Chapter 1

Searching and Seizing Computers Without a Warrant

A. Introduction

The Fourth Amendment limits the ability of government agents to search for and seize evidence without a warrant. This chapter explains the constitutional limits of warrantless searches and seizures in cases involving computers.

The Fourth Amendment states:

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.

According to the Supreme Court, a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." United States v. Jacobsen, 466 U.S. 109, 113 (1984), and the Court has also characterized the interception of intangible communications as a seizure. Furthermore, the Court has held that a "'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." If the government's conduct does not violate a person's "reasonable expectation of privacy," then formally it does not constitute a Fourth Amendment "search" and no warrant is required. In addition, a warrantless search that violates a person's reasonable expectation of privacy will nonetheless be constitutional if it falls within an established exception to the warrant requirement. Accordingly, investigators must consider two issues when asking whether a government search of a computer requires a warrant. First, does the search violate a reasonable expectation of privacy? And if so, is the search nonetheless permissible because it falls within an exception to the warrant requirement?

B. The Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers

1. General Principles

A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy. This inquiry embraces two discrete questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" In most cases, the difficulty of
contesting a defendant's subjective expectation of privacy focuses the analysis on the objective aspect of
the *Katz* test, *i.e.*, whether the individual's expectation of privacy was reasonable.

No bright line rule indicates whether an expectation of privacy is constitutionally reasonable. For example,
the Supreme Court has held that a person has a reasonable expectation of privacy in property located
inside a person's home; in "the relative heat of various rooms in the home" revealed through the use of a
thermal imager; in conversations taking place in an enclosed phone booth; and in the contents of opaque
containers. In contrast, a person does not have a reasonable expectation of privacy in activities
conducted in open fields; in garbage deposited at the outskirts of real property; or in a stranger's house
that the person has entered without the owner's consent in order to commit a theft.

**2. Reasonable Expectation of Privacy in Computers as Storage Devices**

To determine whether an individual has a reasonable expectation of privacy in information stored in a
computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The
Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in
a computer if it would be prohibited from opening a closed container and examining its contents in the
same situation.

The most basic Fourth Amendment question in computer cases asks whether an individual enjoys a
reasonable expectation of privacy in electronic information stored within computers (or other electronic
storage devices) under the individual's control. For example, do individuals have a reasonable
expectation of privacy in the contents of their laptop computers, USB drives, or cell phones? If the answer
is "yes," then the government ordinarily must obtain a warrant, or fall within an exception to the warrant
requirement, before it accesses the information stored inside.

When confronted with this issue, courts have analogized the expectation of privacy in a computer to the
expectation of privacy in closed containers such as suitcases, footlockers, or briefcases. Because
individuals generally retain a reasonable expectation of privacy in the contents of closed containers, they
also generally retain a reasonable expectation of privacy in data held within electronic storage devices.
Accordingly, accessing information stored in a computer ordinarily will implicate the owner's reasonable
expectation of privacy in the information.

Although courts have generally agreed that electronic storage devices can be analogized to closed
containers, they have reached differing conclusions about whether a computer or other storage device
should be classified as a single closed container or whether each individual file stored within a computer
or storage device should be treated as a separate closed container. In two cases, the Fifth Circuit
determined that a computer disk containing multiple files is a single container for Fourth Amendment
purposes. First, in *United States v. Runyan*, 275 F.3d 449, 464-65 (5th Cir. 2001), in which private parties
had searched certain files and found child pornography, the Fifth Circuit held that the police did not
exceed the scope of the private search when they examined additional files on any disk that had been, in
part, privately searched. Analogizing a disk to a closed container, the court explained that "police do not
exceed the private search when they examine more items within a closed container than did the private
searchers." In a subsequent case, the Fifth Circuit held that when a warrantless search of a portion of a
computer and zip disk had been justified, the defendant no longer retained any reasonable expectation of
privacy in the remaining contents of the computer and disk, and thus a comprehensive search by law enforcement personnel did not violate the Fourth Amendment.

Other appellate courts have treated individual computer files as separate entities, at least in the search warrant context. Similarly, the Tenth Circuit has refused to allow such exhaustive searches of a computer's hard drive in the absence of a warrant or some exception to the warrant requirement. In particular, the Tenth Circuit cautioned in a later case that "[b]ecause computers can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer."

Although individuals generally retain a reasonable expectation of privacy in computers under their control, special circumstances may eliminate that expectation. For example, an individual will not retain a reasonable expectation of privacy in information that the person has made openly available. Thus, several courts have held that a defendant has no reasonable expectation of privacy in files shared freely with others. Similarly, in United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), agents looking over the defendant's shoulder read the defendant's password from the screen as the defendant typed his password into a handheld computer. The court found no Fourth Amendment violation in obtaining the password because the defendant did not enjoy a reasonable expectation of privacy "in the display that appeared on the screen." Nor will individuals generally enjoy a reasonable expectation of privacy in the contents of computers they have stolen or obtained by fraud.

3. Reasonable Expectation of Privacy and Third-Party Possession

Individuals who retain a reasonable expectation of privacy in stored electronic information under their control may lose Fourth Amendment protections when they relinquish that control to third parties. For example, an individual may offer a container of electronic information to a third party by bringing a malfunctioning computer to a repair shop or by shipping a floppy diskette in the mail to a friend. Alternatively, a user may transmit information to third parties electronically, such as by sending data across the Internet, or a user may leave information on a shared computer network. When law enforcement agents learn of information possessed by third parties that may provide evidence of a crime, they may wish to inspect it. Whether the Fourth Amendment requires them to obtain a warrant before examining the information depends in part upon whether the third-party possession has eliminated the individual's reasonable expectation of privacy.

To analyze third-party possession issues, it helps first to distinguish between possession by a carrier in the course of transmission to an intended recipient and subsequent possession by the intended recipient. For example, if A hires B to carry a package to C, A's reasonable expectation of privacy in the contents of the package during the time that B carries the package on its way to C may be different than A's reasonable expectation of privacy after C has received the package. During transmission, contents generally retain Fourth Amendment protection. The government ordinarily may not examine the contents of a closed container in the course of transmission without a warrant. Government intrusion and examination of the contents ordinarily violates the reasonable expectation of privacy of both the sender and receiver.
Government acquisition of an intangible electronic signal in the course of transmission may also implicate the Fourth Amendment. The boundaries of the Fourth Amendment in such cases remain hazy, however, because Congress addressed the Fourth Amendment concerns identified in Berger by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), 18 U.S.C. §§ 2510-2522. Title III, which is discussed fully in Chapter 4, provides a comprehensive statutory framework that regulates real-time monitoring of wire and electronic communications. Its scope encompasses, and in many significant ways exceeds, the protection offered by the Fourth Amendment. As a practical matter, then, the monitoring of wire and electronic communications in the course of transmission generally raises many statutory questions, but few constitutional ones.

Individuals lose Fourth Amendment protection in their computer files if they relinquish control of the files.

Ordinarily, once an item has been received by the intended recipient, the sender’s reasonable expectation of privacy in the item terminates. More generally, the Supreme Court has repeatedly held that the Fourth Amendment is not violated when information revealed to a third party is disclosed by the third party to the government, regardless of any subjective expectation that the third parties will keep the information confidential. For example, in United States v. Miller, 425 U.S. 435, 443 (1976), the Court held that the Fourth Amendment does not protect bank account information that account holders divulge to their banks. By placing information under the control of a third party, the Court stated, an account holder assumes the risk that the information will be conveyed to the government. Id. According to the Court, “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”

Courts have applied these principles to electronic communications. For example, in United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986), the defendant emailed confidential pricing information relating to his employer to his employer’s competitor. After the FBI searched the competitor’s computers and found the pricing information, the defendant claimed that the search violated his Fourth Amendment rights. The Fourth Circuit disagreed, holding that the defendant relinquished his interest in and control over the information by sending it to the competitor for the competitor’s future use.

Defendants will occasionally raise a Fourth Amendment challenge to the acquisition of account records and subscriber information held by Internet service providers where law enforcement obtained the records using less process than a search warrant. As discussed in Chapter 3.D, the Stored Communications Act permits the government to obtain transactional records with an “articulable facts” court order and specified subscriber information with a subpoena. These statutory procedures comply with the Fourth Amendment because customers of communication service providers do not have a reasonable expectation of privacy in customer account records maintained by and for the provider’s business. This rule accords with prior cases finding no Fourth Amendment protection in customer account records. Similarly, use of a pen register to capture email to/from address information or Internet Protocol addresses of websites provided to an Internet service provider for routing communications does not implicate the Fourth Amendment.
Although an individual normally loses a reasonable expectation of privacy in an item delivered to a recipient, there is an exception to this rule when the individual can reasonably expect to retain control over the item and its contents. When a person leaves a package with a third party for temporary safekeeping, for example, she usually retains control of the package and thus retains a reasonable expectation of privacy in its contents.

In some cases, the sender may initially retain a right to control the third party's possession, but may lose that right over time. The general rule is that the sender's Fourth Amendment rights dissipate as the sender's right to control the third party's possession diminishes. For example, in United States v. Poulsen, 41 F.3d 1330 (9th Cir. 1994), overruled on other grounds United States v. W. R. Grace, 526 F.3d 499 (9th Cir. 2008) (en banc) computer hacker Kevin Poulsen left computer tapes in a locker at a commercial storage facility but neglected to pay rent for the locker. Following a warrantless search of the facility, the government sought to use the tapes against Poulsen. The Ninth Circuit held that the search did not violate Poulsen's reasonable expectation of privacy because under state law Poulsen's failure to pay rent extinguished his right to access the tapes.

4. Private Searches

The Fourth Amendment "is wholly inapplicable 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." As a result, no violation of the Fourth Amendment occurs when a private individual acting on his own accord conducts a search and makes the results available to law enforcement. According to Jacobsen, agents who learn of evidence via a private search can reenact the original private search without violating any reasonable expectation of privacy. What the agents cannot do without a warrant is "exceed[] the scope of the private search." This standard requires agents to limit their investigation to the scope of the private search when searching without a warrant after a private search has occurred. Where agents exceed the scope of the private warrantless search, any evidence uncovered may be vulnerable to a motion to suppress.

Private individuals often find contraband or other incriminating evidence on computers and bring that information to law enforcement, and the private search doctrine applies in these cases. In one common scenario, an individual leaves his computer with a repair technician. The technician discovers images of child pornography on the computer, contacts law enforcement, and shows those images to law enforcement. Courts have agreed that such searches by repairmen prior to their contact with law enforcement are private searches and do not implicate the Fourth Amendment.

One private search question that arises in computer cases is whether law enforcement agents must limit themselves to only files examined by the repair technician or whether all data on a particular storage device is within the scope of the initial private search. The Fifth Circuit has taken an expansive approach to this question. Under this approach, a third-party search of a single file on a computer allows a warrantless search by law enforcement of the computer's entire contents. Other courts, however, may not follow the Fifth Circuit's approach and instead rule that government searchers can view only those files whose contents were revealed in the private search. Even if courts follow the more restrictive
approach, the information gleaned from the private search will often provide the probable cause needed to obtain a warrant for a further search.

Importantly, the fact that the person conducting a search is not a government employee does not always mean that the search is "private" for Fourth Amendment purposes. A search by a private party will be considered a Fourth Amendment government search "if the private party act[s] as an instrument or agent of the Government." The Supreme Court has offered little guidance on when private conduct can be attributed to the government; the Court has merely stated that this question "necessarily turns on the degree of the Government's participation in the private party's activities, . . . a question that can only be resolved 'in light of all the circumstances.'"

In the absence of a more definitive standard, the various federal Courts of Appeals have adopted a range of approaches for distinguishing between private and government searches. About half of the circuits apply a "totality of the circumstances" approach that examines three factors: whether the government knows of or acquiesces in the intrusive conduct; whether the party performing the search intends to assist law enforcement efforts at the time of the search; and whether the government affirmatively encourages, initiates, or instigates the private action. This test draws a line between situations where the government is a mere knowing witness to the search and those where the government is an active participant or driving force. However, this line can be difficult to discern. For example, in United States v. Smith, 383 F.3d 700 (8th Cir. 2004), police detectives participating in "parcel interdiction" at Federal Express removed a suspicious package from a conveyor belt, submitted it to a canine sniff, and delivered the package to the Federal Express manager, telling the manager that "if she wanted to open it that would be fine." However, because the police did not actually ask or order the manager to open the package, and because there was no evidence that the manager felt obligated to open the package, the Court found that the manager was not a "government agent" for Fourth Amendment purposes. By contrast, in United States v. Souza, 223 F.3d 1197 (10th Cir. 2000), the Court found that a UPS employee was a government agent. In Souza, the police identified and removed the package from the conveyor belt, submitted it to a canine sniff, and told the UPS employee that they suspected it contained drugs. The police then told the employee that they could not tell her to open the package, but they pointed to it and said "but there it is on the floor." Id. at 1200. The employee began to open the package, but when she had difficulty, the police assisted her. While the officers' actual aid in opening the package made this an easy case, the Court's analysis suggests that the officers' other actions--identifying the package and encouraging the employee to open it--might have made the employee a government agent, particularly without evidence that the employee had an independent motivation to open it.

Other circuits have adopted more rule-like tests that focus on only the first two factors.

Two noteworthy private search cases involve an individual who hacked into computers of child pornographers for the purpose of collecting and disclosing evidence of their crimes. The hacker, who refused to identify himself or meet directly with law enforcement, emailed the incriminating evidence to law enforcement. In both cases, the evidence was admissible because when it was gathered, the individual was not an agent of law enforcement. In the first case, United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003), the court had little difficulty in determining that the search did not implicate the Fourth Amendment. Because the relevant searches by the hacker took place before the hacker contacted law enforcement, the hacker was not acting as a government agent, and the private search doctrine applied.
In the *Steiger* case, a law enforcement agent thanked the anonymous hacker, assured him he would not be prosecuted, and expressed willingness to receive other information from him. Approximately a year later (and seven months after his last previous contact with law enforcement), the hacker provided to law enforcement information he had illegally obtained from another child pornographer, which gave rise to *United States v. Jarrett*, 338 F.3d 339 (4th Cir. 2003). In *Jarrett*, the court ruled that although “the Government operated close to the line,” the contacts in *Steiger* between the hacker and law enforcement did not create an agency relationship that carried forward to *Jarrett*. Moreover, although the government created an agency relationship through further contacts with the hacker during the second investigation, that agency relationship arose after the relevant private search and disclosure. *See id.* at 346. Thus, the hacker’s private search in *Jarrett* did not violate the Fourth Amendment.

5. Use of Specialized Technology to Obtain Information

The government's use of innovative technology to obtain information about a target can implicate the Fourth Amendment. *See Kyllo v. United States*, 533 U.S. 27 (2001). In *Kyllo*, the Supreme Court held that the warrantless use of a thermal imager to reveal the relative amount of heat released from the various rooms of a suspect’s home constituted a search that violated the Fourth Amendment. In particular, the Court held that where law enforcement “uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without a physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.” Whether a technology falls within the scope of the *Kyllo* rule depends on at least two factors. First, the use of technology should not implicate *Kyllo* if the technology is in “general public use,” although courts have not yet defined the standard for determining whether a given technology meets this requirement. Second, the Supreme Court restricted its holding in *Kyllo* to the use of technology that reveals information about the interior of the home.

Defendants have occasionally--and unsuccessfully--invoked *Kyllo* in cases in which the government used cell tower information or an electronic device to locate a cell phone. For example, in *United States v. Bermudez*, 2006 WL 3197181 (S.D. Ind. June 30, 2006), aff'd 509 F.3d 820 (7th Cir. 2007), the court rejected a *Kyllo* challenge to the use of an electronic device to locate a cell phone because cell phones are used to transmit signals to parties outside a home. In rejecting the defendant's *Kyllo* argument, the court explained that "the cell phone signals were knowingly exposed to a third-party, to wit, the cell phone company."