CHAPTER 19

bercrime generally falls into three categories:

- Cases in which technology is integral to commission of a crime (electronic fraud, money laundering, child pornography).
- Cases in which the technology is used to commit a crime (identity theft, computer sabotage, theft of privileged information).
- Cases in which technology is used as an incidental aspect of a crime (data and image storage, Internet and cellular communication).[1]

e investigator should be familiar with the more common types of crime ng information technology. The National Institute of Justice's *Electronic me Scene Investigation: A Guide for First Responders* is an important publica- n that should be of interest to all investigators.[2] Some of the material for s chapter was culled from this NIJ guide, as well as other publications. See x 19.1.

X 19.1 COMMON TYPES OF CYBERCRIME

- Child pornography and exploitation
- Economic related fraud
- Electronic stalking and harassment (cyberstalking)
- Extortion
- Gambling
- Identity theft
- Illegal drug activity
- Intellectual property crimes
- Mail and wire fraud
- Money laundering
- Prostitution
- Software theft
- Telecommunications fraud
- Terrorism
- Transporting stolen property
- Data theft
- Electronic sabotage
- Ransomware
- Phishing

t is virtually impossible to determine the monetary amounts of various types of IT crime, but costs and losses easily run into billions of dollars and may have

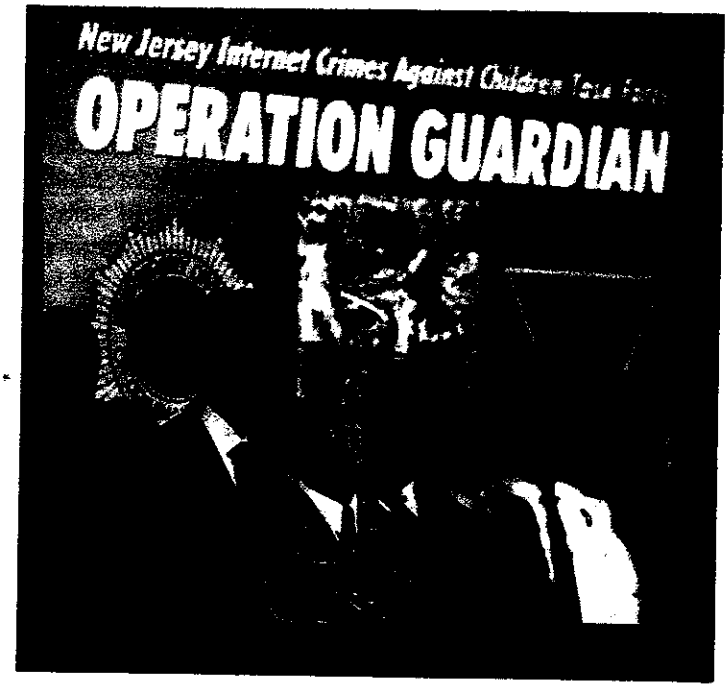

FIGURE 19.1
A news conference is held in New Jersey following arrests of a high school hockey coach, a pediatric neurosurgeon, and 37 others on child pornography charges in a sting that authorities said was assisted by new computer technology used by state police detectives.

Source: AP Photo/ Tim Larsen

tes, devoted to fostering ideological positions, racism, ethnic hate, and dissatfaction with the government. Free speech rights protect these sites, and many f them draw a fine line between what is legal and what is illegal. The fact that n individual visits a web site is not a crime, and an investigator must take care a how such information is used. In cases involving pedophiles, the fact that hey subscribed to or visited web sites may serve as circumstantial evidence hen a sex crime is involved.

A number of federal agencies monitor the web sites of suspected violent roups, largely as a means of keeping track of potential criminal activity. owever, it should be noted that care must be taken in attempting to develop ses based on information from a site. Web sites also serve as one of the larst libraries in the world, providing information about people, places, and ings. Many web sites may also be targets for hackers trying to disrupt an rganization.

NVESTIGATING HIGH-TECH AND IT CRIME

thorough discussion of investigative methods involving high-tech crime beyond the scope of this chapter, but it is important to have a basic nderstanding of the type of crimes that an investigator may come across. ecause computers have become so common in everyday life, it is important

be called. One should not turn the computer off or on or ask the suspect to assist unless an expert is present.

Most experts agree that training and education of investigators must increasingly include a basic knowledge of computers and how they can be used in criminal activities. In many cases, the investigator will have to rely on the victim to explain how a crime was carried out, and what damages may be attributed to the offender. The investigator, frequently in cooperation with legal counsel, will be faced with determining what crime took place and the legal standards and jurisdiction that are involved.

Of the crimes that are predominantly carried out using various forms of technology, child pornography and exploitation, electronic and economic fraud, identity theft, and gambling are quite common. The following illustrations and case studies provide an overview of the more common methods employed.

The Internet has become a notorious tool for pedophiles, child pornographers, and other child sex abusers. ICE, the Postal Inspection Service, and the FBI generally investigate international providers. Depending on how information comes to authorities, federal, state, and local law enforcement may handle local investigations of users. Users of child pornography may also be pedophiles who are active in recruiting children for photos or using chat rooms to entice children to meet them.

A growing number of states have expanded or initiated child exploitation units, which usually include a computer specialist who is familiar with the methods used by suspects who make contact with young people through chat rooms as a means of luring victims to a prearranged location. When a parent or other person makes a complaint, the investigator should be thoroughly familiar with local laws relating to solicitation of a minor. Generally, it must be proved that the suspect was aware that the individual was a minor and, in most cases, it will be necessary to prove that something more than a meeting was planned. For this reason, it is important to obtain prior communications. If a meeting is arranged, it must be proved that the suspect was actually going to make contact and that a positive identification of the suspect has been made. See Figure 19.2.

Economic Crimes—Fraud, Embezzlement, and Identity Theft

There are a great many types of economic-related fraud, including business fraud and embezzlement, perhaps the largest of which was the Enron case in Texas, which involved a broad range of criminal activities. A major component of this scheme involved computer usage for money transfers and communications. The sale of products that are not delivered as well as misrepresentation of sellers has become a growing problem, and investigations may involve multiple jurisdictions and countries.

Keeping transactions within the computer allows the suspect to destroy information rapidly. However, in many cases, transactions may have been sent to one or more other computers or organizations with which the suspect is

Courtesy, Peter Massey, Department of Forensic Sciences, University of New Haven

FIGURE 19.2
This photo illustrates the type of crime scene that may be encountered in cybercrime investigations. Note clues, such as the eyeglasses and the business card in the ashtray. This type of investigation will usually necessitate a computer expert.

conducting business. Further, with the development of small storage devi that can hold enormous amounts of data, as well as cloud computing, it w be increasingly common for criminals to maintain suspect records separ from the computer.

One of the more common types of electronic fraud involves the use stolen or forged credit cards. Despite efforts by companies to create "safe credit cards using photos and fingerprints, this problem continues to gr due in some measure to the ability to purchase products and services o the Internet. Identity theft is one of the fastest-growing crimes in the Uni States. Criminals use a variety of means to secure information. They then this information to commit fraudulent purchases, acquire other forms of fa identification, receive large cash advances, and establish fraudulent lines credit in the forms of loans and other credit cards.

A number of schemes involving telecommunications fraud have arisen w the increase in the number of cell phones available throughout the wor Each type of telecommunications offering, from voice to wireless data, is v nerable. For instance, through fraudulent access to networks, perpetrators c avoid paying for wireless service, steal and resell long-distance minutes, hija a network device to send unsolicited commercial e-mail or pornographic spa to unsuspecting end users, or use stolen cell phones to make large numbe of calls.

Additionally, a number of organized crime groups, frequently with inte national connections, have developed sophisticated fraudulent credit ca rings. Investigations of these types of activities must be handled quick because perpetrators are likely to move frequently to avoid apprehensio

nfortunately, in many cases, the victim whose number or card has been olen is not aware of the crime until he or she receives a statement.

On a higher level, fraudulent wire transfers, bank fraud, telecommunications aud, and money laundering have also become commonplace. In many stances, the illegal activities are carried out across borders and will involve ultiple jurisdictions. Electronic funds' transfers have made it possible for dividuals to move funds to offshore accounts, to gain entry illegally into nding institutions and make transfers, and to embezzle large amounts of oney. Section 2314 of Title 18 of the U.S. Code makes it illegal to transrt interstate computer data[18] and stolen computer hardware worth at least 5,000.[19]

Economic espionage has also become a major problem. Although relatively le attention is paid by law enforcement to the issue of economic espionage, tent or intellectual property infringement, or the stealing of trade secrets, this an area in which the amount of criminal activity has been growing steadily. many cases, the companies being victimized are unaware of the problem or not have procedures for reporting or investigating such activities. Estimates annual misappropriations and fraud (frequently committed by trusted ployees) of U.S. companies amount to more than $250 billion. Although tutes differ by states, the elements of computer fraud make it unlawful for y person to:

- use a computer or computer network,
- without authority, and
- with the intent to: (a) obtain property or services by false pretenses; (b) embezzle or commit larceny; or (c) convert the property of another.[20]

mputer Hacking/Cracking and Sabotage

e of the more pervasive illegal uses of the computer is hacking, more corly cracking, which generally involves entering a computer system illegally ithout knowledge of the victim. The term *hacker* generally refers to individwhose goal is to reduce their lines of code without inhibiting the program perate optimally (see Box 19.6). The term *cracker*, on the other hand, is l more often to describe a person who attempts to destroy, change, or programs or information. Often undertaken as what hackers refer to as intellectual challenge," the practice has become a major problem in both ublic and private sectors. A growing number of individuals and "clubs" ghout the world have been involved in developing methods to break s or find ways to enter a system, and they have frequently been successful crashing" web sites, altering information, and introducing viruses. In net slang, the term "white hat" refers to nonmalicious, ethical hackers, ding those who perform penetration tests and vulnerability assessments. lack hat" hacker is a hacker who violates computer security for malicious ons or personal gain.

CYBERCRIME INVESTIGATION AND THE ELECTRONIC CRIME SCENE

There are several considerations that should be observed when dealing with a high-tech crime scene. The National Institute of Justice (NIJ) Guide stresses the importance of documentation in detail. The following steps are recommended:

- Observe and document the physical scene, such as the position of the mouse and the location of components relative to each other (e.g., a mouse on the left side of the computer may indicate a left-handed user).
- Document the condition and location of the computer system, including power status of the computer (on, off, or in sleep mode). Most computers have status lights that indicate the computer is on. Likewise, if fan noise is heard, the system is probably on. Furthermore, if the computer system is warm, that may also indicate that it is on or was recently turned off.
- Identify and document related electronic components that will not be collected.
- Photograph the entire scene to create a visual record as noted by the first responder. The complete room should be recorded with 360 degrees of coverage, when possible.
- Photograph the front of the computer as well as the monitor screen and other components. Also take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity.[22]

The computer has come of age in law enforcement as departments and other agencies develop applications through which this technology can benefit the field. In many cases, the technology and the application software—the programs used to handle and manipulate the data—exist in various forms but require modification for law enforcement purposes. In other cases, software is available (frequently through hardware vendors) that has been designed specifically for police work. Included in this category are programs ranging from relatively simple data-storage programs to extremely complex systems for tasks such as imaging (for storing photographic images on the computer) and optical scanning (for storing fingerprints for later retrieval).

In the field of criminal investigation, the computer has not yet come close to the potential it offers as an investigative tool. Although one reason for this is a lack of sufficient funding, other considerations also limit computer utilization—for example, concern about the right to privacy, a lack of trained technicians, and an entrenched resistance by officers who have little understanding of the computer's capabilities.

As new generations of computer-literate personnel move into the law enforcement profession, there is likely to be a growing trend toward acceptance. Many federal agencies have begun to develop and adopt computer-based systems that go far beyond mere data storage and retrieval. A number of police departments—including those in Chicago, Los Angeles, and Houston—have invested millions

of dollars in Automated Fingerprint Identification Systems (AFISs) and seeing their value in the investigative function. Illustrative of this potential va is a case involving a forcible rape in which a latent fingerprint was lifted fr the handbag of the victim. Fingerprint analysis provided no suspects. Howe more than a year later, a suspect arrested in a burglary was surprised to le that, despite the passage of time, his prints identified him as the rapist. (At time of the rape, he had been too young to be fingerprinted, despite his l record as a juvenile offender.) This illustrates the capability of technology solve what in all likelihood would have remained an unsolved case.

Computers are also being used for developing crime patterns; for artifici intelligence, and, with imaging, for storing online mug shots of suspects a photographs of stolen artwork or other valuable collections.

Perhaps the greatest innovation in programming software in the past fe decades has been the development of very sophisticated relational databas and linking and geospatial programs for law enforcement purposes. A re tional database combines a large number of individual databases into a syste that makes it possible to link a broad range of disparate variables for search a profiling purposes. The Chicago Police Department's CLEAR program mak it possible to link millions of records from different sources (including oth police departments) to provide a powerful tool for investigators. The progra utilizes artificial intelligence, photographs, images, and geospatial techniqu in addition to text-based records. Some of these include:

- Nickname database
- MO file
- Informants file
- Business locator index with emergency telephone numbers f business owners
- Case file indicating which cases are assigned to which investigator
- Skills index listing the names of those who can assist with specific need such as language skills, scuba divers, technicians, etc.
- Intelligence file offering a source for various bits of information that ca be pieced together to form a clearer picture of suspects or crime pattern (This file, which usually requires the expertise of an analyst or other ind vidual familiar with the technology, represents one of the more significa changes appearing in the field of criminal investigation.)
- Stolen property files
- Building layouts and schematics
- Tattoo files
- Gang symbols and descriptors
- Motor vehicle records
- Victimization files

The FBI utilizes Rapid Start Teams, which are teams of experienced investigato and technical experts who can quickly load information from hundreds o

leads and investigative tips into a database to assist in major case investigations. Established in 1995, the Rapid Start Team has assisted in numerous high-profile cases, including the Oklahoma City Bombing in 1995, the Atlanta Olympics Bombing in 1996, and the 9/11 attacks in 2001. Rapid Start Teams are also available for child abduction cases and other major cases.

On an individual basis, investigators can use PCs, laptops, PDAs, and other devices to maintain their own data sources, address and telephone files, case information, as well as for numerous other applications.

If a picture is worth a thousand words, imaging technology offers immense possibilities. One of the most obvious uses today is through computer-based identification kits, which make it possible to prepare a composite of a suspect relatively easily. However, the quality and color of newer monitors and systems make it possible to have a four-color, instant-access mug shot book readily available. Indeed, coupled with search technology, the investigators can feed in information on *modus operandi*, physical descriptors, type of victim, and so on, to call up groups and individuals in various categories for the victim to view on the scene.

Electronic surveillance takes many forms, and is being used more frequently in terrorism and organized crime investigations. Some of these, most of which require a court order, include:

- Telephone wiretap
- Electronic intercept of oral conversation
- Voice paging
- Digital display paging
- Cellular telephone intercepts
- Pen register
- Internet or computer communications intercept

Additionally, there are also a great number of sources on the Internet that are available to investigators to seek information.

THE FUTURE

Computer-related crime deserves more attention from a futures perspective, largely because of the rapidly changing nature of technology. One can only speculate as to the types of crime the world will face in the years to come. Of particular importance to the investigator is the ability to foresee ways in which new forms of technology will be embraced by criminal elements. Cybercrime is not an American innovation, and today borders are no obstacle to criminals who can use many forms of communication and transportation to carry out criminal activity. Some of this involves what are now traditional types of crime, such as fraud, child pornography, cyber-attacks on national security, and stalking. Others involve relatively new types of crime, such as data manipulation, asymmetric warfare, identification theft, and cyberbullying. A report by

already come close to reaching a trillion dollars. Such high-volume crimes child pornography and identity theft, two types of crime that cross national a international borders, involve thousands of individuals, both as perpetrat and victims.

The U.S. National Consumers League (NCL) data in 2007 indicated th the total losses of Internet fraud amounted to $17,508,480, and the most f quent schemes were fake checks (29 percent), general merchandise (23 p cent), auction (13 percent), Nigerian advance fee loans (11 percent), lotter (7 percent), phishing (3 percent), advance fee loans (3 percent), friendsh and sweetheart swindles (1 percent), and Internet access services (1 p cent).[3] A growing industry in counterfeit documents exists, including drive licenses, personal identification cards, and other forged documents, which c be bought online through web sites, some of which originate in China a Panama. See Box 19.2 for a typology of Internet fraud.

BOX 19.2 A TYPOLOGY OF INTERNET FRAUD

- Identity theft
- Credit card fraud
- Online auction fraud
- Short firm fraud
- Advance fee fraud
- Direct investment fraud
- Drug sale scams
- Prize/sweepstakes fraud
- Social engineering and Internet fraud

Source: Tae J. Chung, "Policing Internet Fraud: A Stud of the Tensions Between Private and Public Models o Policing Fraudulent Activity in Cyberspace with Particula Focus on South Korea and Special Reference to the United Kingdom and the United States." Unpublished dis sertation, The University of Leeds School of Law, Leeds, UK (December 2008), 64.

Reported cybercrime numbers are quite low compared to reality, according to many experts, who note that many victims fail to report Internet fraud because of the embarrassment associated with being scammed. In addition, some large companies and corporations do not report cybercrime and cyber-attacks because they may fear customer lack of confidence, or do not wish to draw attention to the vulnerability of their system.

Individuals involved in economic fraud are more likely to be older than those involved in "hacking" or software piracy; child pornographers cut across international dimensions that may involve persons from two or more countries; identity theft is usually either an individual or group-related criminal activity; and terrorist web sites may involve numerous persons. Enterprise and organized crime groups have taken to the use of various forms of technology to elude detection and foster communication.

Investigations following the September 11, 2001, terrorist attacks in the United States and the foiled attack in England in August 2006 revealed a global computer network used by terrorists to communicate, as well as the use of computers, especially the Internet, to gather information about targets and to

investigations. The computing power of today's technology is enormous, enabling the user to run a broad range of programs, commonly referred to as software, in conjunction with internal and external drives.

The computer contains a number of files that are connected to different types of software, such as word processing, spreadsheets, databases, e-mail, or web sites. Some of these programs, such as dictionaries and directories, may not be alterable, whereas user-created files are developed by the user and generally prove to be the most valuable from an investigative standpoint. One of the major exceptions involves downloaded images or documents that may be used in developing a *prima facie* case, such as for child pornography.

Some of the more important files that an investigator should be familiar with appear in Box 19.3 on "File Types of Interest."

BOX 19.3 FILE TYPES OF INTEREST

- Address books
- Audio or video files
- Bookmarks
- Calendars
- Databases
- Documents, correspondence files
- E-mail files
- Favorite sites
- Images and graphics
- Indexes
- Spreadsheets
- Voicemail
- Social networking accounts

Moreover, the development of high-quality peripheral devices, such as scanners and printers, has increased opportunities for the criminal element to perform further illicit activities, including counterfeiting, various types of fraud, child pornography, and identity theft.

LEGAL ISSUES

In many ways investigation involving various forms of technology, especially computers and the Internet, are complicated by a myriad of legal issues, court decisions, and policy issues of organizations. Because case law in this area is relatively new, there are times when the investigator may be operating in uncharted territory, or may come up against newly designed software or innovative criminal activities. (For example, terrorists and organized criminals frequently communicate within interactive games, making it difficult to intercept using conventional technology.) Further, because many policies may be based on individual state laws, they may not be applicable from one state to another. For this reason, when in doubt, the investigator should consult with appropriate legal counsel.

On the federal level, there has been a steady stream of decisions by circuit courts that serve to give better clarification to the procedures that must be followed by investigators. Generally, a search warrant is required to conduct

research on everything from bombs to building layouts and tracking air transport vulnerabilities.

Emerging databases and search engines on the Internet enable individuals to gather information on virtually any subject, including biographical data on millions of individuals. For instance, the Google search engine has integrated several public information databases into its basic search capabilities. Anyone can now enter a Vehicle Identification Number (VIN) into the search engine and get free a basic report on the history of the vehicle from CarFax.com and other similar enterprises.

As the amount of public information about individuals has increased, the availability of inexpensive, portable storage capacity has also increased. For instance, today it is possible to carry gigabytes of information on a storage device the size of a pack of chewing gum. These portable storage devices allow a person to carry as much as 16,000 pictures (at 500KB each) or more than 10,000 pages of text in their pocket, plugging it into a computer only when needed. The most popular of these devices are the so-called flash or USB drives, because they allow users to transport many gigabytes of data that can be plugged into any computer (Windows or Macintosh) without restrictions of computer ownership or permissions. Handheld personal digital assistants (PDAs), electronic organizers, iPods and iPads, and memory cards may also be used to store information that may be of interest to investigators.

Additionally, smart cards and other small devices may contain their own microprocessors that enable a card to hold and change information, such as funds balances (known as debit cards). Removable storage devices come in many different forms, ranging from the early floppy disks, to zip disks, CDs and DVDs, and tape drives, to name a few.

A further complicating factor in cases involving various forms of electronic technology involves case preparation and the presentation of evidence for court. Because this is a relatively new area in which lawbreakers frequently know more about the technology than investigators or the courts, there is the increasing problem of not being able to present a case that can be understood by a jury. Everything from initial investigations to the collection, presentation, and admissibility of evidence is important.

Electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.[4]

SYSTEMIC COMPONENTS

At the heart of virtually all information technology lies a computer system or central processing unit (CPU). Generally, these systems contain a data storage component and a "hard" drive that is programmed to run the system. The introduction of *cloud computing* represents another dimension that can hamper

investigation of the contents of a computer's hard drive, or to gather information from an Internet source (e-mail or Internet service providers—ISPs). suspect may give permission for an investigator to conduct a search of his or er computer, but it is advisable to get this permission in writing. Courts have ecome more involved in Fourth Amendment issues related to the search and izure of computers and data culled from ISPs.[5]

The U.S. Supreme Court held in *Riley v. California* that cell phones could ot be searched incident to an arrest without a warrant. The reasoning behind e decision was that cell phone data was not dangerous to the officer nor ld information that may lead to an arrested person's escape from authorities. herefore, any search of cell phone data would require a search warrant (*Riley California*, 573 U.S.___(2014)).

The search of a computer or other electronic device is generally developed m search warrants in other more traditional contexts, with Fourth endment guarantees that protect a person from unreasonable searches d seizures being an important consideration. The highest privacy interest is ached to private dwellings.[6]

In searches and seizures of computers and other forms of electronic storage, investigator is generally required to establish probable cause to obtain a rrant. This includes reasonable grounds to believe that the data to be seized ually exists and will provide evidence of a crime, the location of what will searched, and a reasonably detailed description of the information or data at will be retrieved.[7]

The primary issue in computer-related cases centers on an individual's right privacy regarding information stored in a computer or other device. There e numerous locations from which information can be obtained. As it relates digital forensics, the most important case law for investigators is the decision ndered in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (509 U.S. 579, 1003), at addresses the issue of the admissibility of expert witness evidence. The so-lled "Daubert Test" of Rule 702 of the Federal Rules of Evidence requires that pert testimony must:

- Be grounded in knowledge.
- Have a valid *scientific* connection.
- Be supported in scientific journal publications.[8]

e Box 19.4.

OX 19.4 SOURCES OF INFORMATION

- The home
- The workplace
- Personal computers and other portable devices
- Social networking sites (e.g., Twitter, Facebook, Instagram, LinkedIn)
- Internet service providers (ISPs)
- Chat rooms
- Web sites
- External storage devices

Home Computers

As indicated earlier, home computers and other personal and portable devices fall under the purview of the Fourth Amendment of the U.S. Constitution, which protects citizens from unreasonable searches and seizures. A search warrant requires permission to gain entry to the residence or portable devices in possession of a suspect. As noted, the warrant must include a statement as to what technological equipment (computers, storage devices, cameras, printers, etc.) is to be searched, what is to be sought, and why the warrant is requested. The investigator must show probable cause for the search, which may be based on a variety of circumstances, such as prior knowledge based on the experience of the investigator; the past criminal record of the suspect; or information provided by informants and victims. There is no reasonable expectation of privacy when the information was openly available, where the device has been stolen, where control of the device was given to another person, or when the individual owner loses control of the device.[9] In cases in which the home or computer may be shared by another person, the other person may give permission to search the computer, but not access to password-protected files.[10]

Workplace Computers

Workplace searches present a somewhat different issue, and it has been held that an employee does not necessarily have a right to the expectation of privacy.[11] However, in determining an individual's expectation of privacy, Stephen W. Cogar suggests that the following questions should be considered:

- Is the employee's office shared?
- Is the hard drive password-protected?
- Is the computer physically locked?
- Is the office locked, and if so, who has access?
- Can the files be accessed remotely through a network program?
- Is there an employee policy in place regarding computer usage that states that files can be searched or monitored?
- Is the policy enforced uniformly?
- Is there evidence that the employee was aware of the policy?
- Is software used to monitor computer use, and are employees aware of this practice?
- Do work stations contain a message when the computer is accessed that the computer can be monitored?[12]

In many instances, employees may contend that they were not aware of company policy, which may negate permission given by the employer to conduct a search. For this reason, it is advisable to seek a search warrant whenever possible.

Internet Service Providers

When a suspect may be anonymous, using a screen name or other form of e-mail address, the best source of identification is likely to be an ISP, such as

Comcast, Earthlink, Windstream, and so on. Although the content of information may be protected under the Fourth Amendment, the Courts have held that the identity of the subscriber is not protected. However, a number of recent cases in which the government has sought to obtain information from Internet service providers, specifically in terrorism-related cases, have sparked debate, and it is likely that the issue will be addressed by the Supreme Court in the future.

While under certain circumstances a person may have an expectation of privacy in content information, a person does not have an interest in the account information given to the ISP in order to establish an e-mail account. This is considered non-content information.[13] This includes: Name; billing address; and home, work, and fax telephone numbers. The Stored Wire and Electronic Communication and Transactional Records (SWECTRA) Act requires ISPs to disclose non-content information to the law enforcement community pursuant to legal authorization.[14] The Cyber Security Enhancement Act of 2003, which is part of the Homeland Security Act of 2002, "makes it easier for police agencies to obtain investigative information from Internet service providers (ISPs) and shields from lawsuits ISPs who hand over user information to law enforcement officers without a warrant."[15]

Cases involving terrorism investigations permit disclosure of more non-content information than is permissible in other types of criminal investigations. The USA PATRIOT Act:

> can force the disclosure of a subscriber's name; address; local and long distance telephone connection records, or records of session times and duration, length of service (including start date and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporary assigned network address; and means and source of payment for such service of a subscriber).[16]

Chat Rooms and Social Networking

One of the most common forms of communication today is the use of social media that have changed in large measure the way Americans relate to each other. Twitter, text messaging, Internet "chat rooms," and social networking sites such as Facebook, Instagram, and LinkedIn have made it possible to exchange photos and other data on a variety of communications technology. These methods of communication have become commonplace in the United States and most other developed and developing countries. The changing capabilities of new forms of communications technology provide a broad range of opportunities available to users, including access to geospatial technology, relational databases, visualization, sophisticated statistical and analytical tools, and access to thousands of web sites. See Box 19.5 on cyber-harassment.

BOX 19.5 DID YOU KNOW ... CYBER-HARASSMENT

Cyber-harassment disproportionately impacts women. The US National Violence Against Women Survey reports that 60 percent of cyber stalking victims are women, and the National Center for Victims of Crimes estimates that the rate is 70 percent. Of those reporting and other studies, the following emerges:

- Nonwhite women are more likely to be cyber victims. (53%)
- White females are the second most common (45%), but a BJS study found that 84% of white women were victims.
- Least likely to be victims are white males (31%).
- Males are more likely to target female victims.
- Males are more likely to be victims for expressing ideas, or for actions.
- Sexual orientation is also likely to be a "trigger" for cyber-harassment.

Source: Danielle Keats Citron, "Hate Crimes in Cyberspace," *Harvard University Press* (2014), 13–15.

The many advantages notwithstanding, the potential for utilizing these technological advances for criminal purposes represents a challenge for law enforcement. Two of the more common investigative approaches include identifying pedophiles and child molesters, and investigations of child pornographic images on web sites and in the possession of individuals.

"Sting" operations by police departments, in which investigators communicate with suspected pedophiles who are trying to lure children into illicit relationships, have become commonplace in a number of state and local agencies.

> Child pornography and individuals who possess pictures or video (collectively "images") that are sexually exploitative of children represent one of the darkest sides of the Internet. Investigating and prosecuting child pornography cases inevitably involves more than just the evidence that certain images were found on a computer used by the defendant ...
>
> Child pornography investigations often involve people who are quite knowledgeable about technology, computers, and the Internet. They trade images with other collectors within their own towns and around the world using, for example, Web sites, file sharing, e-mail, buddy lists, password protected files, or *encryption* (emphasis in original).[17]

See Figure 19.1.

With the growth of social networking sites on which many young people post revealing or sexually explicit photographs, the problem has become more complex, and some sites have agreed to remove individuals who have a criminal record involving children from access.

Web Sites

Today there are thousands of web sites, making it possible to gather information on almost any subject. Some of these are nothing more than propaganda