

Cybercrime generally falls into three categories:

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

The investigator should be familiar with the more common types of crime using information technology. The National Institute of Justice's *Electronic Crime Scene Investigation: A Guide for First Responders* is an important publication that should be of interest to all investigators.<sup>2</sup> Some of the material for this chapter was culled from this NIJ guide, as well as other publications. See Box 19.1.

#### BOX 19.1 COMMON TYPES OF CYBERCRIME

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

It 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

do 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 100,000 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 fund 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.<sup>4</sup>

## 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

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

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 and 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

s, enabling an investigation of the contents of a computer's hard drive, or to gather information as software from an Internet source (e-mail or Internet service providers—ISPs). A suspect may give permission for an investigator to conduct a search of his or her computer, but it is advisable to get this permission in writing. Courts have become more involved in Fourth Amendment issues related to the search and seizure of computers and data culled from ISPs.<sup>5</sup>

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

The search of a computer or other electronic device is generally developed from search warrants in other more traditional contexts, with Fourth Amendment guarantees that protect a person from unreasonable searches and seizures being an important consideration. The highest privacy interest is attached to private dwellings.<sup>6</sup>

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

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

- Be grounded in knowledge.
- Have a valid *scientific* connection.
- Be supported in scientific journal publications.<sup>8</sup>

Box 19.4.

#### BOX 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 device 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 where the individual owner loses control of the device.<sup>9</sup> 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.

### 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.<sup>11</sup> 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?<sup>12</sup>

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.<sup>13</sup> This includes: Name; billing address; and home, work, and fax telephone numbers. The Stored Wire and Electronic Communication and Transactional Records (SWEETRA) Act requires ISPs to disclose non-content information to the law enforcement community pursuant to legal authorization.<sup>14</sup> 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."<sup>15</sup>

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).<sup>16</sup>

### 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 emerging 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 pornography 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).<sup>17</sup>

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

sites, devoted to dissatisfaction with them draw an individual in how such they subscribe when a sex c A number groups, large However, it s cases based c gest libraries things. Many organization

#### INVESTIC

A thorough is beyond tl understandir Because com

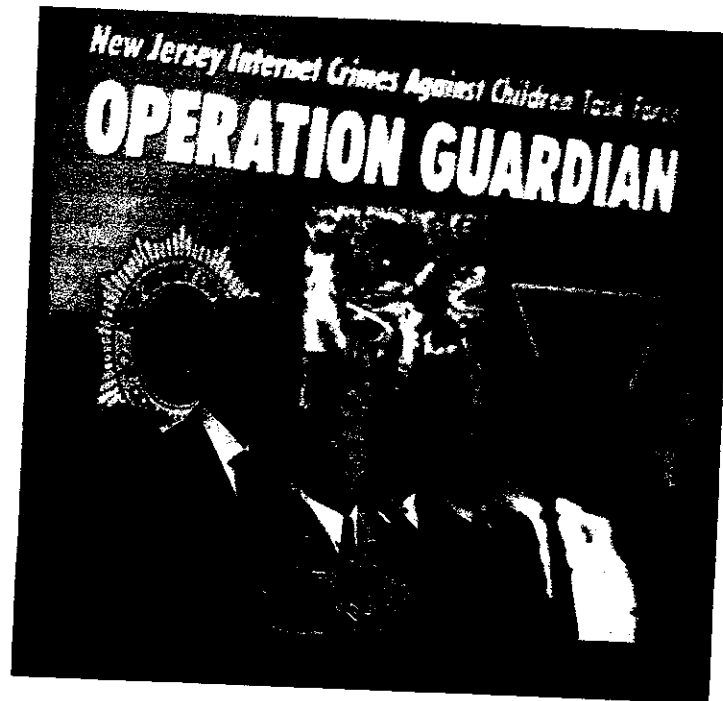


FIGURE 19.1

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

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

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

## INVESTIGATING HIGH-TECH AND IT CRIME

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

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

the Intelligence and National Security Alliance, a nonprofit group, points out that "the growing increase in sophisticated cyber-attacks has moved beyond acceptable losses for government and businesses that simply threaten finances or intellectual property."<sup>23</sup>

Army General Keith Alexander, commander of the U.S. Cyber Command, and Director of the National Security Agency (NSA), at a conference on cyberwarfare in 2011, said that "massive losses of private and public data in recent years to computer criminals and spies represent the largest theft in history," adding that, "Threats posed by cyber-attacks on computer networks and the Internet are escalating from large-scale theft of data and strikes designed to disrupt computer operations to more lethal attacks that destroy entire systems and physical equipment."<sup>24</sup>

Gordon Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation, in testimony before a congressional committee warned in 2011 that cyber criminals represent a major threat to financial and business corporations. He noted that, "[T]he number and sophistication of malicious incidents has increased dramatically over the past five years and is expected to continue to grow."<sup>25</sup>

Information technology offers investigators one of the most important advances in law enforcement, and is a growing area of development. Most federal agencies and many police departments are now employing crime analysts—specialists schooled in this technology—who can serve as an important source of support to field investigators.

### IMPORTANT CASES

*Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993)

*United States v. Hambrick* (2000)

*Trulock v. Freeh* (2000)

*United States v. Simons* (2000)

### DISCUSSION QUESTIONS

1. Why is changing technology important in criminal investigation, and how will these changes affect future investigators?
2. Why is so-called cybercrime of increasing concern?
3. What are the three categories that cybercrime usually falls into?
4. What are some of the common types of cybercrime?
5. Why are cybercrimes frequently difficult to prosecute?
6. What types of computerized files can be of importance to an investigator?

7. The *Daubert*
8. Why is ar
9. Why mus
- of compu
10. In genera

### NOTES

- 1 Susan W. J  
*Cybercrime:*  
Ralph D. Cl
- 2 U.S. Depart  
2nd ed. (W  
com/Electr
- 3 Tae J. Chun;  
Models of  
Korea and S  
dissertation
- 4 Ibid., 4.
- 5 Stephen W.  
Providers,"  
2003), 11.
- 6 *Welsh v. W*  
Prosecutor  
a Computer  
Academic P
- 7 Donald Res
- 8 Brian Carri  
digital-evid
- 9 Rolando V.  
9th ed. (Ne
- 10 *Trulock v. Fr*
- 11 *United State*
- 12 Cogar, op. c
- 13 *United State*
- 14 Cogar, op. c
- 15 Frank Schr  
Saddle Rive
- 16 Cogar, op. c
- 17 U.S. Depa  
Courtroom  
Institute of
- 18 *United State*

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

The U.S. National Consumers League (NCL) data in 2007 indicated that the total losses of Internet fraud amounted to \$17,508,480, and the most frequent schemes were fake checks (29 percent), general merchandise (23 percent), auction (13 percent), Nigerian advance fee loans (11 percent), lottery (7 percent), phishing (3 percent), advance fee loans (3 percent), friendship and sweetheart swindles (1 percent), and Internet access services (1 percent).<sup>3</sup> A growing industry in counterfeit documents exists, including driver's licenses, personal identification cards, and other forged documents, which can be bought online through web sites, some of which originate in China and 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 Study of the Tensions Between Private and Public Models of Policing Fraudulent Activity in Cyberspace with Particular Focus on South Korea and Special Reference to the United Kingdom and the United States." Unpublished dissertation, The University of Leeds School of Law, Leeds, UK (December 2008), 6.

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, so many 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