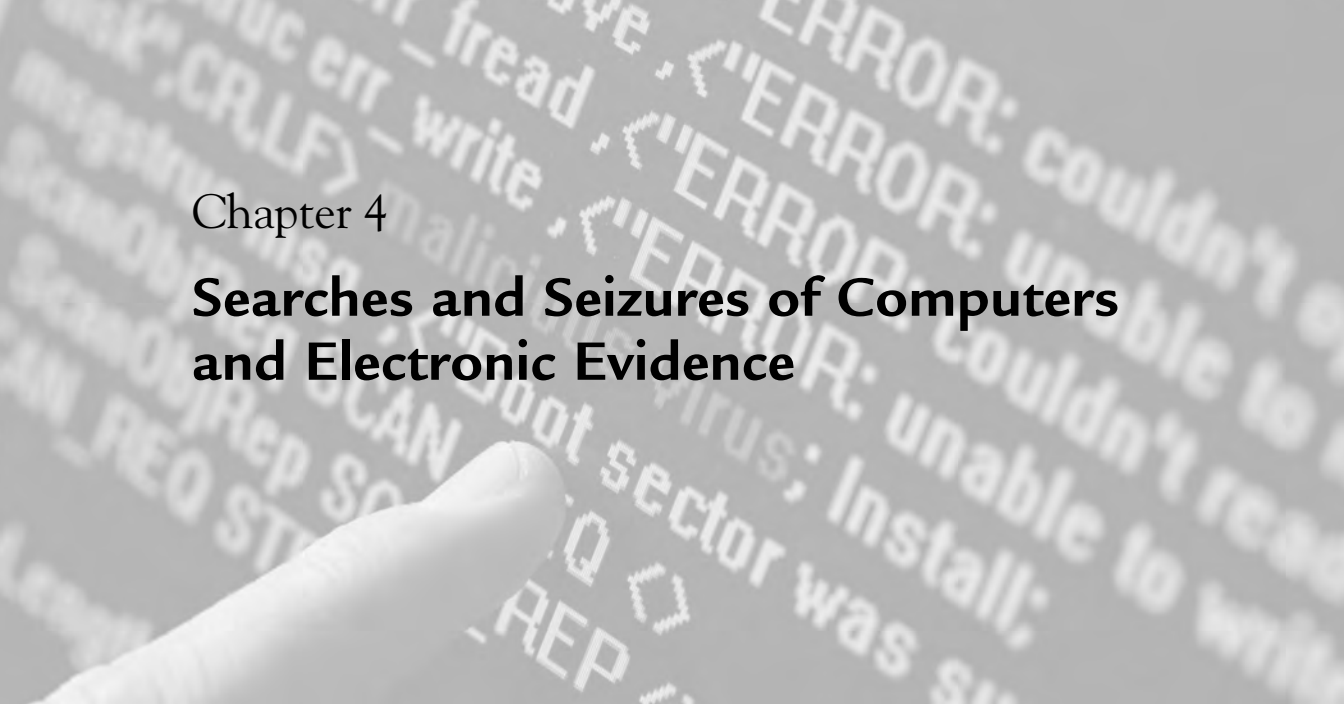

Chapter 4

Searches and Seizures of Computers and Electronic Evidence

This chapter examines the notion of privacy and its importance. In addition, it explores what constitutes a search and seizure in computer forensics investigations, looking in particular at the Fourth Amendment to the U.S. Constitution and the restrictions it places on the **searches and seizures** of computers. Moreover, it considers the various exceptions to the Fourth Amendment related to the search and seizure of computer and electronic evidence. Finally, the chapter analyzes the Fourth Amendment's implications for searching a seized computer for electronic evidence and searching computers that contain privileged material.

What Is Privacy and Why Is It Important?

Privacy is a multivalent social and legal concept, where the definitions of privacy have ranged from the right to be let alone,[1] to the capacity to keep certain things secret,[2] to the right to control other individuals' access to oneself and information about oneself.[3] Despite its complexity and ambiguity, "privacy is closely connected with the emergence of a modern sense of self."[4] The emergence of the modern self, however, depends on individuals' ability to achieve self-determination and develop their personality free from coercion. That is, they must be free to make choices about who they are, who they associate with, and with whom they want to share information.

Choice is a prerequisite for leading a successful, fulfilling, and authentic existence, which requires that an individual must be able to "deliberate about and choose projects he or she will take up in life from an adequate range of options accommodating the diversity of human aptitudes, abilities, interests and tastes."[5] As an autonomous being,

an individual is morally entitled to act in ways, or under conditions, of his or her own choosing, so long as there is no compelling moral reason to override his or her choice.[6] It is the right for an individual to choose for himself or herself—with only extraordinary exceptions being made in the interest of society—when and on which terms his or her actions should be revealed to the general public.[7]

The requirement that individuals should have control over information about themselves is an important aspect of privacy. The deprivation of control over what individuals do and who they are is considered as the "ultimate assault on liberty, personality, and the self."[8] Indeed, self-disclosure is one of the major mechanisms individuals use to regulate their privacy.[9] Privacy, therefore, functions as a means to control "access to information about, or to the intimate aspects, of oneself" by limiting access to information about the individual unless he or she chooses to reveal those details.[10] This notion of privacy reveals its connection to human dignity, to the extent that dignity requires nonexposure.[11] Specifically, certain types of information should be exposed only under conditions of trust, such as intimate details of an individual's private life. An individual's sexual preference is one such example. When intimate details of an individual's private life are collected, stored, and disclosed to others without that person's consent, it is damaging to the individual. The disclosure of this information may trigger emotions such as anxiety, fear, and humiliation. Here, the understanding of privacy is based in the intimate sphere, where invaded privacy can lead to dignitary harms such as exposure and shame.[12] Accordingly, courts have ruled that reasonable suspicion that a crime was committed is required before conducting searches and seizures because they affect the dignity and privacy interests of persons who are subjected to these intrusions.[13]

The right to privacy is the principle that "protects personal writings and any other production of the intellect or of the emotions."[14] Computer and other electronic storage devices are capable of amassing vast amounts of personal information. As Kerr observed, in 2005 alone, the computer hard drives that were sold had approximately 80 gigabytes of storage capacity, which is "roughly the equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library."[15] The storage capabilities of computers and related electronic devices have significantly increased since 2005, of course.

As one court ruling noted, "a laptop and its storage devices have the potential to contain vast amounts of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records."[16] Furthermore, "opening and viewing confidential computer files implicates dignity and privacy interests. Indeed, some may value the sanctity of private thoughts memorialized on a data storage device above physical privacy."[17] As such, the privacy of these files should be afforded protection, because they can provide an enormously detailed account of an individual's private life.

Constitutional Source of Privacy Protection: The Fourth Amendment

The Fourth Amendment of the United States Constitution encompasses an individual's right to privacy. The Fourth Amendment to the U.S. Constitution provides that

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

What You Should Know About the Fourth Amendment

- The Fourth Amendment provides everyone in the United States (e.g., citizens, noncitizens, illegal immigrants, foreign nationals visiting the United States for work or education) with the right to be free from unreasonable searches and seizures.
- The Fourth Amendment does not apply to searches conducted by private individuals, businesses, and nongovernmental agencies; in other words, it applies only if government action is involved. Specifically, the Fourth Amendment is not applicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official."[18] Conversely, private searches may have Fourth Amendment implications if the individual conducting the search is acting as an "instrument" or agent of the government.[19] Private individuals who act to further their own ends and who have not been directed by the government to act in a certain way are not considered to be acting as agents of the government. For instance, a court ruled that a hacker who had provided police with child pornography images that he had found on a suspect's computer was not acting as an agent of the government.[20] Likewise, an individual who lives in a house with a suspect and turns over disks containing child pornography images to the government is not acting as an instrument of the government.[21]
- The Fourth Amendment is enforced with the **exclusionary rule**, which makes evidence that was obtained in violation of the Fourth Amendment generally inadmissible in court.[22] The exclusionary rule seeks to:
  - Deter law enforcement agencies from conducting unreasonable searches and seizures
  - Motivate law enforcement agencies to comply with warrant requirements to ensure the admissibility of this evidence in a court of law
  - Protect individuals from being convicted based on illegally seized evidence

Prior to the decision in *Weeks v. United States*,[23] all evidence was admitted in court, no matter how it was obtained by law enforcement agencies.

Certain exceptions to the exclusionary rule do exist, however. For example, the **inevitable discovery exception** allows evidence that has been illegally obtained to be introduced in court if it would have inevitably been discovered through lawful means. The **good faith exception** holds that illegally seized evidence is admissible in court if a law enforcement agent acted in good faith belief that he or she was acting according to a valid search warrant that is later found defective.[24]

A Reasonable Expectation of Privacy in Communications

In *Katz v. United States*,[25] the court stated that the Fourth Amendment protection applies only to situations where an individual has a subjective expectation of privacy that society willingly recognizes as reasonable.[26] The "reasonable expectation of privacy" test provided by the decision in *Katz* has been used to define what constitutes a "search" under the Fourth Amendment.

In the case of *Katz v. United States*,[27] government agencies monitored the conversations of Katz in a public phone booth. The information retrieved from the communications was then introduced in court as evidence against him. Katz argued that such evidence violated his Fourth Amendment rights. The court agreed. Specifically, it stated that "one who occupies [the phone booth], shuts the door behind him, and pays the toll . . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[28] Accordingly, "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[29] Based on this rationale, Katz had a reasonable expectation of privacy in his communications in the public phone booth.

In contrast, exposure of communications to outsiders provides an indication that this information was not considered private by the individual. The courts have ruled, for example, that individuals do not have a reasonable expectation of privacy in respect to information they post on an online public bulletin board (discussion forum)[30] and in chat room conversations.[31] A case in point is *United States v. Charbonneau*,[32] where the court affirmed that individuals who sent messages to the "public at large" are at risk of having their information read by law enforcement agencies. In particular, the court affirmed that in *Charbonneau,* "when [the defendant] engaged in chat room conversations, he ran the risk of speaking with an undercover agent."[33]

An individual does not have a reasonable expectation of privacy in regard to the messages that he or she transmits to a third party. This applies to e-mails,[34] text messages, and messages sent to pagers. For example, in *United States v. Meriwether*,[35] the court held that an individual had no expectation of privacy for a text message the individual transmitted to a third party's pager.

Expectations of Privacy in the Workplace

Fourth Amendment principles apply to physical searches conducted by government employers in areas in which employees have a reasonable expectation of privacy.[36] Similar considerations espoused in cases involving physical searches have been adapted to employees' expectations of privacy in computer, Internet, e-mail, and text use monitoring by employers.

Consider *K-Mart Corporation Store No. 7441 v. Trotti*.[37] In this case, Trotti, who was an employee of K-Mart, claimed she had a reasonable expectation of privacy in respect to the locker K-Mart had provided so that she could store her personal items. While K-Mart owned the locker, it afforded Trotti (and other employees) with the opportunity to provide their own locks and did not require Trotti (or any other employee for that matter) to provide the combination or a duplicate key to management. The court ruled that Trotti did, indeed, have a reasonable expectation of privacy based on the provision of the lock. Had Trotti purchased her own lock but provided management with the combination or duplicate key to the lock, then she would not have a reasonable expectation of privacy. The same argument could be made about the lockers at schools, gyms, or other establishments.

In *Trotti*, the court also found that the policy on workplace searches was not clear to employees. Many cases have turned to favor the plaintiff who complains of privacy violations when employers have failed to take all necessary steps to inform employees of the search policy of their spaces and computers. That is, clear policies need to be posted in areas where employees can clearly see them; companies also protect themselves when they have employees sign a statement that says that they are aware that their spaces and computers are subject to searches (which is one of the best methods of protecting employers from invasion of privacy lawsuits).

Generally, the courts have determined the expectation of privacy that an individual has based on several factors, including whether an individual reasonably expected that his or her computer files would remain private and whether he or she took steps to conceal them from disclosure.[38] Recall the *Trotti* case. A personal lock she provided on her locker indicated that Trotti had a reasonable expectation of privacy; she was also the only person who had access to her locker. By analogy, a "lock" on computers and computer files should indicate an individual's expectation of privacy in respect to those objects. Indeed, the courts have held that an individual who uses passwords to protect his or her files from disclosure to a third party has a reasonable expectation of privacy in regard to those files.[39] It is important to note that an individual cannot be compelled by authorities to reveal passwords to computers or files.[40] By doing so, the individual may incriminate himself or herself—and the Fifth Amendment to the U.S. Constitution protects individuals against such self-incrimination.[41]

In *United States v. Arnold*,[42] the court found that an individual has a reasonable expectation of privacy for the data and files within a computer or other electronic storage devices where the person has taken steps to conceal the data files from view. For instance,

an individual has a reasonable expectation of privacy relative to files that have been deleted. In fact, in *United States v. Upham*,[43] the court rejected the government's argument that "by deleting the images, [the defendant] 'abandoned' them and surrendered his right of privacy. Analogy is a hallowed tool of legal reasoning; but to compare deletion to putting one's trash on the street where it can be searched by every passer-by . . . is to

Attorney–Client Privilege in E-mails

The **attorney–client privilege** protects the communications between a client and an attorney concerning a legal matter. To ensure that the attorney–client privilege is protected, the communication must be made confidentially.[52] In *United States v. Schwimmer*,[53] the court held that the attorney–client privilege "requires a showing that the communication in question was given in confidence and that the client reasonably understood it to be so given." For the privilege to be protected, it must be made "under circumstances from which it may reasonably be presumed that it will remain in confidence."[54] Disclosure should occur only to those parties involved in the legal action that the communication concerns.[55] If the communication is disclosed either directly or inadvertently to a third party, then the privilege is waived. Information may be disclosed inadvertently if a communication is monitored, for example. Accordingly, if an employee has been notified that computer use and communications will be monitored, the attorney–client privilege is waived.

One case dealing with this issue concerns a former physician of a hospital who sued his employer, Beth Israel Medical Center, for a breach of contract. The individual sought the return of the communications he had with his attorney via the hospital's e-mail server, arguing that these communications were protected by attorney–client privilege. To determine whether these communications were privileged, the court looked at Beth Israel's e-mail policy, which stated the following:[56]

1. All Medical Center computer systems, telephone systems, voice mail systems, facsimile equipment, electronic mail systems, Internet access systems, related technology systems, and the wired or wireless networks that connect them are the property of the Medical Center and should be used for business purposes only.
2. All information and documents created, received, saved, or sent on the Medical Center's computer or communications systems are the property of the Medical Center. Employees have no personal privacy right in any material created, received, saved, or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice.

Critical Thinking Questions

1. What do you think the court held in this case?
2. Was the physician's e-mail communications on the hospital's computer confidential?
3. Did attorney–client privilege apply? Why or why not?

reason by false analogy." Essentially, if a person does not take any steps to limit other employees' access to a workplace computer, the individual cannot have a reasonable expectation of privacy. Computers can be hidden from view by merely locking them in a private office.[44] In *Leventhal v. Knapek*,[45] for example, the court held that Leventhal had a reasonable expectation of privacy in respect of the computer in his private office because he had exclusive use of the office and computer. Leventhal's employer also did not have computer use and monitoring policies.

In *United States v. Slanina*,[46] the court held that the defendant had an expectation of privacy because his employer did not distribute a policy to employees stating that the storage of personal information was prohibited. In contrast, when an employer has policies that inform employees that the computers they use are subject to monitoring and that the personal or other objectionable use of workplace computers and networks is strictly prohibited, the courts have held that employees do not have a reasonable expectation of privacy.[47] For instance, in *United States v. Simmons*,[48] the court found that a government employee did not have a reasonable expectation of privacy in his Internet use because his employer had a policy stating that the Internet could be used only for business purposes.[49] The court has applied the same reasoning in cases involving mobile devices. In *Quon v. Arch Wireless Operating Company*,[50] for example, the court held that employers must have a policy that informs employees that their communications via these devices may be monitored and should have a history of monitoring such communications. If not, employees have a reasonable expectation of privacy in their communications via mobile phones.[51]

Search Warrants

Search warrants provide law enforcement agencies with the authority to enter a premises, search for the objects named in the warrant, and seize them. To be valid, the warrant must specifically state the crime (or crimes) being investigated, the location to be searched, and the items to be seized. Exceeding the scope of the warrant and making any errors or omissions in the search warrant may result in evidence being deemed inadmissible in court.

Probable Cause and Particularity

Under the Fourth Amendment, search warrants must be supported by probable cause and the objects of the search must be described with sufficient particularity. **Probable cause** "exist[s] where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found."[57] When applying for a search warrant, an investigator must demonstrate probable cause both that a crime has been committed and that the evidence of the crime will be found in the location specified in the warrant.

Consider the crime of sending or receiving child pornography. Some courts have held that an individual's membership for a child pornography site shows probable cause of the receipt or distribution of child pornography.[58] In *United States v. Bailey*,[59] the court stated that when an individual

> Knowingly becom[es] a computer subscriber to a specialized Internet site that frequently, obviously, unquestionably and sometimes automatically distributes electronic images of child pornography to other computer subscribers [that action] alone establishes probable cause for a search of the target subscriber's computer even though it is conceivable that the person subscribing to the child pornography site did so for innocent purposes and even though there is no direct evidence that the target subscriber actually received child pornography on his or her computer.

Other courts, however, have not agreed that membership in a child pornography Web site shows probable cause of the sending or receiving of child pornography.[60] According to these courts, additional information is required to demonstrate probable cause that a crime is being committed. This supplementary information may include, among other things, prior convictions on child pornography or sex offenses involving children and evidence of downloaded child pornography on the suspect's computer.[61]

In regards to **particularity**, the search warrant needs to specify the place that will be searched and the items that will be seized. "Mere reference to 'evidence' of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize."[62] The courts have found warrants that seize all documents and computer files without specifying how the items relate to a suspected criminal activity invalid and contrary to the Fourth Amendment.[63] By contrast, a warrant is considered sufficiently particular if it includes a description of the crime under investigation and describes which types of evidence are sought in relation to that crime.[64] For instance, if the crime being investigated is child pornography, a warrant authorizing the search and seizure of computers and electronic storage devices containing images of minors engaging in sexual activity as defined by child pornography statutes is sufficiently particular.[65] Basically, the search and seizure of items should be limited to the electronic devices that are connected to the criminal activity being investigated.

In *United States v. Upham*,[66] the court pointed out that the particularity requirement of the Fourth Amendment was implemented to protect citizens from general warrants authorizing "the wholesale rummaging through a person's property in search of contraband or evidence." A general warrant either provides too much discretion to law enforcement agencies to decide what to seize or permits law enforcement officers to indiscriminately seize both incriminating evidence and innocent items.

When Search Warrants Are Not Required for Searches and Seizures

Certain exceptions that justify a search without a warrant, include stop-and-frisk procedures, open fields, automobile exceptions, search incident to arrest, exigent circumstances, plain view, consent searches, and border searches.[68] Searches may occur during a stop-and-frisk procedure if the law enforcement agent believes that the individual being

No-Knock Warrants

When executing a search warrant, law enforcement agencies must knock before entering the premises, announce their presence, and give the resident (if present) a reasonable amount of time to comply with the requirements of the warrant. Failure to do so can result in the application of the exclusionary rule. However, law enforcement authorities could obtain a **no-knock warrant**, which would exempt them from having to knock and announce their presence before executing a search.[67] These warrants can prove quite beneficial, especially when dealing with situations where authorities believe that announcing their presence may lead to vital evidence being destroyed by the offender. This is highly likely with cybercrime, as computer evidence can be damaged, modified, concealed, or deleted in a matter of seconds.

"patted down" is armed and dangerous.[69] Searches may also occur in open fields without a warrant because these areas are exposed and accessible to the public.[70] A **warrantless search** of an automobile may occur if a law enforcement agent has probable cause to believe that the vehicle holds evidence of a crime.[71] The remaining four exceptions are explored in further detail in the following subsections, as they are particularly applicable to computers and related electronic devices.

Search Incident to Arrest

Searches that occur upon the arrest of individuals (**search incident to arrest**) encompass searches of the arrestees and the areas under their immediate control. As the court stated in *United States v. Robinson*,[72] "in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment." These searches are authorized to protect the arresting officer, to ensure that the evidence in the arrestee's possession is not destroyed, and to prevent an individual from escaping arrest with the items on his or her person. Law enforcement agents may also search the arrestee for evidence of the crime he or she is being suspected of committing.[73] Indeed, in *United States v. Ortiz*,[74] the court affirmed that a law enforcement agent's "need to preserve evidence is an important law enforcement component of the rationale for permitting a search of a suspect incident to a valid arrest."[75]

The primary reason for searching for such evidence is to prevent its destruction. For instance, in respect of pagers, the court stated that due to "the finite nature of a pager's electronic memory, incoming pages may destroy currently stored telephone numbers in a pager's memory. The contents of some pagers also can be destroyed merely by turning off the power or touching a button."[76] Essentially, the courts have upheld the searches of portable electronic devices, such as pagers, cell phones, and personal digital assistant (PDAs), incident to arrest.[77] The applicability of this doctrine to electronic devices such as laptops, however, has yet to be addressed by the courts.

Exigent Circumstances

Another exception to the warrant requirement occurs in **exigent circumstances**. In *United States v. David*,[78] the court stated that evidence can be seized without a warrant if "the destruction of [this] evidence is imminent" and "there is probable cause to believe that the item seized constitutes evidence of criminal activity." Generally, emergency circumstances arise with computers if a suspect seeks to damage the computer or damage or delete its files. The suspect can accomplish this by either physically damaging the computer (e.g., by breaking it) or using computer commands or program designed to destroy evidence (e.g., by deleting files or formatting entire disks).

Usually, this exception allows a law enforcement agent to seize a computer or other electronic device. The search of the device, however, usually requires another search warrant. For example, in *United States v. David*,[79] the law enforcement agent seized the defendant's computer memo book because the defendant was deleting files in it. After the memo book was seized from the suspect's possession, the law enforcement agent was required to obtain a warrant to search it.

Sometimes emergency access to electronic devices is required because evidence may be destroyed independent of any action by the suspect. In *United States v. Parada*,[80] the defendant's cell phone records were accessed due to exigent circumstances. Specifically, swift access to these records was required because incoming calls had the potential of overwriting call memory, thereby possibly destroying vital evidence in the case.

Consent

One of the most relevant exceptions to the requirement for a warrant to conduct the search and seizure of computers is the **consent search**. According to the ruling in *Schneckloth v. Bustamante*,[81] "consent searches are part of the standard investigatory techniques of law enforcement agencies. They normally occur on the highway, or in a person's home or office, and under informal and unstructured conditions." Searches can occur without a warrant and without probable cause if an individual who has authority over the place or items to be searched has consented to the search.[82] For the consent to be legal, the individual must not have been tricked or coerced into consenting to the search. If an individual consents to a search when a law enforcement agent falsely claims to have a warrant to search the premises, the court has found the consent is invalid and has deemed the search unconstitutional.[83] The individual must also have voluntarily consented to the search. If the "consent was not given voluntarily—that it was coerced by threats or force, or granted only in submission to a claim of lawful authority—then [the courts] have found the consent invalid and the search unreasonable."[84] As such, it is imperative that investigators advise subjects that the search is voluntary and that the subject may withdraw his or her consent to the search at any time.

If a computer is searched with the consent of a third party, its legitimacy may be challenged. In addition, a search can be contested if the search of a subject's property or computer exceeds the scope of the consent given. The scope of consent defines the area that the individual is allowing to be searched. For instance, if a police officer asked a subject,

"Can I search your car for drugs?" and the subject consents, it is quite clear that the scope of the consent includes the inside of the car, underneath the seats, and so on.

Principally, a warrant is not required in the following circumstances:

1. The suspect himself or herself consents to the search.
2. A third party with authority over the property consents to the search.
    - *Employers/Employees.* They can consent to searches of areas not exclusively set aside for the employee suspected of the crime. However, the court has also found that an employee can consent to the search of an employer. Specifically, in *United States v. Longo*,[85] an employee—the secretary—was found to have authority to consent to a search of her employer's computer. Additionally, coworkers can consent to searches of computers that are shared with the suspect of a crime.
    - *Parents.* They can give consent to search their child's computer even if the parents do not use or have access to the computer and the computer is located in the child's room or another private space of the child. As long as the child is dependent on the parents and not paying his or her parents rent to live in the room, the parents have the authority to consent to the search.[86]
    - *Spouses.* Generally, they have the authority to consent to a search of the computer of the other spouse as long as the computer of the nonconsenting spouse is not used exclusively by him or her and is not kept in a separate room (where only the nonconsenting spouse enters or has access to). For instance, in *Walsh v. State*,[87] the court ruled that a wife could consent to the search of a computer used by the defendant because she had bought the computer and it was used by the entire family.
    - *Relatives.* The court has held that a relative can consent to a search of a defendant's property if the relative has access and control over the place or object that is the target of the search. For example, a court ruling stated that a son-in-law had the authority to consent to a search over an area he had access to and control over.[88]
    - *Roommates/Housemates.* Similarly to the requirements with spouses and relatives, roommates have the authority to consent to searches of spaces and objects that they share with the defendant. For example, in the case of *United States v. Smith,*[89] a roommate was able to consent to the search of the defendant's computer because she had joint access to it and it was part of the house that she shared with the defendant.[90]

If a third party does not have a key to a locked item of a suspect, he or she cannot consent to its search. For instance, even though parents have the authority to consent to the search of their child's room, they do not have the authority to consent to a search of their child's locked property (e.g., locked toolbox, locked closet).[91] The court reached a similar

conclusion in a case involving the defendant's girlfriend. Specifically, although the defendant's girlfriend consented to the search of the defendant's locked safe, the court found that she did not have the authority to consent to the search.[92] In general, the courts have ruled that boyfriends, girlfriends, roommates (or housemates), parents, spouses, and other relatives are unable to consent to a search of locked items they do not have access to in homes shared with the defendants.

What happens when a third party has partial access to a shared computer? Can a third party consent to the part of the computer that he or she does not have access to? Consider a computer that is shared by two users, A and B. User A has password-protected certain files. User B does not know the password to those files. Can user B consent to a search of user A's password-protected files? In *United States v. Buckner*,[93] the court compared password-protected files to "locked boxes" in common areas. As previously noted, the court has ruled that third parties cannot consent to the search of locked objects in common areas if they do not have the combination or key to open those locks. Consequently, if user A password-protected certain files and user B does not know the password to access these files (because user A has not shared it with user B), then user B cannot consent to have those files searched by law enforcement officers.

The best practice is to get consent in writing because it can serve as evidence that consent was given voluntarily. Written consent can also show the scope of the consent—that is, which locations, property, computers, or electronic devices the subject consented to have searched by law enforcement officers.[94]

Border Searches

The U.S. Congress has authorized customs searches at borders. Each sovereign nation has the right to regulate the entry and exit of individuals at its borders and under what conditions this may occur—the so-called **border search doctrine**. In most cases, U.S. courts have found warrantless border searches reasonable primarily due to the belief that the sovereign nation has the right to "protect itself by stopping and examining persons and property crossing into this country."[95] The interests of the sovereign state to exclude undesirable persons and prohibited goods have been cited to justify warrantless searches and searches conducted without reasonable suspicion or probable cause.[96]

While routine border searches do not require reasonable suspicion, probable cause, or a warrant,[97] the same cannot be said about nonroutine searches. The courts have ruled that "reasonable suspicion is required for the detention of a traveler at the border 'beyond the scope of a routine customs search and inspection.'"[98] Thus any nonroutine search must be preceded by reasonable suspicion of criminal activity and the search must not exceed that which is necessary to find the evidence of the crime.[99] The suspicious behavior of the traveler may also trigger a nonroutine search (e.g., if an individual seems extremely nervous during the routine search or questioning or if an individual purchased a one-way ticket in cash the day of the flight).[100]

Consider two landmark cases concerning border searches as they pertain to computers, *United States v. Romm*[101] and *United States v. Arnold*.[102] In *Romm*, the defendant flew from the

United States to Canada. Upon arriving in Canada, he was questioned by agents from Canada's Border Services Agency concerning his criminal history.[103] The agents also checked his computer and found several child pornography Web sites listed in his Internet history. Romm was denied entry to Canada, detained, and subsequently sent back to the United States. Upon his arrival in the United States, his computer was searched again and the evidence retrieved from it was used to charge Romm with crimes related to child pornography. Romm sought to have the evidence suppressed by claiming that the search and seizure of his computer violated his rights under the Fourth Amendment. The court disagreed, holding that international airports are the functional equivalent of a border and, therefore, the search of Romm's computer fell within the scope of the border search exception.[104]

In *Arnold*, the defendant was selected for secondary questioning at the Los Angeles International airport after arriving from the Philippines.[105] Upon inspecting his luggage, customs officials found a laptop computer, a hard drive, a computer memory stick, and six CDs. A customs official asked Arnold to turn the computer on, which he did. The customs official then accessed two folders on Arnold's computer and found something that the official believed warranted the attention of special agents from U.S. Immigration and Customs Enforcement (ICE). Subsequently, the ICE special agents searched Arnold's laptop and found what they believed to be child pornography. The special agents then seized Arnold's laptop and storage devices. According to Arnold, the warrantless search of his laptop violated his rights under the Fourth Amendment. As such, he insisted that the evidence retrieved from his laptop and storage devices should be suppressed. Although the District Court of the Central District of California agreed with him by finding that the search and seizure of Arnold's laptop by customs agents violated the Fourth Amendment, this decision was later overturned by the Ninth Circuit Court of Appeals.[106] The courts have rendered similar judgments, upholding warrantless searches under the border exception, in other cases involving the transport of child pornography.[107]

Plain View

Another relevant exception to a warrant for the search and seizures of computers is the "plain view" exception. The **plain view doctrine** allows law enforcement agencies conducting a search to seize evidence (not specified in a search warrant) that is in plain view, whose incriminating nature is immediately apparent to the officers.[108] Some courts have held that the plain view doctrine is applicable to computers and electronic evidence;[109] others have claimed that it should not be applied to such devices.[110]

The plain view doctrine has been applied to cybercrime cases where the search of a computer pursuant to a valid warrant subsequently led to the discovery of incriminating information not specified in the warrant. For example, in *United States v. Carey*,[111] the warrant specified that law enforcement personnel could search the suspect's computer for "documentary evidence pertaining to the sale and distribution of controlled substances."[112] While searching the suspect's computer for evidence of the sale and distribution of drugs, the investigator found images of child pornography. The investigator then abandoned the

initial search for drug files and started searching for more child pornography images. However, every image after the initial discovery of an image of child pornography was ruled inadmissible in court. Why? Because if incriminating evidence other than that specified in the warrant is found during a search, the investigator should stop the search and get a new warrant based on the plain view evidence discovered.

Changing the search based on the new incriminating evidence found on a computer will likely result in the evidence being deemed inadmissible in court, as was the case in *Carey*.[113] As a general rule, if a warrant authorizes a search of the files pertaining to a specific crime, it will not authorize the search of files for other crimes not specified in the warrant.[114]

Searching the Computer for Evidence

In *United States v. Barth*,[115] the court held that "the Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers and closed personal effects." Because intimate information may be stored on computers, the courts have ruled that these devices should be placed "into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy."[116] Additionally, given that government agents need to obtain search warrants to access closed containers, the court held that the same requirement should apply to closed computer files and other electronic storage devices.[117] The question that follows is this: How should the search of the computer for electronic evidence of the crime be conducted?

Search Protocols

The process of searching a computer for electronic evidence can easily turn into a sweeping examination of a wide array of information. Computer forensics technology, however, provides investigators with a range of methods by which they can more narrowly target their search of computers for electronic evidence, such as by "limiting the search by date range, doing key word searches [and phrases], limiting the search to text files or graphics files, and focusing on certain software programs."[118] The mere existence of these search tools demonstrates that investigators have the ability to conduct more targeted searches of computers. In one child pornography case, *United States v. Carey*,[119] the court stated that investigators can and should limit searches by searching the computer using filenames, directories, and a sector-by-sector search of the hard drive.

Some courts have stated that a search protocol must be formulated before the search. A **search protocol** is a document that describes what is being searched for in a computer and which methodology will be used. By formulating a search protocol before the search, it is believed that the search will be narrowed and less privacy inva-

sive. This is what Ralph Winick proposed. Specifically, he suggested that, "before a wide-ranging exploratory search is conducted, the magistrate should require the investigators to provide an outline of the methods that they will use to sort through the information"[120] (the **Carey-Winick approach**). *In re Search of 3817 W. West End*,[121] the magistrate of the court did just that by requiring the investigating officers in the case to specify which search protocol they planned to use to search the computer for electronic evidence.

Kerr argues that Winick and the *Carey* court have failed to realize how difficult it is to specify which search strategy is required without first having looked at the types of files that are present on the hard drive of the computer.[122] Indeed, some courts have argued that predetermined search protocols are impractical. For example, in *United States v. Scarfo*,[123] the court stated that when searching computers for information whose nature cannot be known in advance, "law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location."

Incriminating evidence can be stored on a computer in numerous ways. From the perspective of law enforcement officers, computer searches must be broad because suspects may encrypt, hide, or mislabel incriminating files to evade detection. In fact, in *United States v. Gray*,[124] the court noted that suspects may "intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories"; for this reason, the agents searching computer files should not be "required to accept as accurate any file name or suffix" and to limit their search accordingly. Put simply, the seizing agents are not required to accept the labels of objects as indicative of their contents.[125]

Consider the practice of changing the extension at the end of the filename. This widely used and popular method for hiding a file is quite simple to use. To see how it works, follow these steps: First, create an Excel document and save it. Change the .xls extension on the document to .doc. The icon attached to the filename in the directory should change from Excel to Word, but when you try to open the file by clicking on it, the attempt should fail. Now launch Excel and then open the .doc file you created; it should open correctly now.

In the child pornography case known as *United States v. Hill*,[126] the defendant claimed that the search of his computer should have been solely "limited to certain files more likely to be associated with child pornography, such as those with a '.jpg' suffix . . . or those containing the word 'sex' or other key words." The court held that this search methodology was unreasonable:

> Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer . . . Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder."[127]

As the court recognized in *Hill*, "images can be hidden in all manner of files, even word processing documents and spreadsheets."[128] Indeed, a vast number of text file extensions can be used to hide files:

- .doc (Word document)
- .docx (Word Open XML document)
- .pages (Pages document)
- .rtf (rich text file)
- .txt (plain text file)
- .wpd (WordPerfect document)
- .wps (Microsoft Works word processor document)

Of course, an experienced computer user will probably not use common text files to hide evidence of his or her crimes, nor is such a criminal likely to use common image file extensions, such as the following:

- .bmp (bitmap image file)
- .gif (Graphical Interchange Format file)
- .jpg (JPEG image file)
- .png (Portable Network Graphic)
- .psd (Photoshop document)
- .tiff (Tagged Image File Format)

Instead, the criminal will likely employ file extensions that are rarely used, and with which investigators may be unfamiliar. For instance, someone seeking to hide child pornography photos may save the images under the following image file extensions:[129]

- .411 (Mavica thumbnail image)
- .fbm (Fuzzy bitmap image)
- .imj (JFIF bitmap image)
- .kfx (Kofax image file)
- .mip (Multiple Image Print file)
- .mrb (Multiple Resolution bitmap file)

Perhaps a criminal will save the file as an attachment in an e-mail. Given the many different operating systems available today and the many different filename extensions that they use, it can be extremely difficult for an investigator to narrow down which information is included in each file type (even before a suspect seeks to alter the contents or change the file extensions to evade detection by authorities). Accordingly, if a warrant

specifies the search of specific file formats, such as text files, it would exclude from the search image and other files that may potentially hold evidence of the crime.

In summary, most computer forensics investigations cannot follow a predetermined search protocol. To overcome this difficulty, the courts, in cases such as *United States v. Triumph Capital Group, Inc.*,[130] have endorsed the practice of investigators keeping detailed notes of their search of the computer for electronic evidence and explaining the rationale for each part of their search.[131]

Dealing with Privileged Data During a Search of a Computer

What should an investigator do if the computer that he or she is about to search contains **privileged information**? Which steps should be taken to protect such information during a search? The courts have recognized that computers may contain personal, sensitive, confidential, and proprietary information. Some cases may require the collection of evidence from the computer of a lawyer, a medical professional, a member of the clergy, a journalist, or a business person. Special care must be exercised when planning to search such a computer because of the privileged—and, therefore, protected—information that it may contain (e.g., medical data and attorney-client communications). As the court stated in *United States v. Arnold*,[132] "attorneys' computers may contain confidential client information. Reporters' computers may contain information about confidential sources or story leads. Inventors' and corporate executives' computers may contain trade secrets." The search of computers that contain privileged documents requires different rules because these computers may contain hundreds (maybe even thousands) of files and records of disinterested third parties unrelated to the investigation being conducted.

Three main strategies are used for screening computers that may contain privileged data. The first option is for the investigator to review the files while being recorded on camera. The court has stated that the in-camera review of potentially privileged documents "is a relatively costless and eminently worthwhile method to [e]nsure that the balance between petitioners' claims of irrelevance and privilege and plaintiffs' asserted need for the documents is correctly struck."[133] This method has been viewed by courts as "a highly appropriate and useful means of dealing with claims of governmental privilege."[134]

The second and third options involve third parties in the sorting and searching of these files. For the files to be given to the court, one or more third parties must review the files to see which are considered privileged and which can be given over to the prosecution team.

The second method involves taint teams, which are made up of prosecutors and agents—not in any way related to the case at hand—whose task is to view the electronic records seized and screen out any privileged information. In *Khadar v. Bush*,[135] the court approved the government's use of a "filter team" to review potentially privileged documents seized during searches of prisoners' cells at Guantanamo Bay. The search of the prisoners' cells in Guantanamo Bay was triggered by the coordinated suicides of three prisoners there. Such use of filter or taint teams has also been favored by other courts. For

example, in *United States v. Triumph Capital Group, Inc.*,[136] taint teams were used to review privileged information. In *Triumph*, the court stated that "the use of a taint team is a proper, fair, and acceptable method of protecting privileged communications when a search involves property of an attorney."

Other courts,[137] however, have expressed discomfort with the use of taint teams. For instance, in the case known as *In re Search Warrant for Law Offices Executed on March 19, 1992 and Grand Jury Subpoena Duces Tecum Dated March 17, 1992*,[138] the court stated that "reliance on the implementation of a [taint team], especially in the context of a criminal prosecution, is highly questionable, and should be discouraged." It is believed that the prosecutors and agents in taint teams may not be able to ignore other crimes they may potentially find in the electronic records they are reviewing, which creates an appearance of unfairness. One way to try to ensure that these teams remain neutral is to perform regular audits of their practices and to have team members submit a detailed report of the actions they perform during their review.

To alleviate the concerns raised by the use of filter or taint teams, a third method may be used in cases potentially involving privileged information. With this method, a presiding judge appoints a neutral third party known as a "special master" to review potentially privileged files. The use of a special master to determine whether certain seized electronic documents contained privileged information was approved by the court in *United States v. Abbell*.[139] Another case where a court preferred the use of a special master to sort through potentially privileged electronic documents was *United States v. Hunter*.[140] In *Hunter*, law enforcement agents obtained a warrant authorizing the search and seizure of an attorney's computer systems. A special master, who was not employed by the law enforcement agency or the prosecutor's office, was used to screen the privileged material. For the search of the computer systems, a detailed search protocol was also provided to explain how the analyst would access relevant documents while avoiding the observation of privileged files.

Chapter Summary

This chapter focused on the right to privacy, including how it applies to computers. It also considered the areas where individuals have a reasonable expectation of privacy. Specifically, case law indicates that individuals have a reasonable expectation of privacy in the contents of their computers and related electronic devices (with certain exceptions).

Investigators are bound by the Fourth Amendment to the U.S. Constitution when they conduct searches and seizures. In particular, searches conducted by police officers (and anyone acting as an agent of the government) are limited to items and areas described in a warrant. Warrantless searches may occur under certain exceptions.

Special issues arise in searching computers for evidence. Some believe that a search protocol should be used during this process to minimize the intrusion into an individual's privacy. Others argue that by doing so, vital evidence may be overlooked because an investigator may not know how evidence of the crime was stored in the computer. Computers may also contain private and confidential information that should not be accessed by

investigators. To conduct searches in such cases, special rules and procedures need to be followed to deal with and protect privileged information in computers.

Key Terms

Attorney–client privilege
Border search doctrine
Carey-Winick approach
Consent search
Exclusionary rule
Exigent circumstances
Good faith exception
Inevitable discovery exception
No-knock warrant
Particularity
Plain view doctrine
Privacy
Privileged information
Probable cause
Search and seizure
Search incident to arrest
Search protocol
Warrantless search

Critical Thinking Questions

1. What are your thoughts on the Carey-Winick approach? Is it beneficial or bad news?
2. In your opinion, what is the best strategy for reviewing privileged information on computers and why?

Review Questions

1. Why is privacy important?
2. Is all evidence that is illegally searched and seized inadmissible in court? Why do you think this is the case?
3. How is the "reasonable expectation of privacy" test applied to computers?
4. Does an employee have a reasonable expectation of privacy in the workplace?
5. When does the government need a search warrant to search and seize a suspect's computer?
6. What are some examples of warrantless searches, and under which circumstances may they be conducted?
7. Under which circumstances can a portable electronic device be seized and searched after a suspect is arrested?
8. Which type of exigent circumstances may arise in respect to computers?
9. When can a third party consent to a search?
10. Should search protocols be used in investigations? Why or why not?
11. What should investigators do if a computer that is being searched might contain privileged information?

Footnotes

[1]Cooley, T. (1907). *A treatise on the law of torts*. Chicago: Callaghan; Wong, R. (2005). Privacy: Charting its developments and prospects. In M. Klang & A. Murray (Eds.), *Human rights in the digital age*. London: GlassHouse, p. 148.

[2]Janis, M., Kay, R., & Bradley, A. (2000). *European human rights law: Text and materials* (2nd ed.). Oxford, UK: Oxford University Press, p. 300.

[3]Fried. C. (1970). *An anatomy of values*. Cambridge, MA: Harvard University Press; Wong, R. (2005). Privacy: Charting its developments and prospects. In M. Klang & A. Murray (Eds.), *Human rights in the digital age*. London: GlassHouse, p. 141.

[4]Galison, P., & Minow, M. (2005). Our privacy, ourselves in the age of technological intrusions. In R. A. Wilson (Ed.), *Human rights in the "War on Terror."* Cambridge, UK: Cambridge University Press, p. 258.

[5]Roberts, P. (2001). Privacy, autonomy, and criminal justice rights. In P. Alldridge & C. Brants (Eds.), *Personal autonomy, the private sphere and the criminal law: A comparative study*. Oxford, UK: Hart, p. 59.

[6]Schoeman, F. D. (1984). Privacy: Philosophical dimensions. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology*. Cambridge, UK: Cambridge University Press, p. 20.

[7]Westin, A. F. (1966, June). Science, privacy and freedom: Issues and proposals for the 1970s: Part I—The current impact of surveillance on privacy. *Columbia Law Review*, *66*(6), 1031.

[8]Fried, C. (1984). Privacy [a moral analysis]. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology*. Cambridge, UK: Cambridge University Press, p. 212.

[9]Archer, R. L. (1980). Self-disclosure. In D. M. Wegner & R. R. Vallacher (Eds.), *The self in social psychology*. Oxford, UK: Oxford University Press, p. 199.

[10]Schoeman, F. D. (1984). Privacy: Philosophical dimensions. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology*. Cambridge, UK: Cambridge University Press, p. 3.

[11]See footnote 27 in Gavison, R. (1980, January). Privacy and the limits of the law. *Yale Law Journal*, *89*(3),469.

[12]Ehrenreich, R. (2001, June). Privacy and power. *Georgetown Law Journal*, *89*(6), 2051.

[13]For example, see *United States v. Couch*, 688 F.2d 599, 604 (9th Cir. 1982).

[14]Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*, 213.

[15]Kerr, O. S. (2005). Searches and seizures in a digital world. *Harvard Law Review*, *119*, 542.

[16]*United States v. Arnold*, 454 F. Supp. 2d 999, 1003–1004 (C.D. Cal. 2006).

[17]*United States v. Arnold*, 454 F. Supp. 2d 999, 1003 (C.D. Cal. 2006); *United States v. Molina-Tarazon*, 279 F.3d 709, 716 (9th Cir. 2002).

[18]*Walter v. United States*, 447 U. S. 649, 662 (1980) (Justice Blackmun, dissenting); *United States v. Jacobsen*, 466 U. S. 109, 113 (1984).

[19]*Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971).

[20]See *United States v. Jarrett*, 338 F. 3d 339 (4th Cir. 2003); *United States v. Steiger*, 318 F. 3d 1039, 1042–1046 (11th Cir. 2003).

[21]*United States v. Ellyson*, 326 F. 3d 522 (4th Cir. 2003).

[22]Although there are a few exceptions to this, such as the good faith exception, which holds that if a law enforcement agent acted in good faith belief that he or she was acting according to valid search warrant that is later found defective, the illegally seized evidence is admissible in court.

[23]232 U.S. 383 (1914).

[24]See *United States v. Leon*, 468 U.S. 897 (1984).

[25]389 U.S. 347 (1967).

[26]*California v. Ciraolo*, 476 US 207, 211 (1986).

[27]389 U.S. 347, 351 (1967).
[28]389 U.S. 347, 352 (1967).
[29]389 U.S. 347, 351 (1967).
[30]*Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001).
[31]*Commonwealth v. Proetto*, 771 A.2d 823, 831 (Pa. Super. 2001).
[32]979 F. Supp. 1177 (S.D. Ohio 1997).
[33]*United States v. Charbonneau*, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997).
[34]See, for example, *State v. Evers*, 815 A.2d 432, 439-40 (N.J. 2003); *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002); *United States v. Maxwell*, 45 M.J. 406, 418-19 (C.A.A.F. 1996).
[35]917 F.2d 955, 958-59 (6th Cir. 1990).
[36]*O'Connor v. Ortega*, 480 U.S. 709, 721 (1987).
[37]677 S.W.2d 632, 637-38 (Tex. App. 1984).
[38]*United States v. Long*, 61 M.J. 539, 543 (N-M. Ct. Crim. App. 2005); *United States v. Mendoza*, 281 F.3d 712, 715 (8th Cir. 2002).
[39]*United States v. Buckner*, 473 F.3d 551, 554 (4th Cir. 2007).
[40]*In re Boucher*, No. 2:06-mj-91, 2007 WL 4246473 at 5 (D.Vt. 2007).
[41]The Fifth Amendment states: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."
[42]523 F.3d 941 (9th Cir. 2008).
[43]168 F.3d 532, 537 (1st Cir. 1999).
[44]*United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007); *State v. Young*, 974 So. 2d 601, 609 (Fla. Dist. Ct. App. 2008).
[45]266 F.3d 64, 73–74 (2d Cir. 2001).
[46]283 F.3d 670 (5th Cir. 2002).
[47]*Biby v. Board of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005); *United States v. Thorn*, 375 F.3d 679, 683 (8th Cir. 2004); *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002); *Muick v. Glenayre Electronics,* 280 F.3d 741, 743 (7th Cir. 2002); *United States v. Bailey*, 272 F. Supp. 2d 822, 824 (D. Neb. 2003); *Wasson v. Sonoma County Junior College District*, 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997).
[48]206 F. 3d 392 (4th Cir. 2000).
[49]In this case, Simmons had downloaded pornographic material from the Internet to his work computer.
[50]529 F.3d 892 (9th Cir. 2008).
[51]*Quon v. Arch Wireless Operating Company,* 529 F.3d 892, 906–907 (9th Cir. 2008).
[52]*United States v. Melvin*, 650 F.2d 641, 645 (5th Cir. 1981).
[53]892 F.2d 237, 244 (2d Cir. 1989).
[54]*Wilcoxon v. United States*, 231 F.2d 384, 386 (10th Cir. 1956).
[55]*United States v. Evans*, 954 F. Supp. 165, 170 (N.D. Ill. 1997); *United States v. Ryans,* 903 F.2d 731, 741 n.13 (10th Cir. 1990); *United States v. Schwimmer*, 892 F.2d 237, 237 (2d Cir. 1989); *State v. Colton*, 384 A.2d 343, 345-46 (Conn. 1977); *United States v. Tellier*, 255 F.2d 441, 447 (2d Cir. 1958).
[56]*Scott v. Beth Israel Medical Center, Inc.*, 847 N.Y.S.2d 436, 439 (N.Y. Sup. Ct. 2007).
[57]*Ornelas v. United States*, 517 U.S. 690, 696 (1996); *Illinois v. Gates*, 462 U.S. 213, 238 (1983).
[58]See, for example, *United States v. Martin*, 426 F.3d 3 (2d Cir. 2005); *United States v. Wagers*, 339 F. Supp. 2d 934 (E.D. Ky. 2004).

[59]272 F. Supp. 2d 822, 824-25 (D. Neb. 2003).

[60]For example, in *United States v. Corcas*, 419 F.3d 151 (2d Cir. 2005), the court stated that the precedent that membership to child pornography Web sites provides probable cause of the receipt or distribution of child pornography was unsound. See also *United States v. Gourde*, 382 F.3d 1003, 1006, 1011-13 (9th Cir. 2004); *United States v. Perez*, 247 F. Supp. 2d 459, 483-84 (S.D.N.Y. 2003).

[61]For prior convictions as additional evidence see, for example, *United States v. Wagers*, 339 F. Supp. 2d 934, 941 (E.D. Ky. 2004), and *United States v. Fisk*, 255 F. Supp. 2d 694, 706 (E.D. Mich. 2003). For evidence of downloading as supplemental evidence, see, for example, *United States v. Perez*, 247 F. Supp. 2d 459, 483-84 (S.D.N.Y. 2003), and *United States v. Zimmerman*, 277 F.3d 426, 435 (3d Cir. 2002).

[62]*United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992); *United States v. Maxwell*, 920 F.2d 1028, 1033 (D.C. Cir. 1990); *United States v. Holzman*, 871 F.2d 1496, 1509 (9th Cir. 1989); *Voss v. Bergsgaard*, 774 F.2d 402, 405 (10th Cir. 1985); *United States v. Cardwell*, 680 F.2d 75, 77 (9th Cir. 1982).

[63]*United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995); *In re Search Warrant for K-Sports Imports, Inc.*, 163 F.R.D. 594, 597-98 (C.D. Cal. 1995); *Lafayette Academy, Inc. v. United States*, 610 F.2d 1, 5-6 (5th Cir. 1979).

[64]*State v. Askham*, 86 P.3d 1224, 1227 (Wash. App. 2004).

[65]*United States v. Thorn*, 375 F.3d 679, 684-85 (8th Cir. 2004); *United States v. Gleich*, 293 F. Supp. 2d 1082, 1088 (D.N.D. 2003); *State v. Wible*, 51 P.3d 830, 837 (Wash App. 2002); *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000); *United States v. Campos*, 221 F.3d 1143, 1147-48 (10th Cir. 2000); *Davis v. Gracey*, 111 F.3d 1472, 1479 (10th Cir. 1997); *State v. One Pioneer CD-ROM Changer*, 891 P.2d 600, 604 (Okla. Ct. App. 1995).

[66]*United States v. Upham*, 168 F. 3d 532, 535 (1st Cir. 1999).

[67]*Wilson v. Arkansas*, 514 U.S. 927 (1995).

[68]Harr, J. S., & Hess, K. M. (2005). *Constitutional law and the criminal justice system* (3rd ed.). New York: Thomson-Wadsworth, p. 219.

[69]*Terry v. Ohio*, 392 U.S. 1 (1968).

[70]See *Hester v. United States*, 265 U.S. 57 (1924), where the court stated that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields."

[71]*Wyoming v. Houghton*, 526 U.S. 295 (1999); *United States v. Ross* 456 U.S. 798 (1982).

[72]414 U.S. 218, 235 (1973); See also *New York v. Belton*, 453 U.S. 454, 459 (1981).

[73]*United States v. Robinson*, 414 U.S. 218, 233–234 (1973); *Abel v. United States,* 362 U.S. 217 (1960); *Agnello v. United States,* 269 U.S. 20 (1925).

[74]84 F.3d 977 (7th Cir. 1996).

[75]See also *United States v. Robinson*, 414 U.S. 218, 226 (1973).

[76]*United States v. Robinson*, 414 U.S. 218, 226 (1973); *United States v. Meriwether*, 917 F.2d 955, 957 (6th Cir. 1990).

[77]*United States v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007); *United States v. Mercado-Nava*, 486 F. Supp. 2d 1271, 1278-79 (D. Kan. 2007); *United States v. Romero-Garcia,* 991 F. Supp. 1223 (D. Or. 1997); *United States v. Thomas*, 114 F.3d 403, 404 n.2 (3d Cir. 1997); *United States v. Reyes*, 922 F. Supp. 818, 833 (S.D.N.Y. 1996).

[78]756 F Supp. 1385 1392 (D. Nev. 1991).

[79]756 F. Supp. 1385, 1392 (D. Nev. 1991).

[80]289 F. Supp. 2d 1291, 1304 (D. Kan. 2003).

[81]412 U.S. 218, 231– 232 (1973).

[82]See *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973); *United States v. Matlock*, 415 U.S. 164, 171 (1974); *Stoner v. California*, 376 U.S. 483 (1964).

[83]*Bumper v. North Carolina*, 391 U.S. 543, 550 (1968).
[84]*Schneckloth v. Bustamonte*, 412 U.S. 218, 233 (1973); See also *Bumper v. North Carolina*, 391 U.S. 543, 548–549 (1968); *Johnson v. United States*, 333 U.S. 10 (1948); *Amos v. United States*, 255 U.S. 313 (1921).
[85]70 F Supp. 2d 255, 256 (WDNY 1999).
[86]See *United States v. Rith*, 164 F 3d 1323 (10th Cir.), cert. denied, 528 US 827 (1999).
[87]512 S. E. 2d 408, 411–412 (Ga. Ct. App. 1999).
[88]*State v. Guthrie*, 627 N.W. 2d 401 (S.D. 2001).
[89]27 F. Supp. 2d 1111 (C.D. Ill. 1998).
[90]*United States v. Smith*, 27 F. Supp. 2d 1111, 1115–1116 (C.D. Ill. 1998).
[91]*State v. Harris*, 642 A 2d. 1242 (Del. 1993); *People v. Snipe*, 841 N.Y.S. 2d 763 (N.Y. Sup. Ct. 2007).
[92]*State v. Smith*, 966 S. W. 2d 1 (Mo. Ct. App. 1997).
[93]473 F.3d 551, 554 (4th Cir. 2007); See also *Trulock v. Freeh,* 275 F.3d 391 (4th Cir. 2001).
[94]*United States v. Block*, 590 F. 2d 535, 537 (4th Cir. 178).
[95]*United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004); *United States v. Ramsey*, 431 U.S. 606, 616 (1977).
[96]*United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).
[97]*United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). See also *United States v. Ramsey*, 431 U.S. 606, 620 (1977).
[98]See, for example, *United States v. Sandoval Vargas*, 854 F.2d 1132, 1134 (9th Cir. 1988).
[99]*United States v. Couch*, 688 F.2d 599, 604 (9th Cir. 1982); *United States v. Summerfield*, 421 F.2d 684, 685 (9th Cir. 1970).
[100]See, for example, *United States v. Sokolow*, 490 U.S. 1, 4-5 (1989); *United States v. Carter*, 590 F.2d 138, 139 (5th Cir. 1979); *United States v. Olcott*, 568 F.2d 1173, 1174-75 (5th Cir. 1978).
[101]455 F.3d 990 (9th Cir 2006).
[102]454 F. Supp. 2d 999 (C.D. Cal. 2006).
[103]In an unrelated case, Romm had pleaded nolo contendere (no contest) to crimes involving children (including child exploitation by means of a computer).
[104]*United States v. Romm*, 455 F.3d 990, 997 (9th Cir 2006).
[105]*United States v. Arnold*, 454 F. Supp. 2d 999, 1004 (C.D. Cal. 2006).
[106]*United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008).
[107]See, for example, *United States v. Ickes*, 393 F.3d 501, 503 (4th Cir. 2005).
[108]*Horton v. California*, 496 US 128, 134 (1990).
[109]*United States v. Mann*, No. 08-3041, 210 U.S. App. LEXIS 1264 (7th Cir. Decided January 20, 2010); *United States v. Farlow*, 2009 U.S. Dist. LEXIS 94778 (D. Maine September 29, 2009).
[110]*United States v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085 (9th Cir. 2008).
[111]172 F. 3d 1268 (10th Cir. 1999).
[112]*Ibid*. at 1271.
[113]See *Carey* for more information on this issue.
[114]*People v. Carratu*, 755 N.Y.S. 2d 800, 807 (N.Y. Sup. Ct. 2003).
[115]26 F. Supp. 2d 929, 936–937 (W.D. Tex. 1998).
[116]*United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007).
[117]*United States v. Roberts*, 86 F. Supp. 2d 678, 688–689 (S.D. Tex. 2000); *United States v. Barth*, 26 F. Supp. 2d 929, 936–937 (W.D. Tex. 1998); *United States v. David*, 756 F. Supp. 1385, 1390 (D. Nev. 1991).
[118]*In re Search of 3817 W. West End*, 321 F. Supp. 2d 953 (N.D. Ill. 2004).

[119]172 F. 3d at 172.
[120]Winick, R. (1994). Searches and seizures of computers and computer data. *Harvard Journal of Law and Technology, 8,* 108; Kerr, O. S. (2005). Searches and seizures in a digital world. *Harvard Law Review*, *119*, 572–573.
[121]321 F. Supp. 2d 953 (N.D. Ill. 2004).
[122]Kerr, O. S. (2005). Searches and seizures in a digital world. *Harvard Law Review*, *119*, 575.
[123]180 F. Supp. 2d 572, 578 (D.N.J. 2001).
[124]Kerr, O. S. (2005, January). Digital evidence and the new criminal procedure. *Columbia Law Review*, *105*, 302.
[125]*United States v. Abbell,* 963 F. Supp. 1178, 1201 (S.D. Fla. 1997).
[126]459 F.3d 966, at 978 (9th Cir. 2006).
[127]459 F.3d 966, at 978 (9th Cir. 2006).
[128]459 F.3d 966, at 978 (9th Cir. 2006).
[129]This list is by no means exhaustive. There are hundreds of file extensions that could be used.
[130]211 F.R.D. 31 (D. Conn. 2002).
[131]Orton, I. (2006). The investigation and prosecution of a cybercrime. In R. D. Clifford (Ed.), *Cybercrime: The investigation, prosecution and defense of a computer-related crime* (2nd ed.). North Carolina: Carolina Academic Press, p. 162.
[132]454 F. Supp. 2d 999, 1004 (C.D. Cal. 2006), rev'd, 533 F. 3d 1003 (9th Cir. 2008).
[133]*Kerr v. United States*, 426 U.S. 394, 405 (1976).
[134]*Kerr v. United States*, 426 U.S. 394, 406 (1976); *United States v. Nixon*, 418 U.S. 683 (1974); *United States v. Reynolds*, 345 U.S. 1 (1953).
[135]No. 04-1136, 2006 U.S. Dist. LEXIS 65973 (D.D.C. Sept. 15, 2006).
[136]211 F.R.D. 31 (D. Conn. 2002).
[137]See, for example, *United States v. Neill*, 952 F. Supp. 834, 840-841 (D.D.C. 1997).
[138]153 F.R.D. 55, 59 (S.D.N.Y. 1994).
[139]914 F. Supp. 519 (S.D. Fla. 1995).
[140]13 F. Supp. 2d 574, 578 (D. Vt. 1998).