Chapter 9
Seizure of Digital Evidence

Chapter Outline

I. Introduction
   A. The Fourth Amendment to the United States Constitution remains the focus of consideration when it comes to determining the admissibility of evidence from high-technology crimes.
II. The Search Warrant Requirements
   A. The Fourth Amendment's protections against unreasonable searches and seizures are designed to protect citizens from aggressive, overreaching, and inappropriate seizures of information and property, including personal computers and Internet Service Providers.
   B. According to Orin Kerr of the Computer Crime Intellectual Property Section of the U.S. Justice Department, the best definition of "unreasonable" requires that for a search to be reasonable you need one thing—a properly drafted search warrant that satisfies the requirements of particularity and scope pertaining to the items to be seized.
   C. There have been few decisions to address the issue when it comes to digital evidence, and the few court decisions that have been provided are from the various lower courts and not from the Supreme Court.
   D. It is recommended that any search warrant involving the seizure of digital evidence be as thorough as possible, and the Fourth Amendment requires a complete analysis and description of the place (or places) to be searched by law enforcement officials.
      1. If an individual is using a computer in the commission of a criminal activity, then there is the possibility that any or all of these devices may be employed in the criminal activity.
      2. What information should law enforcement officers include in their request for a search warrant?
         a. *United States v. Hunter* (1998)—An officer's failure to list specifically all digital evidence that could be encountered at a crime scene resulted in a search warrant that was overly broad and allowed for officers to engage in what is often referred to as a "fishing expedition," wherein officers broadly write the warrant and seize as much as possible in hopes of finding incriminating evidence.
            i. Many manuals or training materials relating to the handling of digital evidence recommend that the proper means of avoiding this problem is to include as many items as possible as well as the following phrase: "including but not limited to," but at least one court has ruled against the use of this phrasing.
            ii. *Matter of Search Warrant for K-Sports Imports, Inc*. (1995)—The use of the phrase "including but not limited to" resulted in the search warrant's violating the particularity requirement of the Fourth Amendment.
            iii. Other courts have upheld search warrants that did not specifically list all potential computer-related evidence.

1. *United States v. Upham* (1999)—The court held that a search warrant calling for the seizure of all computer-related devices was sufficient because such a search would be necessary to ensure that all evidence was properly collected.
2. *United States v. Graziano* (2008—A search of a computer was found to be valid after the search warrant indicated gambling records could be either paper or electronic.
3. *United States v. Alexander* (2009)—The court held that a search of a computer was acceptable even though the search warrant did not list all computer-related storage media.

iv. As the law stands today, it may still be in the best interest of law enforcement officers to list all possible sources of digital evidence and then include a statement concerning how digital evidence may take many forms and there is the potential that the suspect may have additional pieces of technology that were not included.

E. One final issue that must be considered when examining the search warrant requirement is the judge's level of understanding.

i. It is important that law enforcement officers who request a search warrant ensure that the signing judge understands what is being seized, and this can be accomplished by carrying a pocket dictionary of computer terms.

ii. Officers who encounter judges who are not familiar with the latest technological terminology may also find salvation through the good faith clause of the exclusionary rule.

1. This requires that officers prove that they acted upon what they thought to be a valid warrant
2. Proving this may require extra effort that could be avoided through use of the dictionary and planning on the front end of the search.

III. Preplanning Associated with the Search Warrant

A. Search warrants involving digital evidence and computer technology require specific planning.

B. Because there are numerous types of digital evidence that could be desirable evidence, and each may require separate seizure techniques, it is important that all possible seizure scenarios be considered.

C. Another consideration is the number of computers located at the site upon which the search warrant is to be executed.

1. Many times more than one computer will be seized at a time and because each computer on the scene may be running and occupied by a user, law enforcement personnel must take into consideration several additional factors that govern the seizure of these devices.
   a. If there is no plan in place for this scenario, then evidence could be destroyed by personnel onsite before the computer can be seized.

D. The issue of operating systems in use by the computers is an important consideration.

1. The determination of which operating systems the computers are running will guide the investigator's decisions in regard to powering down the computer before disassembly.

E. Another consideration for investigators is whether the actions of their search warrant will affect any federal legislation.
    1. The Electronics Communication Privacy Act (ECPA) of 1986
        a. Regulates the amount of information that law enforcement officers may obtain with certain levels of service.
        b. An officer needs the following level of service to obtain information about a potential suspect under the ECPA:
            i. Subpoena—basic subscriber information
            ii. Court order—transactional information
            iii. Search warrant—the actual content of e-mail messages.
    2. The Privacy Protection Act (PPA)
        a. Originally drafted to protect those who publish books, magazines, etc. from having their materials confiscated and released by law enforcement officers before they are made available to the public.
        b. Today, it is believed by some that the provisions of the Privacy Protection Act may be interpreted to include individuals who write web pages or conduct other web page design work.

F. Investigators must next consider whether there is the presence of a computer network in the building in which they are executing the search warrant.
    1. The presence of a computer network invokes an additional consideration as to where the data is actually being stored because files may be stored on another computer that is generally considered a server.
    2. The presence of servers can be both a positive and a negative event in the investigation of a computer-related crime.
        a. Positive—Many times there are daily, weekly, or monthly backups created for files stored on the servers, which can help investigators find copies of evidence that was destroyed.
        b. Negative—The server may not be included in the warrant or may be located off-site.
    3. A search warrant for computer-related evidence may not include the server in its description of evidence allowed to be seized if investigators are not aware of the presence of an off-site server, and the investigators will be forced to obtain a new search warrant before seizing the server.

IV. Planning for the Seizure of Electronic Communications

A. ECPA regulates the information about an electronic message's owner, as well as information relating to the actual electronic communication.
    1. Designed to protect communications that are sent via electronic methods such as e-mail, wireless telephones, and similar devices.
    2. The ECPA provides for three levels of service:
        a. The subpoena —Can be used to obtain basic subscriber information such as name, address, local and long-distance telephone connection records, session times and duration, length of service, types of services used, telephone number or IP address, sources of payment (to include bank account or credit card information), and the content of e-mails that are older than 180 days and have been previously opened by the owner.
        b. The court order (aka 2703d court order or articulable facts order)—Can be used to obtain information such as past audit trail information and

addresses of past e-mail correspondents; addresses of past e-mail correspondents is of benefit to investigators to determine how many individuals in the public could have been exposed to the individual's behavior.

c. The search warrant—Needed to seize e-mails that are less than 180 days old and are stored on the Internet Service Provider's web server.

d. Each level of process supersedes the lower level, which means that the court order will not only allow for the collection of information requiring a court order but also information that would be obtainable through a subpoena.

e. The search warrant, while allowing for the collection of the most evidence, is also the hardest level of service to obtain; to obtain a search warrant it is necessary for the investigator to complete a statement of the facts that shows that a crime has been committed, that the individual who owns the account is linked to the crime, and that the electronic account contains information relevant to the investigation of the case.

f. Prior to submitting the subpoena, court order, or search warrant, it is customary for investigators to submit a request for the preservation of evidence.

i. This informs the Internet Service Provider that one of their customers is under investigation and that all materials relating to the account should be preserved until a reasonable effort can be made to obtain one of the three levels of legal service.

ii. May request the Internet provider to not alert the suspect for a period of 90 days (which can be extended once for an additional 90 days).

V. Warrantless Search Doctrines and Technological Evidence

A. Should law enforcement personnel determine that the option of using a search warrant is not available, it is up to the government to prove that the circumstances justified a search without a valid warrant.

B. When examining these warrantless search doctrines, it should be noted that the majority of court decisions have allowed the seizure of digital evidence but either have not directly addressed whether an in-depth examination is warranted absent a search warrant or have limited subsequent searches without a warrant.

C. *United States v. Ross* (1982)

1. A person maintains a reasonable Fourth Amendment expectation of privacy in closed containers.
2. Relied upon by some as an indication that computers should be treated as a briefcase or a filing cabinet.

D. *United States v. Blas* (1990) —A pager or any similar electronic device should be treated in a manner comparable to that of a closed container.

E. The Expectation of Privacy

1. The expectation of privacy is central in the acceptance of Fourth Amendment protection.
2. There are certain situations in which an individual's expectation of privacy may

diminish or completely disappear:

a. A person provides a copy of digital evidence to a third party.

b. *United States v. Charbonneau* (1997)—An individual did not maintain his right to privacy in information that was posted to an America Online chat room; the primary consideration by the court was whether a person could maintain an expectation of privacy when there is little or no means of ensuring that the person on the other end of the computer is in fact who they claim to be.

c. *Moreno v. Hanford Sentinel* (2009)—Person loses their expectation of privacy once they post information on a social networking site, regardless of whether the information was publicly available or only available for select friends, the release of the information was considered public in the eyes of the legal system.

F. Warrantless Consent Searches

1. The courts have long held to the belief that a search warrant is not necessary if the owner of property agrees to allow that property to be searched or seized.

2. Several factors to consider when attempting to seize a computer or search a hard drive on the basis of consent:

a. Does the individual granting the consent have a legitimate right to consent to the search?

i. *United States v. Smith* (1998)—A search of a suspect's computer was valid despite the fact that consent was granted not by the suspect but by the suspect's girlfriend.

1. There was evidence that the two individuals shared a common living space and therefore an expectation of privacy in the computer could be overruled by consent from either party.

2. The computer files obtained were not password-protected, a fact that led to the belief that the files were accessible by anyone in the house.

ii. *United States v. Durham* (1998)—The court found that a mother could not grant consent to law enforcement officers for a search of her son's computer.

1. The court relied on two issues in coming to its conclusion

a. Man had taken steps to ensure that neither his mother nor anyone else in the house could access the files on the computer.

b. Son paid a small fee to the mother for living with her, which in the eyes of the court allowed for an expectation of privacy.

iii. So long as the individual lives in the residence, has access to the room in which the computer or technological device is located, and has access to the computer, then the consent search should be lawful.

iv. *United States v. Andrus* (2007)—Ruled that an individual's 91-year-old father granted lawful consent to search his son's computer, despite the fact that the computer was password-protected and the man granting consent did not have the password.

1. Officers did not know about the password, and the obligation was more or less placed on the father to explain that the computer was password-protected and he did not have the password.
2. Readers are cautioned against using such third-party consent because this is still a very uncertain area of search-and-seizure law.

b. Whether the consent to search and seize has been given by one who is both free from duress and aware of what he or she is consenting to be searched.

i. *Schneckloth v. Bustamonte* (1973)—The Supreme court determined that law enforcement officers did not have to inform a suspect of the right to refuse to grant consent.

1. They only had to ensure that the person was mature in age and mental capacity and understood what their consent covered.
2. Some states do go beyond and provide forms to individuals to sign stating they understand their rights and that having given them up will impact them.

ii. If the individual granting consent and the seizing officer do not have the same idea with regard to what is to be searched or seized, there is the potential for the evidence to be excluded.

1. *United States v. Blas* (1990)—The court determined that an officer's request to examine a pager, and the owner's subsequent consent to do so, did not grant the officer the right to search the pager for names or phone numbers.
2. *United States v. Carey* (1999)—The court found that an investigating officer overstepped the bounds of his search when he took a computer off property before he searched the device.

iii. States that do use an informed consent document should ensure that their documents thoroughly address the following components of the search:

1. The area to be searched.
2. What the investigator is intending to search for.
3. The investigator's desire to search within any computer or technological device found within the area.
4. The potential need to make a duplicate copy of the hard

drive (either onsite or offsite).

c. *Georgia v. Randolph* (2005)

i. The issue was whether a wife who had joint access to a residence could grant consent to a warrantless search over the objection of her husband.

ii. It was the opinion of the court that allowing one party to grant consent over the second party's objection would violate the objecting partner's expectation of privacy.

3. Revoking consent

a. Even a written consent form does not prohibit an individual from revoking consent to a search should the individual change his or her mind.

b. Consent may be withdrawn by any of the following:

i. The individual may revoke consent verbally (*State v. Hammonds*, 1990).

ii. The individual may revoke consent through an intentional act such as grabbing the investigator's hand in order to stop the search of a particular area (*Jimenez v. State*, 1994).

iii. The individual may revoke consent to a search by fleeing from the search (*Davis v. State*, 1986).

c. Having a search warrant to search the contents of the computer will prevent a suspect from claiming any of these actions were attempted during the search of the computer.

G. Searches Based on Exigent Circumstances

1. According to *United States v. Reed* (1991), an exigent circumstance falls under the following circumstances:

a. Degree of urgency must be shown.

b. The amount of time it would take to obtain a properly drafted search warrant could prevent the furtherance of justice.

c. Whether the evidence is about to be destroyed or moved beyond the reach of law enforcement.

d. Whether there is danger to the officers, or to the evidence, at the crime scene.

e. Whether the suspect has information that alerts him or her to law enforcement's intent to seize the evidence.

f. How easily the evidence could be destroyed by the suspect.

2. A look at the relationship of exigent circumstances and warrantless seizure of digital evidence is important due to the ease with which data can be moved, hidden, and ultimately deleted.

a. *United States c. David* (1991)—The court stated that:

i. Police officers have the authority to seize evidence (in this case an electronic date book) without a search warrant when a suspect attempts to prevent information from being obtained by deleting it.

ii. Exigency ended the moment the date book was seized because there was no further danger to the integrity of the evidence.

b. *United States v. Ortiz* (1996)—The court found that the warrantless seizure, as well as the subsequent search, was acceptable when phone numbers were retrieved from a pager following the arrest of the suspect.
    i. Pagers and the data located within them are extremely susceptible to deletion and/or damage should the batteries be removed or die.
c. *United States v. Romero-Garcia* (1997)—The court found that a law enforcement officer exceeded his authority when a search was conducted on a battery-operated computer.
    i. When dealing with computers, there is little chance of losing evidence should the batteries die.
d. *State v. Rupnick* (2005)—The court found that the development of probable cause was enough to seize a computer believed to have evidence on it without a warrant, but the search of the hard drive's contents would require a search warrant.
e. *Commonwealth v. Kaupp* (2009)—The court found that requiring officers to stand by a computer and obtain a search warrant was an unnecessary inconvenience when the computer could be seized and then searched later.

B. Search Incident to a Lawful Arrest
1. *United States v. Robinson* (1973)—Supreme Court established that subsequent to a lawful arrest it is allowable for law enforcement personnel to conduct a search of the immediate area surrounding the scene of the arrest; the rationale is that this type of search is necessary to ensure the safety of the officer and citizens.
2. *United States v. Tank* (2000)—The court found that following the arrest of a suspect, officers seizure and search of a zip disk located in the immediate area was valid.
    a. Two potential problems with this ruling:
        i. The court appears to have neglected to consider the original intention of the search-incident-to-arrest doctrine protection because the digital evidence posed little to no physical threat.
        ii. Because the search took place after booking instead of immediately following the arrest when the disk was seized, there appears to be a violation of the section requirement of the search-incident-to-arrest doctrine, which states that searches should be conducted along with the arrest.
3. *United States v. Gant* (2009)—Supreme Court ruled that officers could not search a vehicle incident to arrest once the suspect was placed into custody.
4. *United States v. Finley* (2007)—The court found that a search of a cellular telephone was conducted contemporaneously with the arrest and therefore did not require a search warrant.
5. *United States v. Park* (2007)—The court found that a warrantless search of a

cellular phone was unacceptable given that the search took place two hours after the arrest but prior to the completion of the suspect's booking and arrest.

C. Plain View Seizures

1. In regard to physical-realm searches, the plain view doctrine has been interpreted to allow the warrantless seizure of evidence that comes to the officer's attention without assistance from the officer and while the officer is in a place he or she has a legal right to be.
2. Plain view could be encountered in two different types of scenarios involving technology.
    a. Evidence found during the course of conducting a search in the physical realm.
    b. Evidence found during the course of conducting a forensic analysis search of a computer.
3. *United States v. Carey* (1999)—Court determined that an officer was allowed to seize the initial images of child pornography that were discovered during a search of a computer hard disk for narcotics records, but it limited that seizure to the first images located because additional images were no longer being inadvertently discovered.
4. *United States v. Gray* (1999)—The court ruled in opposition to the *Carey* court by stating that as long as officers conducted searches in the same systematic manner in which he discovered the first image of child pornography, then all subsequent images would have been accepted.
5. *United States v. Maxwell* (1996)—A military court found that the plain view doctrine cannot be used in situations in which an investigator manually opens a file.
6. While at present there is no clear guidance on this issue from the Supreme Court, it would appear that the majority of courts support at least the opening of the first image that is not covered under the original search warrant.
    a. Subsequent images may require an additional search warrant, but the question is whether obtaining a new search warrant would even result in the loss of evidence.
    b. There appears to be little harm in stopping the analysis and obtaining an additional search warrant.

J. Warrantless Searches by a Private Party

1. The Fourth Amendment does not regulate the activities of private citizens when it comes to the search and seizure of property.
2. *United States v. Hall* (1998)—The court found that since a computer repair worker was not acting under color of state law, the Fourth Amendment does not apply to child pornography found during the course of a computer repair and reported to the police.
3. *United States v. Barth* (1998)—The court found that a computer repair worker that is an occasional informant for the police was acting under color of the law when he continued to search a computer after initially finding child pornography and contacting the police.

K. Miscellaneous Warrantless Search Doctrines

1. Seizure of evidence by an employer and the rights of public and private employers.
    a. *O'Connor v. Ortega* (1987)—The Supreme Court determined that while it is not impossible to maintain an expectation of privacy at work, there is a greatly diminished expectation in the workplace.
    b. Each situation will have to be examined based on all the facts surrounding the case.
    c. A person that maintains a locked office away from other employees does have an expectation of privacy.
    d. A person's expectation of privacy does not prohibit searches conducted in furtherance of an investigation related to a violation of an organization's policy or rule.
    e. For searches that do not involve rules and policies of an organization, a policy informing employees about their limited privacy in the workplace can be taken into consideration.
        i. Some companies have attempted to use banners on employee's computers connected to the organization's network that inform them that computer should be used for work purposes only and that they have limited amount of privacy when using work computers.
2. School searches and technology
    a. In the case *New Jersey v. T.L.O.* (1985), the Supreme Court allowed school officials to conduct warrantless searches of students on school grounds if the individual can show that the student in question was either currently, or recently, involved in the commission of a criminal act or an act that was in violation of the school's rules.
    b. Few, if any, cases dealing directly with the seizure of computer-related evidence from a student.
    c. *West Virginia v. Joseph T.* (1985)—Warrantless searches on school grounds required a level of proof so small that reasonable suspicion is sufficient justification.
    d. *Cales v. Howell* (1985)—The level of search must be within reason when considering the particular crime or rule violation.
    e. School searches and high-technology crimes could intersect with the increase of cellular smart phones and laptops used in schools.
    f. Several of the aforementioned areas of warrantless searches could be utilized in conjunction with the diminished privacy expectations in school and allow for a possible search and seizure.

VI. Conclusion

Key Terms

Acceptable use policy: A policy that informs company personnel that they have no privacy interest in the computers on which they perform their job tasks.

Banner: A message that appears to a user when the system is turned on or the computer attempts to connect to an employer's network.

Good faith clause: The requirement of the exclusionary rule that officers must prove that they acted upon what they thought was a valid warrant.

Informed consent document: Form signed by an individual that indicates the person understands what is to be searched and how the search affects him or her.

Plain view doctrine: Allows the warrantless search of evidence that comes to the officer's attention without assistance from the officer and while the officer is in a place he or she has a legal right to be.

Request for preservation of evidence: Informs the Internet Service Provider that one of their customers is under investigation and that all material related to the account should be preserved.

Search incident to a lawful arrest: A search conducted during a lawful arrest to ensure that law enforcement officers, as well as any nearby citizens, are safe.

Server: A computer that is used for nothing more than storing files and applications.