Information From the Public, Social Media, Information Networks, Digital Devices, and Other Sources
OBJECTIVES

After reading this chapter you will be able to:

- Discuss methods of obtaining crime information from the public, including tip lines, television shows, and AMBER Alerts.
- Discuss the role of confidential informants in criminal investigations and their various motivations for providing information to the police.
- Discuss information networks as a source of information in criminal investigations.
- Explain why the collection of gang intelligence is useful for criminal investigations.
- Explain the role of digital devices and digital evidence in investigations.

From the CASE FILE
“Ain’t No Love in the Heart of the City”

On Monday, April 15, 2013, at 2:49 p.m., a bomb exploded on a sidewalk near the finish line of the Boston Marathon. A second bomb detonated thirteen seconds later, 180 yards from the first. Because the bombs were placed among the crowds of people watching the runners, many injuries resulted. Three people were killed, and 264 were injured. Most injuries consisted of leg amputations, burns, and shrapnel wounds. Police, fire, emergency medical personnel, and marathon spectators took immediate action to render aid to the injured. Many public safety and medical personnel were already on scene or nearby due to normal marathon security preparations and routine medical standby for the runners. Immediately after the explosions, Twitter was used extensively by spectators, news outlets, and the Boston Police Department to provide news and updates from the scene. After the injured were tended to and transported to area hospitals, the forensic investigation began, with investigators trying to collect evidence from the bombs to learn how they were constructed and who may have been responsible. It appeared the bombs were similar to each other in construction: Both consisted of nails and BBs contained in pressure cookers. It was believed they had been transported in backpacks. Within hours, authorities issued several press releases, including a request for photographs and video from people on or near the racecourse before, during, and after the explosions.

Because of the law enforcement request, thousands of photos and videos were submitted. Investigators also obtained video from surveillance cameras operating at and near businesses along the racecourse. Many photos were posted on the social media site Reddit for others to examine and analyze. Captured in these photos were many suspicious-looking individuals in the crowds, some of whom were carrying large backpacks. Some people with backpacks who were photographed numerous times in the area near the explosions appeared to have little or no interest in the race. In some photos they were carrying their backpacks; in others they were without them. One particularly curious video showed a subject who was blackened from the explosion running and jumping over bystanders who were injured and laying on the ground. ¹ The New York Post even published on its front page a photo of two suspicious-looking individuals in the marathon crowd.²

In trying to identify who may have carried and placed the bombs, law enforcement authorities spent thousands of hours searching for and examining videos and photos, paying special attention to activities around the two areas where the bombs exploded. After three days of searching, collecting, and analyzing photos and video, investigators were confident they had identified the bombing suspects. On Thursday evening, April 18, at 5:20 p.m., the FBI held a news briefing on national television and released photographs of two suspects in the bombing.
The photos had been obtained from surveillance cameras along the racecourse. The suspects depicted in the photos were not the same individuals whose photographs were earlier published on Reddit or in the *New York Post*. The decision to release the photos was not made lightly due to concerns the suspects would flee or become even more dangerous in their attempt to avoid apprehension, but authorities needed the assistance of the public to identify these individuals. The FBI identified the two men as Suspect #1, who was wearing a black baseball cap, and Suspect #2, who was wearing a white baseball cap. The images showed the subjects carrying large backpacks and walking in the direction of the finish line shortly before the explosions. The FBI also revealed that Suspect #2 was seen placing a backpack on the ground just seconds before the second explosion occurred.

Other photographs of the suspects had also been obtained by authorities prior to the release of this information to the public. Interestingly, the fact that both subjects continuously wore baseball caps helped authorities find and track them in the photos and videos from various locations. Immediately after the press conference, the FBI’s phone and Internet tip lines (1-800-CALL-FBI; bostonmarathontips.fbi.gov) were overwhelmed with information from members of the public who believed they knew the suspects.

Approximately five hours after the news conference, a Massachusetts Institute of Technology (MIT) police officer was shot and killed while sitting in his squad car. It appeared that an unsuccessful attempt had been made to steal his gun. A witness to the shooting reported that the perpetrator fled and entered a train station. The police responded by searching the train stations and trains but discovered no one. Another witness reported the shooter fled in a Honda Civic and...
provided a license plate number. The FBI used Twitter to publicize this license plate number. At this point authorities were unsure if the officer’s murder was related to the marathon bombings.

Approximately ninety minutes after the police officer was shot, at 12:19 a.m., Cambridge police received a call from a person who reported he had been carjacked. He told the police his car was a black Mercedes SUV. He said he was held by the two men for about a half hour and was robbed of his ATM card, but he had escaped when they stopped at a gas station. About twenty minutes into the interview, the victim told the police that the perpetrators had said they were involved in the marathon bombings and were on their way to another city to detonate more bombs. The police were now on the lookout for the Mercedes SUV and the two carjacking perpetrators. When the vehicle’s GPS antitheft system was activated, a signal was received that located the SUV in Watertown, Massachusetts. Watertown police officers responded to the location of the hijacked vehicle but were unaware of the possible connection between the suspects in the vehicle and the marathon bombing. An officer trailed a Honda Civic that was following the Mercedes SUV, unknown by the officer to be associated with the carjacking of the Mercedes or the shooting of the officer. Suddenly, the SUV and the Honda Civic stopped, and one suspect emerged from each car and started firing upon the officer in his squad car. Other squads responded to the scene and were also fired upon. Officers returned fire. One of the suspects then retrieved several explosive devices from the Civic and began throwing them at the officers; two pipe bombs and a pressure cooker bomb exploded. Numerous officers were injured by the bombs, one of whom died from his injuries in 2014. Additional officers from multiple agencies responded and engaged the subjects in gunfire. During the exchange, one officer was struck by gunfire; one or both suspects were also struck. Out of ammunition, one of the suspects charged at the officers, who proceeded to tackle him. The other suspect then got in the SUV and drove toward the officers and the suspect, who were all on the ground. The officers got out of the way of the speeding vehicle, but the suspect did not. He was run over and dragged about twenty-five feet. The suspect fled in the SUV for about a half mile before abandoning it and fleeing on foot. The officer who was shot, among several other officers, and the suspect who was run over were transported to hospitals. The subject was pronounced dead shortly after arriving at the hospital; the officer’s life was saved. Using the fingerprints of the dead suspect obtained at the hospital, he was identified as Tamerlan Tsarnaev. Tamerlan resembled Suspect #1 in the photos released by the FBI. His immigration records included a photo of his younger brother, Dzhokhar Tsarnaev, who looked like Suspect #2. During and immediately following the shootout between the suspects and the police, the Watertown Police Department received more than 500 calls to 911; normally that dispatch center received thirty calls per day.

Now, at about 1:00 a.m., the search was on for Dzhokhar Tsarnaev, Suspect #2. As the suspect had fled on foot, authorities cordoned off a twenty-block area around the location of the abandoned SUV. Watertown residents were informed by the police to stay in their homes because of the active situation and to report any suspicious activity. With no trace of the suspect, police decided to conduct a house-to-house search, and by 5:30 a.m. that search was underway. Residents of Boston and the surrounding suburbs were advised to shelter in place. One report of a suspicious person carrying a package and being picked up by a taxi was pursued but determined to be false. Taxis, trains, and buses were ordered to stop operations. By this time more than 2,500 officers from over 100 law enforcement agencies had arrived at the staging area to search for the suspect, although many of them had not been requested and did not have official assignments. The management and coordination of the operation were becoming increasingly difficult.

With the name of the missing suspect released to the public, more leads came in about his background and possible whereabouts, including the location of his college dormitory at the University of Massachusetts in Dartmouth. Officers were deployed to the university via helicopter, but he was not located. At 12:35 p.m. on Friday, another press conference was held to update the public on the active manhunt and to reinforce the order to shelter in place. Later in the day, with the suspect still not located, the order was lifted and transit systems were again allowed to operate. It was beginning to look like the suspect had simply disappeared.

Shortly after the order was lifted, a citizen of Watertown went outside to check the cover on his boat, which was parked in his backyard, and noticed what appeared to be blood on it. He quickly looked under the cover and saw a body lying in the boat. He immediately returned to his house and called the Watertown Police. Within seconds, more than 100 officers responded to the scene. One of the officers,
for undetermined reasons, fired his gun at the boat. Other officers believed the gunshot came from the boat and opened fire. Upon ceasefire, officers were still unable to confirm the presence of a person in the boat, so an infrared camera mounted on a helicopter was used to determine that a person was indeed alive and moving in the boat.

Finally, at 8:41 p.m., after communicating with the police, Dzhokhar Tsarnaev emerged from the boat and was arrested. He had sustained multiple gunshot wounds and was taken to the hospital by ambulance. After his condition stabilized, he was interrogated by investigators.

He told investigators that he and his brother acted alone, were motivated by U.S. involvement in the wars in Iraq and Afghanistan, and had planned to travel to New York City to detonate bombs in Times Square. While in the boat, Dzhokhar wrote what amounted to a confession on a panel of the boat. In gathering evidence, investigators obtained access to Dzhokhar’s Twitter account. One of his tweets on the evening of April 15, the day of the bombing, was “Ain’t no love in the heart of the city, stay safe people.” On April 8, 2015, Tamerlan was convicted of thirty charges, including use of a weapon of mass destruction resulting in death. The following month he was sentenced to death.

Case Considerations and Points for Discussion

1. What do you think was the most challenging aspect of the investigation for investigators? What were some other challenges of the investigation?

2. What was the role of the public in the investigation? How did members of the public both help and hinder the investigation?

3. Identify and discuss two things that investigators did well in this investigation and two things that were not done well.
Information from the Public in Criminal Investigations

People may have knowledge about a crime simply because they saw or heard something during the course of their normal activities, but they may not realize their observations relate to a crime. Some of these people may be identified as witnesses through traditional methods, such as neighborhood canvasses. At other times, however, the task for the police is to get these people to realize they may have information that relates to a crime and to report that information. To achieve this the police have several strategies at their disposal. These include the use of tip lines, television shows, special alerts, and social media postings, along with other public information strategies. All of these strategies are discussed in the following subsections.

TIP LINES

Tip lines are designed to be an easy and convenient method for citizens to provide information to the police via a telephone or the Internet. Tip lines can be created for and dedicated to specific crimes, such as the one set up during the Boston Marathon bombing investigation, or they can be oriented toward any crime on which a citizen may wish to report information.

Crime Solvers, WeTip, and Crime Stoppers are examples of well-established and continuously operating tip lines. Crime Stoppers is a nonprofit corporation established in 1976. It offers cash rewards up to $1,000 to anonymous persons who contact the tip line and provide information that leads to the arrest of those responsible for crimes. Law enforcement personnel staff the phone lines, which are most often located in police dispatch centers, and draft press releases on crimes in the community.

According to the Crime Stoppers Web site, information provided to Crime Stoppers programs has led to over a million crimes being solved, more than $4 billion worth of stolen property and narcotics being recovered, and more than $1 million of rewards paid out. Although these are impressive statistics, it may actually be quite difficult to determine precisely the role and value of the information received through the tip line in solving crimes. Information in an investigation may come from various other sources (e.g., physical evidence, other witness statements) in addition to people providing information via a tip line, and each of these sources of information/evidence may contribute to the crime being solved. There is no research that has examined the actual impact of tip line information on the likelihood of crimes being solved, nor is there research that has examined what proportion of tips are detailed and credible enough to warrant any police action.

Some tip lines have been established on the Internet, such as the Crime Stoppers Web site. In the wake of September 11, 2001, the FBI established an online tip line as a way of receiving information from the public concerning suspected terrorist activity. During the Unabomber investigation (see Chapter 15), the FBI received 20,000 tips about the case to their tip line. The National Center for Missing and Exploited Children (NCMEC) Web site has a tip line to receive information about child pornography, sex offenders, and children who are at risk of sexual abuse. In 2015 the tip line received over four million reports from the public and electronic service providers; nearly all the reports were about incidents of apparent child pornography.

As discussed in the introduction to this chapter, citizen tips were also key in the identification and apprehension of the Boston Marathon bombers. The images of suspects...
shortly before and after the bombs were detonated were broadcast nationwide by the FBI, and immediately information about the identity of these two individuals was provided to authorities. Another call to the police led to the apprehension of Dzhokhar Tsarnaev in the boat. In this investigation and many others, citizens’ calls to tip lines played a critical role.

TELEVISION SHOWS
Throughout the years, several “crime time” television shows have aired that publicize unsolved crimes and encourage citizens to contact authorities with related information. The most notable was America’s Most Wanted, which aired on FOX and the Lifetime network from 1988 to 2012. The show was hosted by John Walsh, whose own son was abducted and murdered by a serial killer in 1981. During the twenty-five years in which it aired, the show led to the capture of more than 1,200 persons. The most recent iteration of the show is The Hunt with John Walsh, which as of 2017 was airing on CNN. The show consists of reenacted crimes with actors playing the victims and offenders. After the case is presented, viewers who believe they have information about the perpetrator are asked to contact authorities through the show’s toll-free telephone tip line. Nearly all the cases profiled on the show involve serious violent crimes for which the police have a good idea about the identity of the perpetrator. The suspect’s name is often known, a photograph is often shown, and details about the person are often provided.

AMBER ALERTS
Another method of mobilizing the public to provide crime information to the police is the AMBER Alert. The AMBER Alert (America’s Missing: Broadcast Emergency Response) was created in 1996 after nine-year-old Amber Hagerman was abducted and murdered while riding her bicycle in Arlington, Texas. By 2009 each state operated an AMBER Alert system. With AMBER Alerts, when a law enforcement agency is notified that a child abduction has taken place or is suspected of having taken place, an alert that includes a description and photo of the missing child, the suspected perpetrator, the suspected vehicle, a tip line phone number, and any other information that may assist in locating the child is transmitted to area radio and television stations as well as to the corresponding state’s AMBER Alert Facebook page, to cell phones, and to Twitter (@AMBERAlert). In some instances information relating to the abduction is placed on electronic freeway emergency signs. The AMBER plan and alert system is modeled after the alerts used to notify people of impending severe weather.

Although each state can operate AMBER Alerts as it best sees fit, the U.S. Department of Justice recommends the following guidelines for the issuance of alerts:

- Law enforcement must confirm that an abduction has taken place.
- The child is at risk of serious injury or death.
- There is sufficient descriptive information of the child, captor, or captor’s vehicle to issue an alert.
- The child must be seventeen years old or younger.
- The child’s name and other critical data should be entered immediately into the FBI’s National Crime Information Center. Information describing the circumstances of the abduction should be entered and the case flagged as a child abduction.

Most states operate their AMBER Alerts in accordance with these guidelines. Silver Alerts are a similarly designed alert notification system to help locate elderly individuals who may be at risk or lost but in situations where no criminal activity may be involved.
Chapter 9 • Information From the Public, Social Media, Information Networks, Digital Devices, and Other Sources

The logic behind AMBER Alerts is that when children are abducted by strangers, harm comes to them quickly; therefore, a quick law enforcement response is needed. Research has shown that if a child is abducted by a stranger, the victim is killed within the first hour in 44 percent of cases, within three hours in 74 percent of cases, and within twenty-four hours in 91 percent of cases.13

According to the AMBER Alert Web page (www.amberalert.gov), as of 2017 there had been nearly 900 successful recoveries of children as a result of AMBER Alerts (see Case in Point 9.1 and Case in Point 9.2). According to the NCMEC, 179 AMBER Alerts were issued nationwide in 2016.14 This number was similar to those of previous years (see Figure 9.1). Of these 179 alerts, eight of the cases were determined to be hoaxes, and thirteen were determined to be unfounded. One hundred fifty-five cases resulted in the recovery of the child—forty-three as a direct result of the alert. Three children remained missing, and thirteen were located deceased.

Approximately 60 percent (107) of the alerts in 2016 involved an abduction by a parent or other family member (see Figure 9.2). Among the sixty instances of a non-family-related abduction was an unspecified number of abductions by individuals unknown to the child. For perspective, in 2015 law enforcement agencies made 460,699 missing children entries into the NCIC database15 (this number does not reflect cancelations when the child was located and does include runaways). It is unknown, however, how many of those abductions involved the issuance of an AMBER Alert.

Other analyses of 275 AMBER Alerts from 2003 to 2006 showed that 45 percent of the alerts involved abductions by parents (cases where the child is significantly less likely to be harmed), 35 percent involved other relatives or acquaintances, and 20 percent involved strangers (the stereotypical child abduction case).16

PHOTO 9.4: AMBER Alerts can be a useful tool in soliciting critical and timely information in child abductions; however, AMBER Alerts also have limitations.
CASE in POINT 9.1  
**An AMBER Alert Success Story**

The Butte County Sheriff’s Office in California issued an AMBER Alert for three children on June 14, 2014. Nine minutes later the children were recovered safely and the suspect was in custody. A citizen saw the wireless emergency alert on his cell phone and looked up and saw the suspect’s blue van. “I can’t believe right when the AMBER Alert came is right when I see the van. That was right within 5 seconds,” Gurinder Jhutty told a reporter. “My gut told me ‘Let’s go back and check it out.’ That’s when I came back and I looked at the license plate and that’s when I started calling 911 and I saw 3 kids in the back. That’s when I started following him.”

Matthew Kline had allegedly taken his three-year-old daughter, eighteen-month-old son, and an unrelated four-year-old girl earlier in the morning. The AMBER Alert cautioned citizens to not approach the suspect because authorities believed he was carrying firearms. Sergeant Jason Hail had spent nineteen years with the Butte County Sheriff’s Office, and this was the first AMBER Alert for him and the agency. The sheriff’s office immediately set up a command post and a call center. Officers had an idea where the suspect was heading but did not know at the time that the alert would go to all the cell phones in the area. “I was very surprised and relieved how quickly it was resolved,” said Hail. “I was impressed and it renewed my faith by showing that people really do care and will take appropriate action.”

CASE in POINT 9.2  
**Another AMBER Alert Success Story**

One spectacular AMBER Alert case involved two teenagers, Tamara Brooks and Jacqueline Maris. An armed man kidnapped the two young women from a remote location in Los Angeles County, California, and kept them for approximately twelve hours while traveling in a vehicle stolen from the male companion of one of the victims. Based on a citizen tip solicited by the AMBER Alert, the perpetrator was cornered and shot to death by sheriff’s deputies and the young victims were rescued.

According to an article in the *Criminal Justice Police Review*,

> [t]he case was touted as an example of AMBER Alert rescuing victims from imminent harm. . . . However, part of the success must also be attributed to the ineptitude and hesitancy of the assailant, who, if he had murderous intentions, committed several stunning blunders. He left living witnesses (the girls’ male companions) who could report the crime and describe the vehicle, he remained in said vehicle with the young women for 12 hours after the abduction, he stopped at one point to buy the victims refreshments at a convenience store, and later drank himself unconscious. Even when he subdued the girls after they failed in a bid to attack him, he did not murder them. Thus in this case the AMBER Alert was “effective” largely because the abductor was fortuitously incompetent and indecisive. This is certainly not to say that the alert deserves no credit, or that law enforcement officials did not act appropriately and heroically in this case. The point is simply that the “success” resulted in large measure from astonishing good luck, and that it is unreasonable to expect that such luck will typically prevail in stereotypical abduction cases where AMBER Alerts are issued.  

Copyright ©2019 by SAGE Publications, Inc.  
This work may not be reproduced or distributed in any form or by any means without express written permission of the publisher.
Research that has examined the impact of AMBER Alerts highlights some of the particulars of the strategy as well as some of its limitations. First, in nearly all instances (95 percent) when an AMBER Alert is issued, the child is recovered; however, in most of these cases (67 percent) the alert itself had nothing to do with the recovery. The abduction of Tamara Brooks and Jacqueline Maris is an example of an AMBER Alert actually being credited with a positive outcome, but other factors were also important in this regard (see Case in Point 9.2).
Second, and perhaps most important, the researchers found that AMBER Alerts involving stranger abductions were much less likely to result in a recovery of the child. In these cases, harm was also more likely to have been done to the child prior to recovery.

Third, the researchers found that in cases where the child was recovered, in only 17 percent was the recovery within six hours of the abduction. The NCMEC analysis of alerts from 2015 revealed that in only 12 percent of cases was the recovery made within three hours of the alert activation. This is significant given the research finding that if harm is to be done to a child in an abduction case, it is usually done within the first three hours (see Case in Point 9.3). Finally, it is interesting to note that research shows repeated or overuse of such alerts may lead people to ignore them, similar to how people tend to ignore car alarms, thus reducing their effectiveness.21

Timothy Griffin, a noted researcher on AMBER Alerts, concludes that “AMBER Alerts rarely result in the retrieval of abducted children from clearly ‘life-threatening’ situations, and . . . most of the publicized successes involved relatively benign abductors and unthreatening circumstances.”22 In short, while the AMBER Alert does have benefits, it is also important to understand its limitations.

**CASE in POINT 9.3**

**The Murder of Carli Brucia**

The Carli Brucia case provides a tragic example of when an AMBER Alert did not save a life. Carli was abducted by a stranger on the evening of February 1, 2004, near a car wash in Manatee County, Florida. By chance, the abduction was recorded by a surveillance camera that was examined the next evening, leading to an immediate nationwide AMBER Alert. NASA technology was used to improve the surveillance video’s accuracy, and with tips from citizens, investigators had identified, captured, and elicited a confession from Carli’s abductor by February 5. It is difficult to see how authorities could have acted more swiftly or professionally. Yet, tragically, Carli was already dead when the alert was issued on February 2.20

**PHOTO 9.5:** Within approximately twenty-four hours of Carli Brucia’s abduction, an AMBER Alert was issued. The alert led to information about who abducted her (the man seen in this still video photograph). Unfortunately, Carli was murdered prior to the issuance of the alert.

---

**Code Adam:** An alert designed to notify patrons and shoppers of a missing child in a store or other business.

**Code Adam** is a program created by the NCMEC. It is an alert used by participating businesses and stores when a child goes missing on the premises. When a Code Adam is activated, a designated employee obtains a detailed description of the child and broadcasts the description of the child in the store. Other employees then stop working, monitor the
PHOTO 9.6: Another way to get the word out about missing persons is by putting requests for information on semi-trailer trucks.

entrances and exits of the store, and search for the child. If the child is not found within ten minutes, law enforcement is called.

OTHER METHODS OF SOLICITING INFORMATION FROM THE PUBLIC

Along with tip lines, television shows, and special alerts, other methods have also been used to obtain information from the public. For example, in partnership with the NCMEC, more than 4,000 Walmart and Sam’s Club stores post photographs of missing children in the stores, alerting shoppers to be on the lookout for the children. The NCMEC also disseminates information and photos on missing children through Facebook.

Some law enforcement agencies have assembled their own “most wanted” lists and publicize them in newspapers and on the Internet. Some agencies regularly disseminate crime alerts to notify citizens of particular crimes and to put them on the lookout for related suspicious activity. One commonly cited limitation to newspaper and television news alerts is that the people most likely to know about crimes and criminals may not regularly read the newspaper or watch the television news. In recognition of this, many police departments place crime stories and calls for information on their social media sites, in particular Facebook and Twitter (see the following discussion). The Seattle (Washington) Police Department has used billboards and bus ads that feature photos of homicide victims in cases where the perpetrators have not yet been identified.23 Placed above the photos is the simple question, “Who Killed Me?”

Other cities have experimented with making standardized forms available in churches and other public places that citizens can use to anonymously inform on drug dealers and other criminals. The Bergen County Sheriff’s Department in New Jersey developed FaceCrook (www.facecrook.net), a computer application available to jail inmates that allows them to anonymously provide information to implicate others involved in crimes.24

LIMITATIONS

In one way or another, all of these strategies are designed to elicit information from members of the public (or inmates, in the case of FaceCrook). While these methods can assist in investigations, they are not without limitations. First, with regard to tip lines in particular, the police can get easily overwhelmed with “leads,” most of which are likely irrelevant in the investigation. Members of the public may think their information relates to the crime
in question when actually it does not, but at the time the information is received, the police may not be able to recognize the information as false or irrelevant. For example, during the Boston Marathon bombing investigation, police received numerous tips about suspicious individuals in the crowd. In the Washington, D.C., sniper investigation (see Chapter 1), residents called the police to report sightings of hundreds of white vans and white box trucks. As it turned out, none of this information was accurate.

Also, false information received through tip lines and other sources may cause the police to focus on innocent “suspects.” Accordingly, questions may arise about how people might be affected when the police take action against them as a result of anonymous information. It is even possible that individuals might purposely call to falsely report the conduct of friends, associates, ex-husbands, or ex-wives as a way of getting revenge. The police can be used by citizens in this regard, and the consequences may be unpleasant for everyone.

Other potential problems associated with the use of the public as a source of information involve (1) how reward money should be allocated among people who provide useful information; (2) the credibility and motivation of citizens who inform for purposes of money, especially when they remain anonymous; (3) how the publicity on the case may affect the perceptions of others with information on the case; (4) how publicity may affect other dimensions of the case (e.g., pretrial publicity and the ability to receive a fair trial); and (5) whether money should be paid for actions that are arguably one’s civic responsibility. These are difficult questions to address, but investigators should at least be aware of them when considering information from the public.

Information from Social Media in Criminal Investigations

Social media has become an indispensable tool in criminal investigations during the last ten years, and more so now than ever. For many people social media means Facebook and Twitter,
although there are a multitude of other social networking sites also available on the Internet (see Table 9.1 for a listing of some of the most widely used sites). Facebook was created in 2004 and today has nearly two billion users worldwide. The rules of Facebook state that a member must be at least thirteen years old to join. There are no user fees associated with registering or using Facebook; Facebook revenue is derived primarily from advertising. Members register on the site and add other members as “friends.” Friends can communicate with each other in various ways, including through the sharing of messages, photos, and videos. According to Facebook, approximately 250 million photos are uploaded on Facebook every day; currently the site holds more than 100 billion photos. One of the primary concerns associated with Facebook is user privacy. Because it is possible for members to see content posted by other members, Facebook provides various privacy settings that can limit the amount of information available to those who are not on a member’s friends list.

Generally speaking, social media sites can be used by law enforcement agencies in two ways:25 First, agencies can “push out” information, such as when a police department provides notification of a crime and requests information from the public (see Case in Point 9.4). Social media allows the police to quickly release crime information that is unfiltered by other media outlets. Also, as noted earlier, one of the limitations of traditional media as a way of prompting citizens to provide crime information to the police is that the people

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>SPECIAL FEATURE</th>
<th>ACTIVE USERS (WORLDWIDE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>Used to share text, photos, and videos with friends and to follow the profile of businesses, organizations, and VIPs.</td>
<td>User needs to be at least thirteen years old to have an account.</td>
<td>2 billion/monthly (June 2017)</td>
</tr>
<tr>
<td>Flickr</td>
<td>A blog where users can upload photos and videos. The focus is on photo sharing.</td>
<td></td>
<td>92 million</td>
</tr>
<tr>
<td>Google+</td>
<td>Users can create a profile to access many different products.</td>
<td>Products include photos, videos, blogs, etc.</td>
<td>540 million/monthly (October 2013)</td>
</tr>
<tr>
<td>Instagram</td>
<td>Mostly used to share photos or videos with others.</td>
<td>User can use hashtags to make content easier to find.</td>
<td>700 million/monthly (April 2017)</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>Users can create a business profile that resembles their resume or CV. Employers can use it to find job candidates. Also used for networking purposes.</td>
<td>Content focuses on user’s professional life and not private life.</td>
<td>106 million/monthly (April 2016)</td>
</tr>
<tr>
<td>Pinterest</td>
<td>Used to share pictures and ideas. User can find recipes, crafting ideas, vacation ideas, etc.</td>
<td></td>
<td>150 million/monthly (October 2016)</td>
</tr>
<tr>
<td>Reddit</td>
<td>Users can share mostly text content and discuss different topics with others.</td>
<td>Votes determine if the post appears at the beginning or end of a category.</td>
<td>169 million</td>
</tr>
<tr>
<td>Snapchat</td>
<td>Allows users to share photos and short videos with text.</td>
<td>Photos and videos “disappear” after viewing.</td>
<td>Approximately 255 million/monthly (May 2017)</td>
</tr>
<tr>
<td>Tumblr</td>
<td>Users create their own blogs and upload text, video, audio, etc. to them.</td>
<td></td>
<td>420 million blogs</td>
</tr>
<tr>
<td>Twitter</td>
<td>Users share short messages (tweets) with their followers.</td>
<td>Messages can have no more than 140 characters per post.</td>
<td>328 million/monthly (April 2017)</td>
</tr>
<tr>
<td>YouTube</td>
<td>Web site to share various kinds of videos.</td>
<td></td>
<td>1.5 billion/monthly (June 2017)</td>
</tr>
</tbody>
</table>
most likely to have such information may be unlikely to use traditional media. Because of the popularity of and easy access to social media, the use of social media represents a potential remedy to this problem.

One of the concerns with the investigative use of social media is that the police lose control of the information after it has been published. For example, in 2016 and 2017, the Washington, D.C., police began to regularly use Twitter to call attention to missing/runaway juveniles. In 2017 these tweets began to be retweeted and eventually incorrect conclusions were drawn that the missing girls had been abducted by an unknown assailant. This information was then retweeted some more. Essentially the tweets took on a life of their own, and it became a fake news story.27

The second way by which social media can be used by law enforcement agencies is by “pulling in” information about subjects directly from a site. Information can be pulled in using several methods. For example, on Facebook, the easiest way is when an investigator creates an account and anonymously searches for people he or she is interested in learning about. Because this approach involves the collection of public information, it is sometimes referred to as open source information. If a subject does not have privacy settings on her or his account, investigators may be able to identify the subject’s friends and associates; see written conversations between the subject and his or her friends; discover statements, photographs, and/or videos related to crimes in question; learn of the subject’s recent activities and whereabouts, and view other photographs and videos on the subject’s page (see Exhibit 9.1). On Twitter it may be useful for investigators to monitor the musings (tweets) of particular individuals. As such, searches of words using hashtags could be useful. For example, in an attempt to discover and follow gang members on Twitter, hashtags referring to gang names (e.g., #GDK for Gangster Disciple Killers) or other words (e.g., #FuckDaOpps, which is street language referring to hatred of the police) could be searched.28 In identifying possible gang members, certain emoji symbols have also found to be used more by gang members than by others.29

Another pulling in approach is for an investigator to use an alias name to create a social media account. In essence, the investigator goes undercover online. With Facebook, the investigator may then request to be “friends” with people who are of interest or join a Facebook group that allows easy access to other members’ profiles. Although fake accounts are against the rules of Facebook, they are not illegal. On Twitter an undercover investigator can follow subjects and receive their tweets. The information may be useful in learning of recent activities, thoughts, and locations. It is strongly suggested that law enforcement agencies regulate and control the use of aliases and undercover accounts used to obtain information from social media sites.30

A final way by which authorities may obtain information from social networking sites is via subpoenas or warrants, which is commonly the case when confirming Internet Protocol (IP) addresses (see the discussion later in this chapter on digital evidence), subscriber records, and/or account ownership/registration.31

YouTube is an Internet site that contains videos uploaded by individuals as well as by television networks and other sources. Similar to Facebook, some police departments use YouTube to disseminate crime information and to request information from viewers. YouTube is also a source of information on crimes and criminals. Sometimes people post videos that show or discuss their illegal activities. In one instance a subject stole a Taser from a police vehicle, went home, and video-recorded himself and his father using the Taser on each other. The subject then uploaded the video to YouTube, and investigation by the police led to the YouTube video and to the subjects. There are many other stories of subjects video-recording various criminal acts as they occurred and then posting them on YouTube for later discovery by the police. And as technology evolves, no doubt other avenues will present themselves as sources of intelligence for criminal investigations.
On March 24, 2016, at approximately 9:30 a.m., a subject entered a Walgreens drug store in Germantown, Wisconsin, approached the clerk at the front checkout counter, displayed a knife, and attempted to take money from the cash register. The subject fled the store with a bottle of Mountain Dew he did not pay for. Upon arrival at the scene, police officers learned from the clerk that the subject was a white male in his late thirties to early forties, wearing a gray stocking cap, a dark blue hooded sweatshirt with the hood pulled up, and dark-colored pants. The clerk stated that as she scanned the Mountain Dew bottle, the subject put a handwritten note on the counter in front of her. The note read, “Give me the money or I will stab you. I am not kidding.” She stated that she pushed the cash register away from the subject. He then grabbed the Mountain Dew and the note and ran out the front doors.

Investigators also interviewed a customer who was inside the store, about twenty feet from the front counter, when the robbery occurred. She described the robber as a white male in his early twenties, about 6’ tall and about 160 lbs. She stated she saw the subject flee the store and get into an older silver-grey Honda four-door. Another witness who was near the front door when the subject fled told police she noticed a subject wearing a dark blue hoodie run from the store and get into a silver car with maroon lens covers on the taillights. She described the subject as very thin. A witness who was inside his car parked in the parking lot of the store told police that he saw a white male subject who was approximately 5’5” and wearing a blue hoodie run from the store.

As the witnesses were being interviewed, investigators processed the handle of the cooler from which the Mountain Dew was taken and the countertop by the cash register for DNA. Investigators then obtained the surveillance video from inside the store. The video showed the subject and the incident as described by the store clerk. From the video a still photograph showing the subject’s face was produced, and this photograph was posted on the police department’s Facebook page. The Facebook post read as follows:

March 24th, 2016

We are investigating an armed robbery that occurred at Walgreens (Pilgrim and Mequon) this morning around 9:30 a.m. The suspect is described as a white male, approximately 20 years of age, height 6’0, weight 160, wearing a blue Wisconsin hoodie. The suspect displayed a knife and demanded cash. The subject ran towards Francis Drive and got into the driver’s seat of a silver Honda 4 door.

Below are pictures of our suspect. Anyone who may know the identity of our suspect is encouraged to call the Germantown Police Department (262)253-5555. Please help us by sharing the suspect’s photo.

Chief Peter Hoell

Later in the day on March 24, the GPD received a call from an adult female who stated the person shown in the photo on Facebook resembled a man she knew as Ryan Madell; her kids were friends with Madell. She stated Madell had just been released from prison. She stated she was not certain it was him, but she was very convinced. Investigators were then able to obtain booking photos of Madell from a neighboring jurisdiction. The booking photo resembled the video photo of the suspect at the Walgreens store. A photo lineup that included Madell was then constructed and scheduled to be shown to the clerk witness from Walgreens on March 25 at 3:00 p.m. At about this time, Madell appeared at the GPD to turn himself in for the robbery. He was with his sister and his father. According to the detective’s report:

I said hello and asked “what brings you here today?” Ryan Madell replied “I’m wanted in questioning for Walgreens.” I responded by saying “you’re wanted in questioning, who told you that?” Madell said “I don’t know. It was me.” I said “you want to do the right thing.” He said “yeah,” implying that he wanted to do the right thing and turn himself in. Madell was read his Miranda warnings and arrested.

Meanwhile, in another interview room at the police department, the Walgreen’s clerk witness identified Ryan Madell in the photo lineup as the person who committed the robbery. The Facebook post was viewed a total of 24,000 times and shared 423 times. For perspective, the city of Germantown has a population of approximately 25,000 persons.
Confidential Informants

Most people who provide information to the police in criminal investigations are citizen witnesses (or victims) who provide information on a onetime basis regarding a particular crime or a particular offender. **Confidential informants** (CIs) are people who assist law enforcement in a more active and ongoing capacity, often in drug investigations. CIs are often part of the criminal underworld; they have access to people, places, and information the police do not. They may be friends or associates of criminals, or they too may be involved in criminal behaviors. Typically, CIs provide information to the police in exchange for leniency regarding their own previous criminal behaviors or for payment. Although controversial, the reality is that “without informants law enforcement investigators would be hard pressed to learn the intricacies not only of who is involved in criminal activities but also how, when, where, and with whom.” CIs are especially useful in this era of “anti-snitching” (see Chapter 11) in which some citizens may be reluctant to cooperate with the police. The range of information provided by CIs can be broad and may include the identity of particular offenders, the whereabouts of offenders, and/or the nature of criminal activities in particular places.

Four types of informants have been identified, each with a different motivation for cooperating with the police. First, the **hammered** informant, the most common, is coerced by the police to provide information. These individuals are “squeezed” for information. They “cut a deal” with the police to avoid arrest or to obtain lenient treatment. One hammered informant expressed his motivation in this way: “I wasn’t very cool and acted desperate because I thought I was headed to jail. I offered to do what they wanted and just kept saying I didn’t want to go to jail.” This type of informant has also been referred to as an indentured informant. The next most common type is the **mercenary** informant. This person is motivated by money. He or she is interested in basically selling information to the police. Third is the **vengeful** informant. This person is motivated by revenge against others, such as a competing drug dealer, a competing gang, or nuisance neighbors. Finally, the least commonly encountered informant is the **police buff** informer. This person is a fan of the police—a police wannabe. Unlike the others, this person may not be immersed in the criminal culture, so often his or her access to critical and accurate information is limited. Understand that any combination of these motivations may be at play with any particular informant and that people may initially provide information to the police for one reason (e.g., due to coercion) and then continue their relationship with the police for another (e.g., money).
Although the use of informants can be beneficial in investigations, there are also potential problems that may arise. These problems include the availability of investigators to speak to their informants; investigators developing too close of a relationship with informants; informants not doing what is expected of them; informants providing bad information, which could threaten the investigation or the safety of others; and investigators being used by informants to eliminate criminal competitors or to commit additional crimes. Indeed, “working with CIs can be a blessing and a curse for law enforcement agencies and officers.”\textsuperscript{40} The problems and controversies of using informants as a source of information in investigations can be lessened by appropriate policies and procedures, including written guidelines, criteria for CI selection and evaluation, and investigator training on the use and management of CIs\textsuperscript{41} (see Exhibit 9.2).

**Gang Intelligence**

**WHAT IS A GANG?**

There is no single agreed-upon definition of a gang, partially because there are many different types of gangs. The most important gangs from a law enforcement perspective are street gangs and outlaw motorcycle gangs (OMGs). Regardless of the type, gangs have several features in common:\textsuperscript{42}

- They are a group.
- They use symbols, including clothing style, clothing color, and/or hand signs.
- They have forms of communication, such as graffiti and social media.
- The group has permanence.
- The group may have a street orientation (but not always).
- The group is involved in crime, especially drug use, drug dealing, gun ownership and gun carrying, and serious violence.

---

**EXHIBIT 9.2**

**Tips for Handling Informants\textsuperscript{43}**

- Maintain control of the informant and the case; the investigator is in charge, not the informant.
- Limit the informant’s exposure to other undercover officers and share only necessary information with the informant. The informant may be the subject of an investigation in the future, so he or she should not know too much.
- Maintain the informant’s confidentiality when promised; the success of the case and the informant’s safety may depend on it.
- Only make promises to the informant that can be kept.
- Informants should be treated with respect, but the relationship should remain professional.
- Meetings with informants should be with two officers, for safety reasons as well as to guard against allegations of officer misconduct.
- If the informant is to be paid, he or she should receive payment as soon as the agreement has been fulfilled. Payment should be documented and managed.
- Informants should be used and managed in accordance with agency policy.
Although gangs are by definition heavily involved in criminal behavior, their orientation, structure, and operations vary. Some gangs are very tightly organized with a clear chain of command; some are loosely organized. Some gangs are oriented exclusively to drug sales; others are involved in not only drug sales but a wide range of other illegal activity, such as human trafficking, immigrant smuggling, and prostitution, as well. Some gangs are oriented toward turf; others are oriented more toward profit.

**STREET GANGS**

With regard to street gangs specifically, according to the National Gang Threat Assessment released by the National Gang Intelligence Center (NGIC):

- Street gangs are criminal organizations that formed on the street and operate in neighborhoods throughout the United States. Neighborhood-based gangs are confined to specific neighborhoods and jurisdictions, with no known leadership beyond their communities. National-level gangs have a presence in multiple jurisdictions.44

- Street gang activity continues to be oriented toward violent crimes, such as assault, drug trafficking, home invasions, homicide, intimidation, threats, weapons trafficking, and sex trafficking. Respondents report the most prevalent gang-related criminal activities are street-level drug trafficking, assault, threats and intimidation, robbery, and large-scale drug trafficking.45 Drug involvement most often relates to methamphetamine, cocaine, and heroin.46

- A large portion (50 to 90 percent) of violent crimes that occur in large, medium, and even small cities can be attributed to street gangs.47

- Recent reporting indicates that gangs are becoming bolder in both their threats and actions toward law enforcement. Approximately one-third of jurisdictions report an increase in threats to law enforcement. However, the actual number of attacks against law enforcement has remained relatively stable.48

- Gang use of technology and social media has significantly increased over the past two years. Widely used social media platforms, such as Facebook and YouTube, have become ubiquitous in gang activity. According to survey respondents, the most common social media platforms that street gangs use are Facebook, YouTube, Instagram, and Twitter. They use various sites for recruitment, communication, targeting rivals, advancing criminal activities, and thwarting law enforcement.49

Street gangs vary by city (e.g., the gangs in Chicago are not the same as the ones in Los Angeles), within states (e.g., the gangs in northern California are not the same as the ones in southern California), and by geographical region (e.g., gangs on the East Coast are not the same as the ones on the West Coast). Gangs are also most often differentiated by race or members’ country of origin. For example, Gangster Disciples, Bloods, and Crips are primarily African American gangs; Mexican Posse is a Hispanic gang; Asian Boyz is an Asian gang; the Trinitarios is a Dominican gang; and the Juggalos is a primarily Caucasian gang. Law enforcement experiences with gangs will also vary considerably across communities.

Street gangs often use identifiers of colors and symbols. This is actually not unlike your college or university, which also uses colors and symbols. For example, my university, the University of Wisconsin–Milwaukee, has gold and black colors, a panther is the school mascot, and it is known as UWM. Gang colors are often worn by members, and symbols often show up in graffiti, tattoos, and hand signs (e.g., “throwing” a sign). All these signals can be useful in the identification of gang members and activities (see Exhibit 9.3).

Because street gang members can be identified on the basis of their colors, tattoos, and hand signs, some gangs have stopped using these indicators. Some gang members have formed
EXHIBIT 9.3

The Basics of Gang Graffiti

Graffiti is a method of communicating in the world of gangs. Some people post an ad in the newspaper or post status updates on Facebook; gangs write graffiti on walls, street signs, and buildings. Graffiti is most often used to mark gang territory and to communicate with other gangs—or even the police. Graffiti is an indicator of disorder in an area and, as such, can have many negative effects on a neighborhood and its residents. Graffiti should be removed as quickly as possible or more is sure to appear. Not all graffiti is the work of gangs. Tagging appears more as colorful art in the form of words or names and most often consists of “bubble” letters. Sometimes those responsible for this form of graffiti refer to it as street art. This graffiti is not likely to be gang related. Gang graffiti is generally less artistic. It is more likely to be in the form of code, such as a series of letters that do not form a word; to be in only one color of paint; to be written with “stick” letters and numbers; and to include other symbols (e.g., pitchforks, stars, etc.).

Gang graffiti comes in many varieties and has many meanings. Entire books and training seminars are devoted to the topic. Discussed here are a few of the basics. Two-digit numbers most often indicate a Hispanic gang, especially 13 and 14. Other gangs are most often represented with letters or abbreviations (e.g., GD for Gangster Disciples, VL for Vice Lords, B for Bloods, C for Crips). F most often indicates “folks,” and P indicates “people” (most street gangs are affiliated with one or the other larger groups). Three-digit numbers most often refer to an area code in which the gang operates, although it can have other meanings as well. The letter K stands for “kill” and is a threat to what comes before or after it. Similarly, crossed-out letters also indicate a threat to kill. The letters N, S, E, and W most often refer to directions and indicators as to the territory of the gang. A usually stands for “almighty,” N for “nation”—standard add-ons without too much meaning. Of course, the specific types of graffiti present in a particular community will depend on the gangs active in that community.

PHOTO 9.9: Citizens often confuse tagger graffiti with gang graffiti. Shown here is gang graffiti.

Hybrid gangs (gangs with multiple affiliations, a loose structure, and/or members with multiple ethnicities) to avoid police scrutiny and make it more difficult to identify and monitor their activities. Many gangs are becoming involved in more sophisticated crimes, including identity theft, computer hacking, and currency counterfeiting. They are also becoming more and more technologically savvy, using social media (especially Facebook and YouTube) for communication, gang promotion, and threats. These facts clearly underscore the need for investigations to include social networking and other Internet sites as a source of information in gang investigations.

OUTLAW MOTORCYCLE GANGS

With regard to outlaw motorcycle gangs (OMGs), according to the National Gang Threat Assessment released by the NGIC:

- OMGs are ongoing organizations, associations, or groups of three or more persons with a common interest or activity characterized by the
commission of or involvement in a pattern of criminal conduct. Members must possess and be able to operate a motorcycle to achieve and maintain membership within the group.\textsuperscript{51}

- The Hells Angels Motorcycle Club, Pagans, Vagos, Sons of Silence, Outlaws, Bandidos, and Mongols are the largest OMGs.\textsuperscript{52}

- OMGs engage primarily in violent crimes, such as assault, robbery, and homicide. According to (law enforcement agency) survey respondents, weapons possession, threats and intimidation, assault, and drug trafficking were the most common criminal activities committed by OMGs over the past two years. The assaults and robberies were often directed at rival gangs or individuals involved in other criminal activities like drug trafficking. Methamphetamine, cocaine, and marijuana ranked respectively as the top three drugs that led to OMG arrests over the past two years.\textsuperscript{53}

INVESTIGATIVE RESPONSE TO GANGS

Given the involvement of gangs in crime, it is necessary for investigators to understand the operations and workings of gangs in their communities. Many large police departments have a specialized gang unit designed to collect and act upon gang information, especially that of street gangs. This information (or, as it is often called, intelligence) can be obtained from a variety of sources, including citizens, informants, the offenders themselves, and officers on the street. In many instances the information can be stored electronically and can be a useful source of potential leads in investigations. As explained by the NGIC,

...gang units and task forces are a vital component in targeting gangs and have played a substantial role in mitigating gang activity in a number of U.S. communities. The majority of NGIC law enforcement partners report that their agency has or participates in a gang task force, and most utilize a gang database to track and monitor gang members in their jurisdictions.\textsuperscript{54}

Gang databases are designed to compile, store, categorize, and retrieve information on suspected gang members. They can store various types of information on subjects, including demographic data, physical characteristics, gang affiliation, criminal history, aliases, vehicles, and addresses and phone numbers associated with subjects. Pictures of subjects can also be included in the database. Searches of the database can be made on any of these dimensions. A specific example of a gang intelligence database is CALGANG, operated by the State of California. CALGANG contains information on gang affiliations, gang tattoos, involvement in criminal activity, and associates/friends of subjects.\textsuperscript{55} The most significant criticism of the use of gang intelligence databases centers on the criteria by which people are defined as gang members and included in the database.\textsuperscript{56} If it is difficult to define a gang, it is also difficult to define a gang member and a gang crime.

Information Networks

A multitude of electronic information databases exist that investigators may use to obtain critical information needed during a criminal investigation. These databases can be classified as either intradepartmental or interdepartmental.

INTRADEPARTMENTAL AND REGIONAL DATABASES

Intradepartmental databases are ones that are operated and maintained by individual law enforcement agencies. Depending on the resources available and the size of the agency,
there may be many such systems available to investigators. For example, some police departments keep electronic files on all individuals with whom the police have had contact (e.g., as victims, complainants, witnesses, suspects, etc.). This information may be useful in developing a police contact history of individuals. As another example, investigators may have access to information about secondhand transactions made at pawnshops, jewelry stores, or other retail outlets. Depending on the state and jurisdiction, operators of these stores may be required to collect information from subjects who wish to sell merchandise to them. The store verifies and records the identity and address of the seller and photographs the property involved in the transaction. This information is then entered into an electronic network that can be searched by law enforcement personnel using key word descriptors (e.g., “palm tree pendant”) and time frame. Such systems are particularly useful in burglary and robbery investigations.

INTERDEPARTMENTAL DATABASES
The two largest and most commonly used interdepartmental databases are the NCIC and the NLETS. These and several other databases are discussed here.

NATIONAL CRIME INFORMATION CENTER (NCIC)
The National Crime Information Center (NCIC) is the largest and most well-known crime information network system in the United States. It consists of a centralized database and a network of connecting computers. It is maintained by the FBI at its headquarters in Washington, D.C. The NCIC began operations in 1967; by 1971 police agencies in all fifty states were linked to the system. Today, more than 80,000 law enforcement and criminal justice agencies have access to the NCIC database. The system contains more than thirty-four million records (including criminal history records contained in the Interstate Identification Index). Nearly two million queries are made of the system daily.

Representatives of agencies may enter information into the database and make queries of the database. The originating agency also has the responsibility for removing records once the information is no longer valid. According to the FBI’s NCIC Web site, the system contains information in several different files, listed here:

- **Article File**—Records on stolen articles and lost public safety, homeland security, and critical infrastructure identification
- **Gun File**—Records on stolen, lost, and recovered weapons and weapons used in the commission of crimes that are designated to expel a projectile by air, carbon dioxide, or explosive action
- **Boat File**—Records on stolen boats
- **Securities File**—Records on serially numbered stolen, embezzled, used for ransom, or counterfeit securities
- **Vehicle File**—Records on stolen vehicles, vehicles involved in the commission of crimes, or vehicles that may be seized based on federally issued court order
- **Vehicle and Boat Parts File**—Records on serially numbered stolen vehicle or boat parts
- **License Plate File**—Records on stolen license plates
- **Missing Persons File**—Records on individuals, including children, who have been reported missing to law enforcement and there is a reasonable concern for their safety
- **Foreign Fugitive File**—Records on persons wanted by another country for a crime that would be a felony if it were committed in the United States
- **Identity Theft File**—Records containing descriptive and other information that law enforcement personnel can use to determine if an individual is a victim of identity theft if the individual might be using a false identity
- **Immigration Violator File**—Records on criminal aliens whom immigration authorities have deported and aliens with outstanding administrative warrants of removal

Copyright ©2019 by SAGE Publications, Inc.
This work may not be reproduced or distributed in any form or by any means without express written permission of the publisher.
- **Protection Order File**—Records on individuals against whom protection orders have been issued
- **Supervised Release File**—Records on individuals on probation, parole, or supervised release or released on their own recognizance or during pre-trial sentencing
- **Unidentified Persons File**—Records on unidentified deceased persons, living persons who are unable to verify their identities, unidentified victims of catastrophes, and recovered body parts; cross-references unidentified bodies against records in the Missing Persons File
- **Protective Interest**—Records on individuals who might pose a threat to the physical safety of protectees or their immediate families; expands on the U.S. Secret Service Protective File, originally created in 1983
- **Gang File**—Records on violent gangs and their members
- **Known or Appropriately Suspected Terrorist File**—Records on known or appropriately suspected terrorists
- **Wanted Persons File**—Records on individuals (including juveniles who will be tried as adults) for whom a federal warrant or a felony or misdemeanor warrant is outstanding
- **National Sex Offender Registry File**—Records on individuals who are required to register in a jurisdiction’s sex offender registry
- **National Instant Criminal Background Check System (NICS) Denied Transaction File**—Records on individuals who have been determined to be “prohibited persons” according to the Brady Handgun Violence Prevention Act and were denied as a result of a NICS background check (as of August 2012, records include last six months of denied transactions; in the future, records will include all denials.)
- **Violent Person File**—Once fully populated with data from (NCIC) users, this file will contain records of persons with a violent criminal history and persons who have previously threatened law enforcement.

The NCIC has the capability of quickly putting vast amounts of critical information in the hands of police and investigators; therefore, it can be a powerful investigative tool. The list of instances in which NCIC information led to the apprehension of offenders, the discovery of missing persons, and the recovery of property is a long one. As just one example, consider the apprehension of Timothy McVeigh, who was responsible for the bombing of the federal building in Oklahoma City (see Chapter 1). Once investigators had developed McVeigh as a suspect in the bombing, they entered his name in the NCIC database and learned that an Oklahoma state trooper had also just run an NCIC search on him. A telephone call to this agency revealed that McVeigh was stopped on the highway and was currently in custody of the police. Only as a result of the NCIC was such a quick apprehension possible.

**NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (NLETS)**

The National Law Enforcement Telecommunications System (NLETS) is a network that links law enforcement agencies, other criminal justice agencies in the United States, and motor vehicle and licensing departments. The information available through the system includes the following:

- Vehicle registrations by license or VIN
- Driver’s license and driving record by name and birth date or driver’s license number
- Criminal history records by name and birth date
- Boat registration information
- Snowmobile registration information
- Hazardous material file data
- Private aircraft data, including registration information
- Index to parole/probation and corrections information
- Sex offender registration information

---

National Law Enforcement Telecommunications System (NLETS):

A national crime information network that contains information on vehicle registrations, criminal records, and sex offender registrations as well as other information.
INTERPOL CASE TRACKING SYSTEM (ICTS)
The ICTS contains information about persons, property, and organizations involved in international criminal activity.

CENTRAL INDEX SYSTEM (CIS) AND RELATED DATABASES
The CIS is operated and maintained by the Bureau of U.S. Citizenship and Immigration Services (USCIS). It contains information on legal immigrants, naturalized citizens, and aliens who have been formally deported or excluded from the United States. The Nonimmigrant Information System of the USCIS contains information on the entry and departure of nonimmigrants (aliens) in the United States for a temporary stay. The Law Enforcement Support Center is also operated by the USCIS and provides information to local, state, and federal law enforcement agencies about aliens who have been arrested. The National Alien Information Lookout System consists of a USCIS index of names of individuals who may be excludable from the United States. The Consular Lookout and Support System is a related database operated by the U.S. Department of State. It contains information on several million individuals who have been determined to be ineligible for visas, those who need additional investigation prior to issuance of a visa, and those who would be ineligible for visas should they apply for one.

EL PASO INTELLIGENCE CENTER (EPIC)
EPIC is designed to collect, process, and disseminate information concerning illegal drug use, alien smuggling, weapons trafficking, and related criminal activity. EPIC was established to facilitate the exchange of information across agencies responsible for the enforcement of drug and related laws.

SENTRY
Sentry is operated by the Federal Bureau of Prisons and contains information on all federal prisoners incarcerated since 1980. The available information includes an inmate’s physical description, location, release information, custody classification, and sentencing information, among other items.

EQUIFAX AND TRANSUNION
Equifax is a company that provides credit information on individuals. Databases within its operation may be used to collect various information on people, including recent addresses and demographic information. TransUnion is another consumer credit information company that offers background information, spending activity, and employment information on individuals.

OTHER DATABASES
In addition to these databases, numerous other sources of public information (open sources) may be useful to investigators. These sources are diverse, and their particular usefulness depends heavily on the issue at hand. These sources include the following:

- Motor vehicle registrations (e.g., useful when constructing a list of all vehicles registered in a particular area that match a particular description)
- License plate reader (LPR) data (e.g., to determine vehicle presence in particular areas)
- Credit card receipts and information (e.g., to document purchases and travel)
- Bank and financial records (e.g., to verify unusual deposits and withdrawals)
- Attendance records at school or work (e.g., to verify a suspect’s alibi or to
help verify when a victim was last seen)

- Reverse telephone directories (e.g., to determine a phone number from a known address)
- Other telephone records (e.g., to verify phone calls made and received and the timing of those calls)
- Sex offender registries and related Department of Corrections information (e.g., to determine the whereabouts of particular offenders or to identify offenders who live in a particular area)

LIMITATIONS

The primary limitation of information databases is that the database is only as good as the information it contains. If information is not entered into the system—for example, in the case of the NCIC, if a gun is not reported as stolen or a missing person is not entered as missing—the database will be of little use to the police in this regard. Similarly, if a person has not been identified as “wanted” in a particular crime, the information contained in the database will not provide the information necessary to make an apprehension. For example, as discussed in the introduction to this chapter, Tamerlan Tsarnaev was on a national terrorism database watch list, but this information was of no use in the prevention of the bombings or in his identification.

Information from Electronic Devices and Digital Evidence

Digital evidence is “information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.” Today, cell phones are the most common source of digital evidence; in fact, there is seldom a major investigation that does not include a search for information from a cell phone. Text conversations, records of phone calls, photographs, and video are especially useful evidence that can be obtained from cell phones. Other devices, such as desktop, laptop, and tablet computers; GPS devices; digital cameras; video cameras; surveillance equipment; computer servers; video game systems; external hard drives; and other storage devices (e.g., thumb drives), may also contain digital evidence. These devices serve as electronic filing cabinets that may contain evidence related to various types of crimes. In this era of information and computerization, many of our daily activities are in some way recorded digitally—where we went, when we went there, what we did when we got there, who we spoke with, and what we said. This applies to criminals as well, except with criminals this information may constitute evidence. Given the proliferation of electronic devices, it is not an exaggeration to say that nearly every crime could have digital evidence associated with it. Sometimes digital evidence is the primary evidence in a criminal investigation (see Case in Point 9.5).

In some investigations the objective is to confirm a link between a particular device and an Internet site or server (see Case in Point 9.6). In these cases the record of devices that accessed the site or server is analyzed. A linkage between Internet sites and computers is most often done through the identification of an Internet Protocol (IP) address. An IP address is an identifying number associated with a computer or other device that can access the Internet. However, there is much variation in the assignment of IP addresses: IP addresses on computers can change (dynamic), remain the same (static), or be shared by several computers. An IP address can be potentially useful for criminal investigation purposes because it can be obtained from a Web site that maintains a log of IP addresses that accessed that site. When an IP address is in hand, that address can be linked to the Internet service provider (ISP) connecting that computer to the Internet. That ISP can then provide
From the billing name and address associated with the IP address. In this way the identification of an IP address may lead to the name and address of a person who controls or uses a certain computer.

In some investigations the objective is to track or locate a device, usually a cell phone. This is most common when attempting to locate a missing person or monitoring the movements of a subject (see Case in Point 9.7). There are several technologies that can be used for this purpose, the most well-known of which is Stingray (many cell phone tracking devices are now often simply referred to as Stingray). The device sends a signal that tricks the phone to connect to it. Phones can be identified by unique codes, such as the international mobile subscriber number (IMSI) and the electronic serial number (ESN). Cell phone service providers may also provide location information on devices for criminal investigation purposes. Cell phones can also be traced via phone-finding apps.

### CASE in POINT 9.5 “She Is So Raped”

Text messages and cell phone photos and video played a critical role in the 2013 conviction of two high school football players, Trent Mays and Ma’lik Richmond, in Ohio for the crime of rape. Mays and Richmond were found guilty of raping an intoxicated sixteen-year-old girl at party. A critical issue at the trial was that the girl was too intoxicated to consent or resist. The text messages, video, and photos spoke directly to these issue.

The crime was first brought to the attention of authorities by the victim’s parents, who learned that a video making fun of the girl and her assault had been posted on YouTube by some of the teens who attended the party. In that video the victim was referred to as “the dead girl,” and one attendee commented, “She is so raped.” A photo showing the two defendants carrying the girl out of a house by her arms and legs was posted on Instagram. Subsequent to these discoveries, cell phones from seventeen of the teens were seized by the police. Approximately 350,000 text messages were recovered from the phones and analyzed, as were hundreds of thousands of photos, videos, tweets, and other posts. As reported in the media, some of the text conversations recovered from Mays’s phone included the following:

**From the victim’s phone to a friend:**

**Victim:** What the fuck? Who was there? What happened to me?

**Victim:** I swear to God I don’t remember anything. I remember at one point hearing Trent telling me to do something, but I said no.

Later, the victim texted Mays:

**Victim:** Ok, tell me right now what the fuck happened last night and don’t lie to me. We need to talk about this right now.

**Mays:** Nothing happen last night. You [sexual act] last night and that’s it.

**Victim:** Ok, that’s not all that happened. Tell me the truth now.

Later, the victim e-mailed Mays:

**Victim:** Why the fuck would you let that happen to me? Seriously, you have no fuckin respect.

Later, Mays texted a friend:

**Mays:** Dude, I’m so fuckin scared. Her dad knows where we brought her. If we are questioned, just say she was really drunk and we were trying to keep her safe.

It was only as a result of these text messages that investigators were able to reconstruct the past and determine, at the very least, what the participants were saying about the incident prior to the involvement of the police.
In other investigations the objective is to document the content of electronic devices (e.g., Internet sites accessed, text messages sent and received). In cases like this, the content of the device is analyzed (see Case in Point 9.5 and Case in Point 9.7). The method used to obtain digital content from a device depend a great deal on the type of device in question. As noted in Case in Point 9.7, a commonly used machine for this purpose is known as Cellebrite. Cellebrite is a particular brand of a device that can extract data from a phone’s memory, even if that data have been deleted. The cell phone is attached to a computer, and data from the phone are transferred to the computer. The machine can bypass the security codes on most phone models used today. Other methods and machines can be used to obtain information from cloud-based sources, such as Web mail and social media sites.

**SEIZING ELECTRONIC DEVICES AND COMPUTER DATA EXTRACTION**

Regardless of the device, there must be a legal basis for the collection of electronic equipment and the search for digital evidence. There is not a digital evidence exception to the search warrant requirement. Electronic devices are normally seized either as a result of consent, plain view, or the execution of a search warrant.

The place where the electronic item is located should be treated as a crime scene. As such, appropriate precautions and security measures as well as documentation of the scene are

**CASE in POINT 9.6**

**A Killer Identified via an IP Address**

Stephanie Renee Bennett, twenty-three, was found dead in her apartment in northwest Raleigh, North Carolina. She had been sexually assaulted and murdered. Stephanie had lived in the apartment for about ten months with two female roommates, one of whom was her stepsister. Stephanie’s stepsister had asked the apartment manager to enter the apartment to check on the well-being of Stephanie as she could not be contacted. Stephanie was discovered deceased.

Evidence indicated the perpetrator had entered the apartment by removing the screen to an unlocked window in one of the unoccupied bedrooms. Stephanie was found nude, lying on her back, with her legs open and her head tilted to one side. In her mouth was a gag (a pair of panties that belonged to one of her roommates). Visual marks on Stephanie’s wrist and ankles were attributed to a form of restraint used by the offender to immobilize her. A well-defined ligature injury mark encompassed Stephanie’s neck, and several marks at the rear base of her neck gave the appearance that a garrotte-type device was used in conjunction with the ligature. The restraints and ligature had been removed by the offender and taken with him when he left the crime scene. An autopsy report disclosed that Stephanie had been sexually assaulted orally, anally, and vaginally. DNA from the unidentified offender was profiled but no hit was obtained through CODIS.

Approximately three and a half years after Stephanie was murdered, Drew Planten, thirty-five, was arrested in connection with her sexual assault and murder. At the time of the crime, Planten was living in the apartment complex located next to Stephanie’s. Two years after the murder, residents reported to the police that Planten possibly matched the description of a Peeping Tom seen near Stephanie’s apartment weeks before her death. But Planten was just one of many suspects in the investigation. In an attempt to identify the perpetrator, or at least develop leads on the cold case, investigators set up a Web site, www.StephanieBennett.com, and monitored who visited the site. One of the computers that accessed the site (determined by the IP address) was located at the North Carolina Department of Agriculture. This computer was used by Drew Planten, a chemist who worked there. Authorities already knew of Planten from the earlier identification. Authorities obtained a pair of gloves that Planten used at work (taken by a coworker and given to the police), and from the gloves they obtained a DNA profile. It matched the DNA profile taken from Stephanie. Investigators obtained a search warrant of Planten’s premises and recovered numerous items, including property taken from Stephanie’s apartment and a large collection of guns and pornography. One of the guns seized was linked to the unsolved homicide of a young woman in Michigan several years prior. While awaiting trial for the murder of Stephanie, Planten committed suicide in jail.
In a 2016 case, a thirteen-year-old girl (referred to as “NC” here) was reported missing from her home. Her mother believed she might have run away. The window screen in NC’s bedroom had been cut; outside the house, a single set of footprints led away from the window. NC’s mother provided a description of NC and turned over NC’s cell phone to the police. Investigators contacted NC’s friends and learned they believed NC had been communicating with a male subject on the Internet site Kik while at a sleepover the previous night.

To hopefully learn more about NC’s whereabouts, data was extracted from her phone. As written in the police report:

The following programs were used during the acquisition and exam of the Apple iPhone 5s device.

– Cellebrite UFED 4PC [Version 4.5.0.307]
– Cellebrite UFED Physical Analyzer [Version 4.5.1.14]

I began by removing the SIM card from the side of the Apple iPhone 5s. Using a Cellebrite provided nano SIM card reader, I connected the iPhone’s nano SIM card to the GLPD Forensic Computer and obtained a Logical Extraction at 10:10AM on Sunday, 01/31/2016. The SIM card extraction indicated the following information: ICCID: 89168000001510417161; TIMSI: 62238305.

Using the same above Cellebrite provided hardware and software, I connected a blank Cellebrite provided nano SIM card to the GPD Forensic Computer and obtained a Logical Extraction at 10:16AM on Sunday, 01/31/2016. The SIM card extraction indicated the following information: ICCID: 89168000001510417161; TIMSI: 62238305.

I then powered the iPhone 5s ‘on.’ I immediately placed the iPhone into ‘Airplane Mode,’ which disables all forms of wireless communication with the device. Using a Cellebrite provided #210 cable, I connected the above described iPhone to the GPD Forensic Computer and obtained an Advanced Logical Extraction at 10:16AM on Sunday, 01/31/2016.

After completing the above extraction, the iPhone was powered back ‘off.’ The cloned Cellebrite nano SIM card was removed from the device and the original was re-inserted.

Upon searching NC’s phone, the investigator located a note on the phone that read simply, “Shado.g009.” This was believed to be a username. Investigators searched for this name on the Kik Web site and found a matching account. The profile photo for that account was a picture of NC. Investigators then learned that NC might be in possession of another cell phone, one that she might have stolen from a classmate at school.

Investigators obtained an emergency locate order for the stolen phone through the cell phone provider. The track indicated the phone was located at or near the northeast corner of the Bayview Mall, which was in a suburb of the city where NC lived. Investigators found a 2009 Ford Focus at that location. As investigators approached the vehicle, a person known to be NC exited the vehicle, as did another subject later identified as Ethan Harold [not his real name]. Both subjects were detained. Inside the vehicle the investigators found a phone matching the description of the one that was reported stolen and that was being tracked by the cell phone provider. That phone was seized.

When questioning Harold at the scene, he stated that NC was his girlfriend and he had met her on Kik. He stated that he had met NC in person for the first time that morning and they had agreed to meet at the mall. He stated that he believed NC was eighteen and that he had not had sexual intercourse with her. NC also told investigators that they did not have sexual intercourse. When Harold was asked if he had communicated with NC via his phone, he stated that he had. Investigators then seized his phone. He was asked for consent to search the phone and told if he refused a search warrant would be obtained. Harold signed the waiver allowing the police to search his phone. He was released but advised he might face charges in the future as a result of the ongoing investigation.

NC was transported to the police department and interviewed, and her parents were notified. During the interview NC stated that Harold had picked her up at her house and that she had been staying with him since she ran away from
home. She denied that she and Harold had engaged in any sexual contact and said she did not need medical care. NC was then released to her parents.

The subsequent forensic exam of the stolen phone in possession of NC revealed the following:

There were 3,565 images on the phone. Many of the images were related to exchanges on Kik, including naked photos sent by NC and naked photos sent by numerous other people to NC’s Kik account. These photos exchanges were the result of “conversations” NC was having with other Kik users of a sexual nature that led to them asking NC for photos or to NC asking them for photos. There was nothing found in the context of the exchanges to indicate other users having any knowledge of NC’s age.

Located among the Kik conversations was one between NC and Ethan Harold. This conversation was about meeting somewhere to have sex in his car. The last conversation discovered on the phone between NC and Harold was Harold’s statement, “Hey Hun, I’m being real with you. You might want to get yourself checked out because my dick hurts really fucking bad. I’m going to get tested.” Investigators reasoned that this conversation was a reference to Harold being concerned about having a sexually transmitted disease and him advising NC of that possibility, presumably because they had engaged in sexual contact.

Forensic examination of Ethan Harold’s phone revealed a Kik conversation between him and NC in which seven images were sent by NC that showed her either naked or partially clothed. These images included an image of NC’s exposed vagina and one with her buttock exposed. Eight images were sent by Harold to NC of his exposed erect penis. In addition, there were 657 images on Harold’s phone, some of which were more nude photos of NC.

Shortly after the discovery of these conversations and images, NC’s mother contacted the police and stated NC had told her that she and Harold actually did have sexual intercourse while in the car parked at the mall. Upon being interviewed again by the police, NC told investigators that she and Ethan had taken off their clothes and had sex in the car at the mall. NC stated that Ethan had laid down on the seat and began kissing her; he then took off his pants and “went inside of” her. NC clarified he put his penis in her vagina and was moving it in and out. NC stated that Ethan’s “bodily fluid” went inside of her and she was then worried she’d be pregnant.

Subsequent to this interview, Harold was again contacted and interviewed. He stated to the investigator that he and NC first met on the OK Cupid Web site but then moved their conversations to Kik. He stated they had exchanged nude photos and that he thought she was eighteen. He denied having sexual intercourse with NC. In light of the evidence retrieved from the phones and the statements made by NC, Harold was arrested and booked for second degree sexual assault of a child and possession of child pornography.

(Continued)
PHOTO 9.10: Some criminals realize cell phones contain incriminating evidence that can be recovered by the police. As a result, it is not uncommon for investigators to discover cell phones that have been destroyed by suspects.

PHOTO 9.11: In this case a cell phone contained evidence of previous threats made by a suspect to his ex-girlfriend.

be touched or moved unless it appears that files are being deleted. In this case the computer should be immediately disconnected from the power source. If the computer is on and not in the process of deleting files, the computer should be turned off but only under the direction of a trained digital evidence expert. If the computer is off it can be unplugged and carefully transported for forensic analysis. Any external storage devices should also be seized.
(e.g., thumb drives, CDs). Although this is standard practice, some data (e.g., recently typed passwords) may be lost when the device is turned off. Investigators should be aware of all possible devices that may contain digital evidence related to the investigation.  

Information from those persons who have access to or ownership of the devices may also be useful in the investigation, and the following information should be collected from them:

- Names of all users of the computers and devices
- All computer and Internet user information
- All login names and user account names
- Purpose and uses of the computers and devices
- All passwords
- Any automated applications in use
- Type of Internet access used
- Any offsite storage
- Internet service provider
- Installed software documentation
- All e-mail accounts
- Security provisions in use
- Web mail account information
- Data access restrictions in place
- All instant messaging screen names
- All destructive devices or software in use
- Social networking Web site account information
- Any other relevant information

The process of extracting data from a computer for forensic analysis is, in many respects, similar (but not exactly the same) as that of extracting data from a cell phone. Although specific details are beyond the scope and purpose of this chapter, understand that the process is technical. Through the use of various forensic data extraction machines, the content of the hard drive in question is copied to a new, blank hard drive. The new hard drive is then examined for evidence. The imaged hard drive can also be examined for files that have been deleted (i.e., latent files). Systems files that were created by the computer operating system are also examined. These files have been described as sort of like a surveillance tape that shows user activity on the computer and files that were changed by the user.

The field of forensic digital evidence has continued to evolve as digital evidence has become relevant in more investigations. It used to be that a police officer with an interest in electronics would be designated as the digital evidence expert in the department. Now the techniques and standards of digital evidence collection have become more rigorous and scientific. Individuals who are designated as digital evidence collection experts should expect to receive considerable training regarding the collection and analysis of the evidence.

Digital evidence has become more and more significant in criminal investigations due to the increased use of digital devices in our daily lives. It has the unique ability to cast light onto past conversations, statements, and behaviors of victims and offenders. Although the presence of digital evidence may not be obvious and its collection is technical, investigators should always be mindful of the possible role it may play in criminal investigations.

### Psychics

When all else fails, when there is nowhere else to turn, when the police are at a loss regarding what to do next, the police may turn to a psychic for assistance in an investigation. In such a situation, investigators may be trapped between the embarrassment of an unsolved high-profile case and the embarrassment of enlisting the help of a psychic.
Psychic phenomena are related to the science of parapsychology, or extrasensory perception (ESP). There are several forms of ESP, including telepathy (the ability to read minds and transmit thoughts, or thought transference), clairvoyance (the ability to see objects and events beyond the range of physical vision), precognition (the ability to perceive future events), and retrocognition (the ability to see into the past). These phenomena have been studied at length; in fact, there is even a scholarly journal devoted to the study of such phenomena, the Journal of Parapsychology. Although there is a paucity of scientific research that documents and verifies the existence of ESP, much anecdotal evidence exists that some people have such abilities. Indeed, you may believe that you have experienced ESP at some time (or perhaps all the time). If this is the case, you are not alone. Sixty-seven percent of adult Americans have said they have experienced ESP on at least one occasion.67

During the past several decades, there have been a number of stories about psychics assisting in criminal investigations; even today there is occasional reference to “psychic detectives.” However, no empirical studies have demonstrated the usefulness or validity of psychic information in criminal investigations.

Although it is possible that certain people may have psychic abilities at certain times and under certain circumstances, there are undoubtedly many pretenders. With regard to the value of psychics in criminal investigations in particular, one must consider the number of details provided by the psychic in relation to the number of accurate details and the usefulness of those details in advancing the investigation. The problem is that numerous details may be provided and, at best, only a few (if any) may be accurate. Even the information that is accurate may not provide sufficiently specific leads for the police to pursue.

**MAIN POINTS**

1. The police have several strategies by which to find people who have information about crimes. These include the use of tip lines, television shows, special alerts (e.g., AMBER Alerts), and other public information strategies, including the use of billboards, YouTube, and other advertising campaigns.

2. While tip lines, television shows, and alerts can assist in investigations, they are not without limitations. For example, the information provided may be irrelevant, false, or not timely.

3. Social media is a unique and valuable source of information in criminal investigations. Investigators can use social media sites to “push out” information about crimes that have occurred or “pull in” information about the activities, conversations, and whereabouts of suspects in crimes.

4. Confidential informants typically have some connection to or knowledge of the criminal underworld. They most often provide information to the police about ongoing undercover investigations, especially those that are drug related. Although information from informants may be valuable, the use of CIs is not without controversy.

5. Members of street gangs and outlaw motorcycle gangs are disproportionately involved in serious violent crime. Many police departments have a specialized gang unit designed to collect and act upon gang information.

6. Numerous information networks are available for purposes of criminal investigations. These databases may be intradepartmental (e.g., gang intelligence records) or interdepartmental (e.g., the NCIC). Information databases are only as good as the information they contain.

7. Digital evidence from electronic devices is a common and potentially useful form of evidence found in a wide range of criminal investigations. Investigators may seek to locate a device, obtain evidence from a device, or establish a link between a device and an Internet site. Forensic examinations of electronic devices are conducted with the assistance of machines designed for that purpose.
8. Psychic phenomena are related to the science of parapsychology. Although there are stories about the successful use of psychics in criminal investigations, the limited research on the topic does not show psychics to be of use in solving crimes.

**IMPORTANT TERMS**

- AMBER Alert, 242
- Cellebrite, 262
- Code Adam, 246
- Confidential informants, 252
- Digital evidence, 260
- Graffiti, 255
- Internet Protocol (IP) address, 260
- National Crime Information Center (NCIC), 257
- National Law Enforcement Telecommunications System (NLETS), 258
- Outlaw motorcycle gangs (OMGs), 255
- Parapsychology, 267
- Street gang, 254
- Tip lines, 241

**QUESTIONS FOR DISCUSSION AND REVIEW**

1. What are tip lines? What are their major benefits and limitations?

2. What are AMBER Alerts? How are they supposed to work? What are their benefits and limitations?

3. In what ways can social media be used in criminal investigations?

4. What is the role of confidential informants in criminal investigations? Why is the use of CIs sometimes controversial? What are the common motivations of informants?

5. What is a gang? What are some of the basic interpretations of gang graffiti?

6. How can information networks be useful in criminal investigations? What are their limitations?

7. What is digital evidence? Why is it a unique form of evidence in criminal investigations?

8. What are Internet Protocol (IP) addresses? How can they be obtained and used in criminal investigations?

9. What is the value of cell phones in criminal investigations? What types of evidence can be obtained from a cell phone?

10. What are psychics? What value do they add to criminal investigations?
PRACTICE AND APPLY WHAT YOU’VE LEARNED

edge.sagepub.com/brandl4e

CHECK YOUR COMPREHENSION ON THE STUDY SITE WITH:

• eFlashcards to strengthen your understanding of key terms.
• Practice quizzes to test your comprehension of key concepts.
• Videos and multimedia content to enhance your exploration of key topics