibid., 175.
26. Ibid., 178.
27. Ibid., 184.
28. Ibid., 178.
29. Ibid., 177.
30. Ibid., 177.
31. See note 14 above.
33. See note 14 above.
35. Ibid., 182–183.
39. See note 17 above.
42. See note 17 above.
44. Watson, “Private Workplace,” 79.
45. Spykerman, “E-mail Monitoring.”
46. See note 44 above.
47. Cunningham, B2B, 179.
48. Cisar, “Police Department Website.”
50. Ibid.
51. Ibid., 141.
52. See note 48 above.
53. Ibid.
56. See note 6 above.
57. See note 14 above.
58. See note 54 above.
62. See note 6 above.