The background of the cover is a detailed, high-contrast image of a computer circuit board. The board is dark, with various components, traces, and connectors highlighted in bright colors like red, green, blue, and yellow. The overall effect is a complex, technical aesthetic.

J Georgia Bar Journal

Journal

February 2009 • Volume 14 • Number 5

The Fourth Amendment and Computers:
Is a Computer Just Another Container or Are New
Rules Required to Reflect New Technologies?

The Fourth Amendment and Computers:

Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?

by Edward T.M. Garland and Donald F. Samuel

One hundred years ago, there was no “automobile exception” to the search warrant requirement.¹ Of course, there were no automobiles in the 18th century when the Fourth Amendment,² which bars unreasonable searches and seizures, was adopted as part of the Bill of Rights. Determining what is reasonable with regard to automobile searches needed to be decided for circumstances not envisioned by the authors of the Fourth Amendment.

Over the past 100 years, the U.S. Supreme Court has established a set of rules that govern the searching and seizing of automobiles, drivers and passengers. Dozens of Supreme Court decisions have focused on when automobiles may be stopped and searched; when drivers and passengers may be stopped and searched; and the duration and intensity of searches of the occupants, their luggage and the vehicle itself.

There were no computers in the 18th century, either.

It has taken 100 years for the Court to announce dozens of rules that set forth exactly what the police may and may not do when it comes to stopping and searching automobiles, but it could take more than that to craft a set of rules that address the unique problems confronting the police and citizens when it comes to searching for, and seizing, information contained in computers.

Although there is considerable debate about whether traditional Fourth Amendment jurisprudence can adequately address any issue that arises in the context of a computer search, or whether an entirely new set of rules is needed,³ the fact of the matter is that the computer presents new and intriguing problems in the area of the Fourth Amendment, regardless of whether the courts ultimately rely on adapting old rules to solve the problems, or adopting new rules to reflect the technologies.

Law enforcement agents’ increasing reliance on computer seizures reflects the undeniable fact that computers not only contain evidence of criminal wrongdoing, but are primary tools in perpetrating crimes: “The computer facilitates the terrorist organization’s ability to train its members, spread propaganda and case its targets, just as it helps the identity thief locate his victims, the pornograph-

er to collect and view child pornography and the fraudster to generate fake documents.”⁴ According to the U.S. Census Bureau, in 2003, there were over 70 million households with laptop computers—roughly 62 percent of all households.⁵

When the Supreme Court decided *Kyllo v. United States*⁶ eight years ago, the same dilemma confronted the Court: How should the Court apply a 200 year-old right to be free from unreasonable searches and seizures to circumstances (the ability to measure by thermal imaging the heat emanating from a house) that were unimaginable to the founding fathers? Justice Scalia wrote for the majority, “It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”⁷ Indeed, the traditional boundaries of current Fourth Amendment law, including the foundational requirements of expectation of privacy and particularity, to say nothing of the concepts embodied in the various exceptions to the search warrant requirement, were written by the Court when the most technologically advanced instrument was a slide rule.⁸

How, then, should a court consider whether to issue a search warrant for the search and seizure of a computer? When does a person have a reasonable expectation of privacy in the contents of a computer, and does it make a difference if the computer is used at the workplace, or is shared by other people? Must there be a showing that the target computer is likely to contain evidence or contraband, or is it assumed that *all* suspects’ computers contain such evidence if the suspect is shown to be a criminal? Should the police be permitted to seize a computer when a warrant authorizes the seizure of “documents” or “records” or “other evidence of a crime” if the warrant does not expressly permit the seizure of computers or disks in the “to be seized” paragraph of the warrant? How are the search war-

rant exceptions such as consent searches, searches incident to arrest and inventory searches, to be applied when the target is a computer? Are there any limits to what the police can do once they seize the computer? May they look throughout its entire contents? May they do so for days, or weeks or months? May they use sophisticated forensic tools to discover what was deleted years ago, or never even viewed by the computer’s owner?

When considering the application of the Fourth Amendment to computers, consider the following:

- In a typical laptop computer that a consumer buys, a person can save hundreds of thousands of documents, *totaling millions of pages*. This is the equivalent of several thousand bankers boxes of paper. The laptop on which this article was composed can save nearly 600,000 articles of this length.⁹
- The computer will enable the user to access all e-mails previously sent and received for as long as the subscriber has been using e-mail communication (compare that to the “old days” when telephone messages—“While You Were Out” slips—and correspondence were haphazardly catalogued, archived or simply incinerated).¹⁰
- The computer records and “remembers” every Internet site that the computer has visited, sometimes going back for years. The computer also stores the information about every Internet search conducted on the computer.¹¹
- Internet cache files store every picture that has come across the computer from the Internet, including those that “pop-up” and were not consciously retrieved or saved by the person sitting at the computer.¹²
- Forensic tools that are available to law enforcement agencies (and, for that matter, the general public), can retrieve thou-

sands of deleted messages, documents, photographs and Internet searches years after the computer user clicked the “delete” button.¹³ Even emptying the recycle bin will not ensure that the information is, in fact, irretrievable.

- In cases involving larger computers or servers (such as those found at various businesses that might be the subject of a search in a white-collar case), the above statistics increase exponentially.¹⁴

It is no more practical for one to set forth a compact set of rules to govern the searching and seizing of computers today than it would have been reasonable for a scholar to create an entire set of rules for the searching and seizing of automobiles when the first Model T rolled off the assembly line at the Piquette Avenue Plant in Detroit on Sept. 27, 1908. Indeed, it would have been much easier to enact an entire code to guide the police with respect to the searches of automobiles 100 years ago than it would be to promulgate rules for computer searches today. After all, a luxury-class Hummer isn’t that much different from a Model T, but the computers of tomorrow will bear very little resemblance to the computers of today. The day is very near when computers and tracking devices in our homes—inside our refrigerators, our home theaters, our home security systems, our cars, as well as our personal laptop computers—will be connected to the outside world in such a way that the necessity for the police actually to enter the house to conduct a search (and seize the hardware) will be laughably antiquated before the ink dries on our hypothetical new rules. Tomorrow, police investigators will simply get a warrant (hopefully), enter our computers from their precincts and obtain all the information that they desire.

The Constitution is not the only limitation on invasions of privacy. Congress and state legislatures can also enact rules that govern access



to electronic data. Congress, for example, has concluded that Title III (the federal wiretap statute) applies to e-mails.¹⁵ Thus, the more rigorous Title III requirements must be satisfied before e-mails can be intercepted. With regard to stored e-mails (i.e., e-mails stored at AOL or Yahoo!), Congress enacted the Stored Wire and Electronic Communications and Transactional Records Access Act, which prescribes specific rules regarding law enforcement agents' ability to obtain copies of a person's e-mails from those institutions.¹⁶ This article only addresses the constitutional issues raised in the context of computer searches.

Issues of Standing/ Expectation of Privacy

A party alleging an unconstitutional search under the Fourth Amendment must establish both a subjective and an objectively reasonable expectation of privacy in order to succeed in an effort to suppress the fruits of that search. The subjective component requires that a person exhibit an actual expectation of privacy, while the objective

component requires that the privacy expectation be one that society is prepared to recognize as reasonable.¹⁷ Obviously, a person has an expectation of privacy in the contents of a computer, just as he or she would have an expectation of privacy in a briefcase or file cabinet.¹⁸ Certain unique features of a computer, however, render such a simplistic analysis problematic in certain circumstances.

First, of course, a computer may be shared by many people, thus enabling more than one person the ability to consent to a search of the contents. Rarely is a person's briefcase a shared container. A woman's purse is generally not equally accessible to her spouse, but computers are frequently shared by members of the family. The children play video games on the computer, and the adults might have separate e-mail accounts. Indeed, different users may even have their own passwords that they might, or might not, share with other users.

Second, at work, a computer may be subject to certain work-related rules regarding access by the employer. The computer may also be connected to a server that enables

the contents to be viewed by countless other employees, thus negating any expectation of privacy.

Third, much of the contents of the computer might represent communications with another person (e-mails) or another entity. These communications, unlike phone calls, which "exist" only during the course of the communication (unless recorded by a participant), endure for a virtual eternity in the computer's archives or the Internet provider's server.

With regard to workplace computers, the basic law is clear. Generally, a person has an expectation of privacy in his personal work space at a private place of employment.¹⁹ The Supreme Court has also recognized an expectation of privacy for public employees with respect to searches conducted by their employers.²⁰

Courts have extended these cases to the employee's computer at his work station, but this expectation of privacy may be limited or even eliminated by workplace rules and protocols that expressly advise employees that their computers are subject to being audited or reviewed by agency personnel.

When an employer expressly informs employees that the contents of the computer will be monitored and examined, some courts have found no expectation of privacy.²¹

In *United States v. Ziegler*,²² the U.S. Court of Appeals for the 9th Circuit held that an employee of a business had a reasonable expectation of privacy in his computer, even though his computer was provided by the company and he connected his computer to the company's server, which was known to have a firewall that enabled the company's IT employees to review the computer's Internet activity. Despite the accessibility of the computer to other employees, the court focused on the facts that the defendant's computer was kept in an office that he did not share with others and that he maintained a password on the computer demonstrating his subjective expectation of privacy.²³

When an employee fails to demonstrate a subjective expectation of privacy, however, courts have not hesitated to find that there was no expectation of privacy to contest a search. In *United States v. King*,²⁴ the U.S. Court of Appeals for the 11th Circuit held that a soldier who connected his laptop to the military base server could not claim a legitimate expectation of privacy in the contents of the computer, including his hard drive, because he knew that other computer users could access information in his hard drive once his computer was connected to the server. The court was unconvinced that any expectation of privacy in the computer was objectively reasonable, even though King installed security settings that inhibited access to his computer by others.

Similarly, in *United States v. Barrows*,²⁵ the U.S. Court of Appeals for the 10th Circuit held that a city employee who connected his laptop to the city computers and left it in an open area of the office, unlocked, not password-protected and switched on even

when he left for the night, failed to demonstrate an expectation of privacy in the computer's contents.

Circumstances arise in which a person loses his expectation of privacy due to the actions of third parties. Thus, a UPS or Federal Express employee, or airline personnel, may open a package or suitcase entrusted to their care. If contraband is discovered, law enforcement may conduct a co-extensive search without obtaining a search warrant. The theory is that there is no additional violation of the defendant's expectation of privacy.²⁶

The 11th Circuit has also applied this reasoning to the situation of a "hacker" who surreptitiously "invaded" the defendant's computer, made copies of the contents and then supplied them to law enforcement. The 11th Circuit held that the "private search" did not implicate the Fourth Amendment.²⁷ Once the information was revealed to law enforcement, a further search did not invoke any Fourth Amendment protection.

What if the content of a person's computer has been observed by a repairman and he sees what he suspects is child pornography? To what extent may the police conduct a search without obtaining a warrant? Are the entire contents of the computer no longer subject to an expectation of privacy, or just the file observed by the non-state agent? In *Walter v. United States*,²⁸ the FBI was called by a private party to retrieve certain films that had been mistakenly delivered to the private party. The private party examined the labels on the film canisters, but did not actually view the films. The FBI went beyond what was viewed by the private party, and, therefore, was held (by a plurality opinion of the Court, which announced no unified theory) to have conducted a search that was covered by the Fourth Amendment and for which the defendant retained an expectation of privacy. By analogy, if a repairman views one file in a computer,

this does not vitiate the computer owner's continued expectation of privacy in a separate file.

The question remains, how extensively may the police conduct a search based on a limited view of the target area by the private party? In *United States v. Runyan*,²⁹ the U.S. Court of Appeals for the 5th Circuit held that once a particular disk has been examined by a private person who provides the disk to the police, the entire disk may be examined by the police, not just the file contained on the disk that the private person viewed.³⁰ Other disks, however, which were found in close proximity to the disks containing contraband (and which the private searcher also provided to the police, but did not view prior to relinquishing control to the police), could not be examined by the police until they obtained a warrant. The 5th Circuit based this holding on the limitation of the "private search" exception that limits subsequent police searches to situations where "the police knew with substantial certainty, based on the statements of the private searchers, their replication of the private search, and their expertise, what they would find inside."³¹

In *United States v. Carey*,³² however, the 10th Circuit cautioned that because of the voluminous amount of information on computers, the fact that a person has no expectation of privacy in one file or directory (because, for example, a search warrant authorized the police to search one set of files in the computer) does not mean that other parts of the computer are outside of the defendant's retained zone of privacy.³³ A recent case in the U.S. District Court for the Middle District of Pennsylvania also endorsed this view. In *United States v. Crist*,³⁴ the defendant's computer was discarded by his landlord when he was dispossessed from his apartment. Another person retrieved the computer and in the process of looking through the contents, discovered child pornography. He alerted the police, who seized the computer and conducted a thorough forensic

examination of the computer without first obtaining a search warrant. The government claimed that the search was permissible, because the defendant's expectation of privacy was extinguished by the prior private search. The district court disagreed. Relying on *Runyan*, the court concluded that the more extensive search conducted by the police exceeded the scope of the search that the private party pursued and therefore suppressed the evidence.

Probable Cause to Search or Seize a Computer

In order to obtain a search warrant, the police must demonstrate to a neutral and detached magistrate that there is probable cause to believe that evidence of a crime, or contraband, is located in the place that is the target of the search.³⁵

In some situations, the probable cause basis for searching a computer is obvious. Perhaps someone has already seen contraband on the computer, as in *United States v. King*,³⁶ or perhaps the user of the computer has communicated with someone, such as an undercover police agent, by e-mail or in a chat room. Those are the easy cases. What if there is no direct evidence that the computer has contraband on it, or evidence of a crime, but there is evidence that the owner of the computer is a criminal: a drug dealer, a tax evader or a corrupt public official? Does that fact alone establish probable cause that there is evidence of the crime on the computer?

In *United States v. Zimmerman*,³⁷ the U.S. Court of Appeals for the 3rd Circuit held that information that a person was engaged in sexual misconduct and had shown pornography to students was not sufficient to establish that there was any pornography on his computer. This is one of the few cases in *any* jurisdiction in which a court has held that there was no probable cause to look at a computer of the target.³⁸ With an alarming lack of careful analysis, the Georgia appellate courts have routinely—and

nonchalantly—approved search warrants authorizing the seizure of computers regardless of the apparent lack of specific knowledge that any contraband or evidence could be found on the computer.³⁹ Consider the paucity of legal analysis in these cases:

- *Schwindler v. State*⁴⁰: The information presented to the magistrate established that the defendant molested a student repeatedly and showed him pornographic videotapes (apparently on a television). The court held that this was sufficient probable cause to seize computers at the defendant's house.
- *Blevins v. State*⁴¹: Similar to *Schwindler*, the search warrant application showed that the defendant had committed several acts of child molestation and that he was known to have photographs and videotapes of child pornography. Seizing the defendant's computers was justified based on this information. The Court of Appeals reached the same result in *Birkbeck v. State*, where there was considerable evidence that the defendant had molested his stepdaughter for several years, but no information relating to the use of a computer.
- *Daniels v. State*⁴²: The defendant allegedly molested the victim numerous times. A computer was known to be present in the house, though there was no information about what was on the computer. The seizure of the computer was authorized, because computers "are often used" by child molesters.
- *Lemon v. State*⁴³: The defendant was watching a pornographic videotape (apparently on a television) with his girlfriend, and they were using drugs. They had an argument, and he killed her. The court upheld the search warrant that authorized the seizure of the computer in the house because it might con-

tain evidence regarding the couple's relationship.

- *State v. Henley*⁴⁴: The defendant was known to have acquired illegal pornographic videotapes. A search warrant for computers was authorized, because pornographers use computers.⁴⁵
- *State v. Hall*⁴⁶: Police observed crack cocaine in the defendant's stove. No computer was ever seen at the location, but the officer included "this standard language" about seizing computers in the search warrant, because drug dealers use computers to facilitate drug sales.
- *Dole v. State*⁴⁷: A warrant authorizing the seizure of "INSTRUMENTS OF COMMUNICATION, COMPUTERS" found at the defendant's home (where the defendant was believed to be distributing and receiving Valium and other controlled substances in the mail) was proper, based on the information that the defendant received the drugs at that location.

Although the police need not be clairvoyant and precise about the likelihood of finding evidence of a particular crime on a computer, a formulaic statement that "all drug dealers" maintain records, or "all child pornographers have Internet downloads" or "all tax evaders maintain computerized records" or "anybody suspected of murder who has a computer will have some evidence of his whereabouts at a certain time on his computer" should not suffice. The "nexus" requirement that has always been a critical aspect of the probable cause requirement⁴⁸—that is, the requirement that evidence of the crime will be found at a specific location—should be rigorously enforced when the subject matter is the seizure of a computer. Thus, demonstrating that there is probable cause that the suspect has committed a crime is only half the showing that is required to obtain a warrant to seize the suspect's com-

puter. There must also be probable cause to believe that there is evidence of the crime, or contraband, contained in the computer.

Furthermore, in the Georgia cases cited above, there was not the slightest suggestion that the police were required to be circumspect in the review of the contents of the computers once they were seized. In essence, the search warrants in those cases authorized the police to review virtually every document ever written by the user of the computer, regardless of the content or the date that the document was authored, with nothing more than an assumption that the suspect's computer was likely to have some evidence of his criminal behavior on the computer. The lack of particularity in those warrants is discussed in the next section.

With regard to the "staleness" element of the probable cause determination, it is interesting that because deleted files can be recovered, this issue is less problematic in the case of a computer search. If there is information that a year ago the target downloaded child pornography onto his computer, the evidence will likely still be discoverable using various forensic tools, even if there is unmistakable evidence that the target deleted the images months ago.⁴⁹ Further, if there is evidence that the defendant failed to pay his taxes five years ago, records of his expenditures and income might well still be found on his computer.

The Particularity Requirement

The Fourth Amendment requires that a search warrant particularly describe the place to be searched and the things to be seized.⁵⁰ This core concern of the Fourth Amendment prevents the police from seizing anything that they find of interest in a suspect's house based solely on the fact that he is suspected of committing a particular crime. The police must apply for a warrant that particular-

ly describes what they will be searching for, and the magistrate must issue a warrant particularly describing what may be seized. This limits not only what may be seized, but the places where the police may search.

Does probable cause to believe that some evidence might be found on a computer suffice to authorize a search of the entire computer, or should searches only extend to particular files, such as files with particular extension designations ("jpg," "doc," etc.) or programs that are more likely to contain evidence (or contraband)? Should the police be limited to documents or files created during a certain timeframe? These questions require a consideration of the "particularity" requirement in a context previously unknown in Fourth Amendment jurisprudence.

The particularity requirement prevents law enforcement from executing "general warrants" that permit exploratory rummaging through a person's belongings in search of evidence of a crime.⁵¹ The description of the things to be seized must not be so broad that it encompasses items that should not be seized. The description in the warrant of the things to be seized should be limited by the scope of the probable cause established in the warrant. The particularity requirement ensures that agents conduct narrow seizures that attempt to minimize unwarranted intrusions upon privacy.⁵²

The Georgia courts have addressed the particularity requirement in a number of cases. In *State v. Kramer*,⁵³ for example, the defendant was suspected of molesting children. The police obtained a search warrant that authorized the seizure of any instruments used in the crimes of child molestation. There was no evidence given to the issuing magistrate that the defendant possessed any pornographic videotapes, that the children had been exposed to any videotapes or that the defendant videotaped the children. Nevertheless, the police seized videotapes. The Court of

Appeals held that the trial court properly suppressed the videotape evidence. The general description in the search warrant improperly allowed the police to exercise too much discretion in executing the search warrant. The Court of Appeals, moreover, stated that even if the warrant authorized the seizure of "videotapes" with nothing more, this would not pass constitutional muster.

In *Reaves v. State*,⁵⁴ the Supreme Court of Georgia considered a case in which the police were investigating a case of murder and cruelty to children. The warrant authorized the seizure of any "notes and papers" that would be evidence of the crimes. The court—though not without dissent—held that this clause in the warrant was sufficiently particular.

In *United States v. Riccardi*,⁵⁵ the 10th Circuit held that a search warrant that simply authorized the seizure of all computers, hard drives, floppy disks, removable media drives, etc., was not sufficiently specific, because the warrant did not limit what the FBI could do with the computer information once it was seized. That is, this warrant would enable the police to look through tax records, calendars, e-mails and every other bit of information on the computers and disks, despite the fact that the probable cause basis for the search was evidence that the defendant had obtained child pornography.⁵⁶ As one court succinctly held:

The cases and commentary also draw a distinction between the electronic storage device itself and the information which that device contains. Thus, when the government seeks to seize the information stored on a computer, as opposed to the computer itself, that underlying information must be identified with particularity and its seizure independently supported by probable cause.⁵⁷

Naturally, limiting the police to a search of the files in the computer marked “my criminal activities” is not required. Computer users will not catalogue their information in this way. In fact, even the extensions “jpg” or “doc” can be manipulated at the user’s whim.⁵⁸ Nevertheless, in no Georgia case has *any* effort been made to limit the scope of the search of a computer. At a minimum, the searching officers should face the same restrictions that they would face if they were executing a search warrant in a suspect’s home or office. Indiscriminate rummaging through all the suspect’s belongings for an extended period of time would not be authorized. If the magistrate is persuaded by the warrant application that there is probable cause to believe that the computer contains evidence of the defendant’s whereabouts on a certain date, then the warrant should limit the police (and the forensic agents) to searching the computer for that evidence. If the magistrate is persuaded by the warrant application that there is probable cause to believe that the computer contains evidence of the defendant’s drug dealing activity, then the warrant should limit the police and their forensic colleagues to searching the computer for that evidence. This proposal recognizes that the computer itself is merely the location in which the police might expect to find evidence, and not the end result of the search. Just as a warrant authorizes the police to search a house to find certain evidence (particularly described), the police should be limited in their search of the computer to look for, and seize, particularly described evidence or contraband.

A recent 11th Circuit case⁵⁹ provides some guidance in this area. Federal law enforcement agents targeted a company that was believed to have routinely hired illegal aliens for its work force. A search warrant was obtained that directed agents to seize all computers from the location. Once the computers were seized, however, the warrant expressly limited (at

least to some extent) the search that could be conducted by the agents:

The master affidavit limited the search to specified categories of documents pertaining to a number of businesses and four individuals, and limited the chronological reach of the search to documents and records dating back to 1997. The affidavit also required the search activity to be focused on materials related to specified immigration and tax violations.⁶⁰

Of course, if, while legitimately looking for evidence that the magistrate authorizes the agent to look for, the agent discovers some evidence of another crime, the plain view doctrine will authorize the police to seize that evidence, or as a basis for seeking an additional search warrant to search for evidence of the newly-discovered crime. If the magistrate does not limit the scope of the computer search in the first place, however, there is simply no reason to invoke the plain view doctrine, because the agent would be expressly authorized to search the entire computer for the crime that led to the seizure.

Execution of Search Warrant That Does Not Expressly Identify Computers in the “To Be Seized” Clause

If a search warrant does not specifically authorize the seizure of a computer, may the police seize a computer if the warrant does authorize the seizure of “records” or other evidence of the offenses? This issue is closely related to the particularity requirement in a search warrant. In essence, the question is whether a computer qualifies as a “particularly described” item to be seized if the computer is not specifically identified in the warrant.

In *Marron v. United States*,⁶¹ the Supreme Court held that the Fourth Amendment prohibits general exploratory searches through the particularity requirement. This requirement must be applied with a practical margin of flexibility depending on the type of property to be seized. “The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.”⁶²

In *Military Circle Pet Center No. 94, Inc. v. State*,⁶³ the Court of Appeals considered a case in which a search warrant authorized the seizure of euthanizing drugs, cruelly-treated animals that were sick, animals in a diseased and overcrowded environment and certain business records. Yet the officers seized all drugs, all animals not in perfect health and a wide range of records. The Court of Appeals held that the motion to suppress should have been granted. Although the warrant was based on probable cause and did particularly describe the items that were to be seized, a search that is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope. As to what may be taken, nothing, in theory, is to be left to the discretion of the officer executing the warrant.

In *Cayce v. State*,⁶⁴ the court held that an officer in the process of executing a lawful search warrant is authorized to seize any stolen property, contraband or other item, other than private papers, that he has probable cause to consider tangible evidence of the commission of a crime, even though the property is not listed in the warrant. The discovery of the item must, however, have resulted from a bona fide search for the items named in the warrant. The warrant in this case focused on 400 pounds of marijuana. Once in the house, the police opened a jar of rice,

suspecting that it might contain cocaine. This was permissible.

When executing a search warrant to search for marijuana, officers routinely conduct a thorough search for drugs, lists of customers and any other information tending to establish a drug connection. *Martin v. State*⁶⁵ held that this is permissible and authorizes the review of papers that constitute evidence of another crime.

How do these rules apply to the seizure of computers? Several cases have held that if the warrant authorizes the seizure of records of drug-dealing, fraud or "other evidence of child pornography," the police may seize a computer at the site of a search, even if they have no idea what is actually contained on the computer.⁶⁶

In Georgia, however, a 1996 Court of Appeals decision, *Grant v. State*,⁶⁷ held that if the warrant did not specify a computer (or computer disks) as the items to be seized, those items could not be seized, even if the items that were permitted to be seized could be found on the computer. In this white-collar crime case, the warrant authorized the seizure of many different types of documents associated with a timber fraud scheme, including various deeds, correspondence and financial documents. The police seized various documents and computers and computer disks:

This was not a situation in which additional contraband was seized during the search because it was in plain view. . . . Moreover, the "[p]lain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." . . .

Here, the inventory list of the items seized and [the officer's] testimony established that the scope of the search exceeded the warrant, and the Court properly determined that the search was excessive. We find no legal support for the Court's

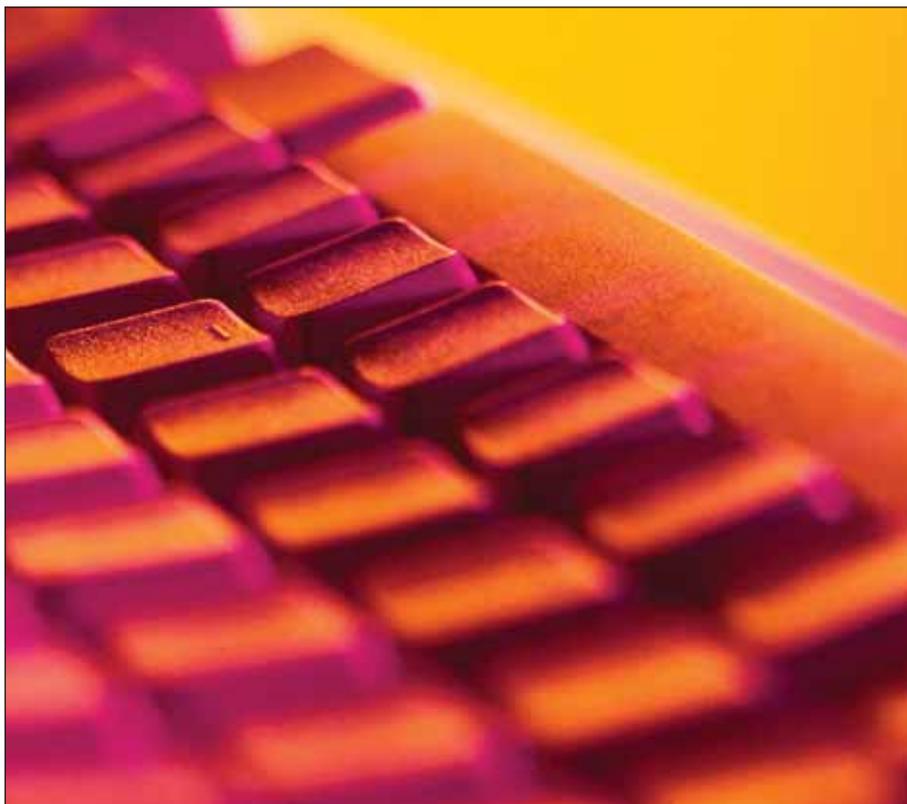
decision that practical considerations and time constraints justified the overly extensive search. Moreover, there is no factual support for this conclusion since many of the items seized which were outside the scope of the warrant (e.g., the computer, calendar) were unrelated to time constraints.⁶⁸

Post-Seizure Conduct

The typical search of a house, of course, involves the presence of numerous law enforcement agents, armed with a warrant specifically identifying what they are permitted to seize. The officers enter the premises and look through all the closets, desks and under the mattress. Items that match the description of the items identified in the "to be seized" clause are seized. Other items that satisfy the plain view standard⁶⁹ are also seized. Then the police leave. With the seizure of computers, however, that is only the beginning of the searching process. Once the computer is removed from the house, it may be delivered to a forensic lab (either at one of numerous federal agencies, or at the GBI

Crime Lab) where the contents of the computer may be examined for hours, days, weeks or years. This occurs regardless of whether the police actually know, at the time of the seizure, that any contraband or evidence of a crime is anywhere on the computer. It does not matter whether the warrant identified computers in the "to be seized" clause, the computer was seized because it qualified as a "record" that was permitted to be seized or it was simply seized because the police believed that it satisfied the definition of a plain view seizure.

When the search of the computer commences, the forensic agent needs to determine whether the magistrate delineated any limits on the scope of the search. That is, did the magistrate satisfy the Fourth Amendment's particularity requirement, as discussed above, by limiting what the agents could look for on the computer? If such limitations exist, the agent must honor those limitations.⁷⁰ Although it may be argued that any such limitation would frustrate law enforcement's legitimate goal of finding evidence of a



crime,⁷¹ there are limits on what the police can do in a home, too, that frustrates their efforts to find every shred of evidence. After all, when searching for drugs or documents in a home, the police are not routinely permitted to tear the walls down and dissect the studs in the walls, remove the floorboards or dig up the back yard. The fact that a search of a computer, limited by the particularity clause, might cause the police to “miss” some evidence is the result of the Fourth Amendment and its particularity and reasonable-ness requirements. The Fourth Amendment causes evidence to be missed every day.

Even if the magistrate has imposed a limit on the scope of the actual search of the contents of the computer, *everything* is suddenly in plain view, and the police have limitless access and ability to view the entire contents of the computer for as long as they desire. Any discovery of evidence that was not envisioned by the search warrant might qualify as a plain view discovery under the traditional definition—the police have the right to be where they are; the document or picture is immediately apparent to be contraband or evidence of a crime—but the discovery of evidence on a computer that is being examined in a forensic laboratory is hardly what the Supreme Court had in mind when the plain view doctrine was first recognized 35 years ago.⁷²

Of course, a principal concern when the police seize computers and disks based on a warrant that authorizes the seizure of records is the length of time that the police may keep the computers and disks in order to determine *whether* these containers include evidence or contraband. Imagine, by analogy, that the police were authorized to search for cocaine at a suspect’s house and that they entered the house and simply took every container—every suitcase, every chest of drawers, every box—and left with these

containers, not knowing what was in them! Imagine that the containers were brought to the crime lab, where they were kept for weeks or months, while technicians went through every square inch of the containers. If this scenario seems inconsistent with the Fourth Amendment, imagine that one of these boxes contains every document that the suspect has written in the past five years, including diaries, favorite recipes and letters to his mistress; every newspaper article that he has read; every picture that he has taken at every family gathering (or at every orgy that he has attended). How does this type of seizure and search (and it should be stressed that the police seize first and search later) square with the limitations of the Fourth Amendment?

In large white-collar crime investigations, the courts have generally approved the removal of file cabinets and computers from the location of a search, even if the contents are not known, in order to *reduce* the length of time that the search takes place on site.⁷³ Generally, these are cases in which the magistrate has approved the removal of a large volume of documents because of the likelihood that evidence of fraudulent invoices or forged contracts will be found among the thousands or millions of documents on site. When such searches occur at a business suspected of being involved in massive fraudulent activities, one hardly senses a major Fourth Amendment violation. When such seizures occur from one’s home based on the alleged commission of a single crime, it is a different matter.

The general rule is that the police may not seize *every* document in a person’s home if the investigation focuses on a particular crime that does not necessitate the careful review of thousands of pages of documents. In the 9th Circuit decision in *United States v. Tamura*,⁷⁴ the court cautioned against this type of limit-

less dragnet seizure even in the case of a company:

It is highly doubtful whether the wholesale seizure by the government of documents not mentioned in the warrant comported with the requirements of the fourth amendment. As a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized. . . . It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search. . . . However, the wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as “the kind of investigatory dragnet that the fourth amendment was designed to prevent.” . . . We cannot sanction the procedure followed by the government in this case.⁷⁵

Yet that is precisely what occurs every time the police seize a person’s computer. Thus, while in the large white-collar case, the seizure of all the file cabinets in the corporate offices may be reasonable, in a typical case involving a search for particularly described evidence, the seizure of a person’s computer results in the *de facto* seizure of all the suspect’s private papers that have been received or written for the past several years. In virtually every case in which computers are seized, they are removed from the premises for an extended period of time, and the search of the owner’s private papers—thousands, if not millions of documents—goes on for a virtually unlimited period of time.

How to limit the scope of the police search of a computer has never been satisfactorily decided. It is simply accepted practice that the

police may look through the entire contents of a computer without any further participation by a magistrate, simply on the basis that the computer *might* contain some evidence of a crime. This practice is incompatible with the requirements of the Fourth Amendment's particularity requirement or the plain view doctrine, and does not satisfy the reasonableness standard any more than a wholesale removal of every piece of paper in a suspect's house — no matter what the crime is — would be tolerated.

Some courts that have considered this problem conclude that the Fourth Amendment's "reasonableness" standard controls the length of time that the police may keep a computer and conduct the search.⁷⁶ In *United States v. Brunette*,⁷⁷ the magistrate ordered that the forensic search of the defendant's computers be conducted within the first 30 days of the seizure. The agents' failure to comply with this requirement led to the suppression of certain evidence. A recent case in Washington, however, held that the statutory 10-day limitation on the validity of a warrant does not apply to the search of a computer that has been seized pursuant to a lawful search warrant.⁷⁸

The issue is complicated by the fact that once contraband is found on a computer (child pornography, for example) or once it is determined that the computer is an instrumentality of the crime (drug ledgers, for example), the computer is subject to forfeiture under both state and federal forfeiture laws,⁷⁹ and the owner's possessory interest is reduced, if not non-existent. In addition, the police will often make a mirror of the entire computer and return the computer itself to the owner, keeping the exact duplicate. Whether this retention of a copy of the entire computer — all the Word documents, all the e-mails, all the Internet searches, all the calendars and journals — for an eternity is "reasonable" or consistent with our concept of a right of privacy, remains to be decided.

CERTIFIED POLYGRAPH EXPERT

IMBORDINO POLYGRAPH EXAMINATIONS, LLC

"When the Need for the Truth is Important"

- FORMER FEDERAL POLYGRAPH SUPERVISOR
- 21 YEARS OF POLYGRAPH EXPERIENCE
- EXPERT WITNESS
- AMERICAN POLYGRAPH ASSOCIATION
- AMERICAN COLLEGE OF FORENSIC EXAMINERS
- APA CERTIFIED POLYGRAPH INSTRUCTOR

DONALD J. IMBORDINO

(678) 986-9600

E-mail: dimbordino@earthlink.net Web site: www.lmbordinoPolygraph.com

Business Valuations

Divorces • Estate/Gifts • ESOPs • Disputes • Fairness Opinions
Family Limited Partnerships • Intangible Assets

Mitchell Kaye, CFA, ASA

(770) 998-4642

e-mail: Valuation@MitchellKaye.com

American Society of Appraisers • Past President, Atlanta Chapter
Chartered Financial Analyst

servicing appraisal clients since 1981

Court Testimony / IRS Experience

ARTHUR T. ANTHONY

**Certified Forensic Handwriting and
Document Examiner**

(770) 338-1938

Diplomate-American Board of Forensic Document Examiners
American Society of Questioned Document Examiners
American Academy of Forensic Sciences

P.O. Box 620420
Atlanta, Georgia 30362

Practice Limited to Civil Matters

EXPERT WITNESS: Forensic Accounting • Financial Fraud

M. Martin Mercer, JD, CPA, FCPA, CFE

7768 S. Steele St., Centennial, CO 80122 • Phone: (303) 621-5825

Website: www.MMartinMercer.com • E-mail: mmercerc@b2bcfo.com

Specialization: Mr. Mercer leads the B2B CFO® Litigation Services Practice which offers to litigating attorneys over 85 partners averaging 25 years of experience in finance, accounting, business valuations, litigation support, financial fraud investigations, forensic accounting, and expert witness services. Mr. Mercer is an attorney and a CPA as well as a Certified Fraud Examiner (CFE) and Forensic CPA with over 25 years of experience in all aspects of finance, accounting, financial fraud, litigation support, and forensic accounting.

Should a search warrant be bifurcated, initially authorizing the seizure of the hardware (the physical computer itself, despite the fact that the vast majority of information on the computer will not be evidence of a crime) and then detailing what the “forensic” examiners may examine—that is, the “files” or directories that are likely to contain evidence of the crime? Or is the judge’s job simply to authorize the seizure of the entire computer, and the rest is left to the police?

A federal court in Illinois concluded that the government would be required to detail its “search protocol” prior to commencing its search, though the court approved the seizure of the target’s computer.⁸⁰ The court required the government to explain how it intended to minimize the intrusion into areas that were not likely to include such evidence.

For an example of a warrant that prescribed various limitations on the search method, consider the case of *United States v. Triumph Capital Group, Inc.*⁸¹ The magistrate authorized the search of the entire hard drive, but required that (1) certain keyword searches be conducted to minimize the intrusion; (2) in addition to keyword searches, the searching agents would be entitled to do certain manual searches through directories and folders; (3) a “taint team” would be required, which would comprise of prosecutors not involved in the investigation, who would make sure that no privileged information was shared with the prosecutors who were involved in the case; and (4) the search would be conducted pursuant to rigorous protocols that would protect the integrity of the information.

Some courts have *required* that the government use various forensic tools (not just a rudimentary “word search”) to limit the government’s intrusion into sensitive information that has no relevance to the investigation. Among the limits that can be imposed are “date range” limitations; limita-

tions to “graphics” or “text” files; and limiting the search to certain software programs. Other courts, however, have rejected the requirement that the government set forth its method of conducting the search in the warrant itself, assuming that the warrant itself satisfies the particularity requirement and does not operate as a blank check authorizing the limitless rummaging through the contents of the computer.⁸²

Consent Searches

In *Trulock v. Freeh*,⁸³ the U.S. Court of Appeals for the 4th Circuit held that a person who shares a computer with her significant other is not capable of consenting to a search of the computer’s contents that were password-protected and created by the other person, if each user has a password that the other person does not know. The court compared this situation to the situation where a homeowner lacks consent to authorize the search of another occupant’s room if the other occupant is permitted to maintain a separate bedroom under lock and key.

In *United States v. Buckner*,⁸⁴ the police went to the defendant’s house and secured his wife’s consent to “mirror image” the computer that was seen on the table in the living room. The wife said that she used the computer occasionally to play solitaire. The agents then used forensic tools to examine the contents of the computer and determined that the defendant had used the computer to engage in various fraudulent acts. The 4th Circuit held that the consent of the wife was *not* valid to enable the police to view the password-protected files on the computer, but that she had apparent authority to grant consent, because the police were not aware that files were password-protected by the defendant and had a reasonable belief that the wife had access to the entire computer’s contents. Thus, the evidence would not be suppressed.

The 10th Circuit reached a similar result in *United States v. Andrus*,⁸⁵

where the court concluded that the defendant’s father had apparent authority to consent to a search of the son’s computer. In *Andrus*, the son had a different password from the father’s, and the father did not know the password. When the police seized the computer, however, they were unaware of the existence of the password, and the forensic investigators who examined the computer did so without having to enter a password. The fact that the father did not, in fact, have the password and therefore arguably did not have the authority to consent to the search of the son’s computer was not determinative, because he had the apparent authority to consent, and that appearance was sufficient to authorize the police to seize the computer and provide it to the forensic investigators for further analysis.⁸⁶

Conclusion

Although the federal courts have begun to grapple with complex Fourth Amendment issues that confront the police and the courts when computers are seized and searched, the Georgia courts have viewed computers as little more than “another briefcase” that can be searched if there is probable cause to believe that evidence might be found therein. This simplistic view fails to recognize the scope of the searches that are being undertaken; fails to consider the amount of information found in computers that has nothing to do with legitimate law enforcement concerns and results in the violation of the particularity requirement of the Fourth Amendment and the requirement that searches and seizures be reasonable. Magistrates who are issuing search warrants in the first instance, trial courts that view the results of these searches and seizures and the appellate courts that ultimately decide the lawfulness of these searches need to begin the process of limiting the scope of computer searches and crafting rules to protect citizens’ legitimate privacy rights. 



Edward T.M. Garland is the senior partner in the Atlanta law firm of Garland, Samuel & Loeb, P.C., a litigation boutique law firm in Atlanta, specializing in criminal defense and major plaintiff's civil litigation. Garland is past president of the Georgia Association of Criminal Defense Lawyers, a former three-term member of the board of directors of the National Association of Criminal Defense Lawyers, and presently serves as a board member of the Southern Center of Human Rights and Georgia's Innocence project. He is a recipient of the State Bar of Georgia's Tradition of Excellence award and the Anti-Defamation League's Elbert P. Tuttle Jurisprudence award. Garland is a member of the American College of Trial Lawyers, the International Academy of Trial Lawyers, the American Board of Trial Lawyers, the American Trial Lawyers Association, the State Bar of Georgia and the Atlanta Bar Association.



Donald F. Samuel is a partner at Garland, Samuel & Loeb, P.C., where he specializes in criminal trial practice at the state and federal

levels and criminal appellate practice at the state and federal levels. Samuel graduated from Oberlin College in 1975 and the University of Georgia School of Law in 1980 *cum laude*, where he was an editor of the *Georgia Journal of International and Comparative Law*. He is past-president of the Georgia Association of Criminal Defense Lawyers and a member of the National Association of Criminal Defense Lawyers. Samuel can be reached at 404-262-2225 or by visiting www.gsllaw.com.

Endnotes

1. The Supreme Court first addressed what later became known as the automobile exception in the case of *Carroll v. United States*, 267 U.S. 132 (1925).
2. 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. U.S. CONST. amend. IV.
3. See, e.g., Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39 (2002); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193 (2005); Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75 (1994).
4. *United States v. Vilar*, No. S3 05-CR-621 (KMK), 2007 U.S. Dist. LEXIS 26993, at *115 (S.D.N.Y. Apr. 5, 2007).
5. U.S. DEPARTMENT OF COMMERCE, ECONOMICS AND STATISTICS ADMINISTRATION, U.S. CENSUS BUREAU, "COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003," at 1 (Oct. 2005), available at <http://www.census.gov/prod/2005pubs/p23-208.pdf>.
6. 533 U.S. 27 (2001).
7. *Id.* at 33-34. Justice Scalia was focusing on the extent to which new technologies enabled greater intrusions on the right to privacy, rather than the extent to which new technologies, such as computers, required a different Fourth Amendment analysis.
8. Of course, thermal imaging is not the only scientific development that has required the court to apply old rules to new technologies. The use of helicopters and "fly-overs" to review what is being grown in someone's backyard is also a method of searching unknown to law enforcement in the 18th century. See *Florida v. Riley*, 488 U.S. 445 (1989); *California v. Ciraolo*, 476 U.S. 207 (1986). The application of the Fourth Amendment to telephone wiretaps was another matter that required adapting the Fourth Amendment rules to new technologies. *Katz v. United States*, 389 U.S. 347 (1967).
9. http://en.wikipedia.org/wiki/Gigabyte#Consumer_confusion. This article, written on a laptop computer, consumes approximately 135 kilobytes of hard drive space. The hard drive in total can accommodate 75 gigabytes. Thus, the hard drive has the capacity to store nearly 600,000 articles of this length.
10. <http://en.wikipedia.org/wiki/E-mail>.
11. <http://www.google.com/support/accounts/bin/answer.py?answer=54068&topic=10472>.
12. See *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 46 n.12 (D. Conn. 2002); *Barton v. State*, 286 Ga. App. 49, 49-50, 648 S.E.2d 660, 661-62 (2007).
13. *Triumph Capital Group*, 211 F.R.D. at 46 nn. 6 & 8; *People v. Gall*, 30 P.3d 145, 161 (Colo. 2001) (Martinez, J., dissenting).
14. For example, a CD-ROM's storage capacity is 650 megabytes, the equivalent of 325,000 typewritten pages. Computer networks, on the other hand, create backup data measured in terabytes (1,000,000 megabytes). MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004).
15. The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2521).
16. Pub. L. 99-508, § 201, 100 Stat. 1861 (1986) (codified as amended at 18 U.S.C. §§ 2701-2710).
17. *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).
18. This is not to suggest, however, that every aspect of a computer's contents is protected by the Fourth Amendment. In *United States v. Forrester*, 495 F.3d 1041 (9th Cir. 2007), cert. denied, 129 S. Ct. 249 (2008), the police employed a

- device that enabled them to record the “to and from” location of every e-mail that the defendant sent and received and also recorded the IP address of every website visited by the defendant’s computer and the amount of data sent and received from that computer. The U.S. Court of Appeals for the 9th Circuit held that this was not a “search” that required a warrant, analogizing this investigative technique to a pen register, which is not a search. *Id.* at 1048-49. *See* *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979). The court noted, however, that if the police actually record the URL of the search (the actual content of a website that was visited), this might constitute a search. Thus, as the court noted, discovering that the suspect visited the *New York Times* website does not amount to a search. Discovering that the suspect read a particular article while at that site might constitute a search. 495 F.3d at 1049 n.6.
19. *Mancusi v. DeForte*, 392 U.S. 364, 368 (1968).
 20. *O’Connor v. Ortega*, 480 U.S. 709 (1987). Whether the exclusionary rule applies, however, is a different matter, as the case of *Joines v. State*, 264 Ga. App. 558, 591 S.E.2d 454 (2003), illustrates. A school official went into the defendant’s classroom and searched his computer, discovering evidence that was later used in his child molestation trial. Although the school official was obviously a public official, the search was not undertaken in a law enforcement capacity and for that reason the exclusionary rule did not apply. *Id.* at 559-60, 591 S.E.2d at 456.
 21. *See, e.g., United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (CIA agent downloaded pornography to his computer, but agency rules proclaimed that all computers were open to inspection by agency personnel).
 22. 474 F.3d 1184 (9th Cir. 2007), *cert. denied*, 128 S. Ct. 879 (2008).
 23. *Id.* at 1190; *see also United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir.) (defendant employed at a university who connects his computer to a network does not thereby lose his expectation of privacy in the computer’s contents; court notes that others at the university did not audit his use of the computer or monitor its use), *cert. denied*, 128 S. Ct. 635 (2007).
 24. 509 F.3d 1338, 1341-42 (11th Cir. 2007) (per curiam).
 25. 481 F.3d 1246, 1249 (10th Cir. 2007).
 26. *United States v. Jacobsen*, 466 U.S. 109, 125 (1984); *United States v. Simpson*, 904 F.2d 607, 609-10 (11th Cir. 1990).
 27. *See United States v. Steiger*, 318 F.3d 1039, 1045-46 (11th Cir. 2003).
 28. 447 U.S. 649, 658-59 (1980) (plurality opinion).
 29. 275 F.3d 449 (5th Cir. 2001).
 30. *Id.* at 465; *see also United States v. Slanina*, 283 F.3d 670, 680 (5th Cir.) (once search of certain contents of a computer and zip disk had been justified as a government workplace search, a complete search of the contents of the entire computer by the FBI was authorized without a warrant, even though the FBI examined files that were not viewed during the prior search by the employer), *vacated on other grounds*, 537 U.S. 802 (2002).
 31. 275 F.3d at 463.
 32. 172 F.3d 1268 (10th Cir. 1999).
 33. *Id.* at 1274; *see also United States v. Walser*, 275 F.3d 981, 985 (10th Cir. 2001) (after discovering child pornography on computer being searched for other reasons, police sought and obtained new search warrant authorizing continued search for child pornography).
 34. No. 1:07-cr-211, 2008 U.S. Dist. LEXIS 84980 (M.D. Pa. Oct. 22, 2008).
 35. In *State v. Stephens*, 252 Ga. 181, 311 S.E.2d 823 (1984), the Supreme Court of Georgia adopted the formulation of probable cause in *Illinois v. Gates*, 462 U.S. 213 (1983), and held that in reviewing the sufficiency of information supporting a search warrant application, the magistrate must make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of crime will be found in a particular place. The duty of the reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed. Corroboration by an officer of details furnished by an informant is valuable. The court cautions, however, that *Gates* represents the “outer limit” of probable cause and urges attesting officers to make every effort to see that supporting affidavits reflect the maximum indicia of reliability. 252 Ga. App. at 184, 311 S.E.2d at 826.
 36. *See supra* text accompanying note 24.
 37. 277 F.3d 426, 437-38 (3d Cir. 2002).
 38. The U.S. Court of Appeals for the 6th Circuit recently reached a similar conclusion in *United States v. Hodson*, 543 F.3d 286, 292 (6th Cir. 2008).
 39. *See Birkbeck v. State*, 292 Ga. App. 424, 434, 665 S.E.2d 354, 362 (2008).
 40. 254 Ga. App. 579, 582, 563 S.E.2d 154, 160 (2002).
 41. 270 Ga. App. 388, 394, 606 S.E.2d 624, 629-30 (2004).
 42. 278 Ga. App. 332, 334, 629 S.E.2d 36, 39 (2006).
 43. 279 Ga. 618, 621, 619 S.E.2d 613, 615 (2005).
 44. 279 Ga. App. 326, 327-28, 630 S.E.2d 911, 913 (2006).
 45. One recent federal appellate court decision held that if a person is known to have subscribed to an Internet site that provided child pornography to subscribers, this is sufficient to authorize a search warrant for the seizure of the subscriber’s computer. *United States v. Gourde*, 440 F.3d 1065, 1070-71 (9th Cir. 2006) (en banc).
 46. 276 Ga. App. 769, 774 n.2, 624 S.E.2d 298, 303 n.2 (2005).
 47. 256 Ga. App. 146, 147, 567 S.E.2d 756, 758 (2002).
 48. *State v. Brantley*, 264 Ga. App. 152, 153, 589 S.E.2d 716, 718 (2003); *State v. Staley*, 249 Ga. App. 207, 207, 548 S.E.2d 26, 27 (2001); *State v. Toney*, 215 Ga. App. 64, 65, 449 S.E.2d 892, 893 (1994).
 49. *See Birkbeck v. State*, 292 Ga. App. 424, 434, 665 S.E.2d 354, 362 (2008); *Buckley v. State*, 254 Ga. App. 61, 62-63, 561 S.E.2d 188, 190 (2002) (images on computer were likely to still be on the computer long after they were disseminated, so information was not stale).
 50. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *Reaves v. State*, 284 Ga. 181, 185, 664 S.E.2d 211, 215 (2008).

51. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *Marron v. United States*, 275 U.S. 192, 195-96 (1927).
52. *Andresen v. Maryland*, 427 U.S. 463, 482 n.10 (1976); *Hunt v. State*, 180 Ga. App. 103, 104, 348 S.E.2d 467, 468 (1986).
53. 260 Ga. App. 546, 549, 580 S.E.2d 314, 317 (2003) (physical precedent only).
54. 284 Ga. at 188, 664 S.E.2d at 217.
55. 405 F.3d 852 (10th Cir. 2005).
56. *Id.* at 863; *see also* *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (seizure of law office computers in money laundering case violated Fourth Amendment, because it did not limit what the police could look for—or what crime was being investigated—with respect to the computers).
57. *United States v. Vilar*, No. S3 05-CR-621 (KMK), 2007 U.S. Dist. LEXIS 26993, at *117 (S.D.N.Y. Apr. 5, 2007).
58. *See Tennille v. State*, 279 Ga. 884, 884, 622 S.E.2d 346, 347 (2005) (defendant kept photographs of nude females in a user-created folder titled “2002 side jobs and receipts”). As one court observed, “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.” *United States v. Hill*, 322 F. Supp. 2d 1081, 1090-91 (C.D. Cal. 2004), *aff’d*, 459 F.3d 966 (9th Cir. 2006), *cert. denied*, 127 S. Ct. 1863 (2007).
59. *United States v. Khanani*, 502 F.3d 1281 (11th Cir. 2007).
60. *Id.* at 1285.
61. 275 U.S. 192 (1927).
62. *Id.* at 196.
63. 181 Ga. App. 657, 661, 353 S.E.2d 555, 559, *rev’d on other grounds*, 257 Ga. 388, 360 S.E.2d 248 (1987).
64. 192 Ga. App. 97, 98, 383 S.E.2d 648, 649-50 (1989).
65. 189 Ga. App. 483, 493, 376 S.E.2d 888, 897 (1988).
66. *See, e.g., United States v. Sissler*, No. 1:90-CR-12, 1991 U.S. Dist. LEXIS 16465, at *11-12 (W.D. Mich. Aug. 30, 1991) (authorizing seizure of 500 CDs under warrant authorizing seizure of drug records); *United States v. Musson*, 650 F. Supp. 525, 531-32 (D. Colo. 1986) (authorizing seizure of 54 diskettes pursuant to warrant that authorized seizure of “records and writings” of whatsoever nature); *People v. Gall*, 30 P.3d 145, 153-54 (Colo. 2001). In *United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008), the federal agents obtained a warrant to search for documents related to the target’s failure to pay child support and his use of false identification documents. There was no mention of computers in the warrant. When the agents arrived, they observed a computer connected to a printer and false identification documents on the printer. The agents seized the computer, but did not search it until a second search warrant was obtained, authorizing the search of the computer for additional documents relating to the creation of false identification documents. *Id.* at 888-89.
67. 220 Ga. App. 604, 469 S.E.2d 826 (1996).
68. *Id.* at 607, 469 S.E.2d at 829 (quoting *Hogan v. State*, 140 Ga. App. 716, 717-18, 231 S.E.2d 802, 804-05 (1976)) (citations omitted); *see also* *State v. Kramer*, 260 Ga. App. 546, 548-49, 580 S.E.2d 314, 317 (2003) (warrant authorized seizure of “instruments” involved in crime of child molestation; this did not authorize seizure of videotapes found at the location of the search) (physical precedent only).
69. *Horton v. California*, 496 U.S. 128 (1990); *Arizona v. Hicks*, 480 U.S. 321 (1987); *State v. Tye*, 276 Ga. 559, 562-63, 580 S.E.2d 528, 531 (2003).
70. In *United States v. Khanani*, 502 F.3d 1281 (11th Cir. 2007), the court explained how the forensic agent complied with the restrictions contained in the search warrant, which are set out in the text *supra* accompanying notes 59-60: [A] computer examiner eliminated files that were unlikely to contain material within the warrants’ scope. The culling process winnowed down the files seized from approximately three million to approximately 270,000. FBI Agent Scott Skinner testified that agents used “keyword searches,” and “if a document was opened and it wasn’t . . . covered by the warrant, then it wasn’t analyzed.” *Id.* at 1290.
71. *See, e.g., Giberson*, 527 F.3d 882 (agents had warrant authorizing them to search computer for evidence of identification fraud and discovered child pornography; after reviewing several images, a search warrant was obtained permitting thorough search for child pornography); *United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006) (“requiring such a pin-pointed computer search, restricting the search to an e-mail program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought.”).
72. *Coolidge v. New Hampshire*, 403 U.S. 443 (1971).
73. *See, e.g., United States v. Schandl*, 947 F.2d 462, 465-66 (11th Cir. 1991); *United States v. Shilling*, 826 F.2d 1365, 1369-70 (4th Cir. 1987) (per curiam); *United States v. Wuagneux*, 683 F.2d 1343, 1352-53 (11th Cir. 1982).
74. 694 F.2d 591 (9th Cir. 1982).
75. *Id.* at 595 (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)) (citations omitted).
76. *See, e.g., United States v. Grimmitt*, No. 04-40005-01-RDR, 2004 U.S. Dist. LEXIS 26988, at *14-15 (D. Kan. Aug. 10, 2004), *aff’d*, 439 F.3d 1263 (10th Cir. 2006); *United States v. Syphers*, 296 F. Supp. 2d 50, 58 (D.N.H. 2003), *aff’d*, 426 F.3d 461 (1st Cir. 2005).
77. 76 F. Supp. 2d 30, 37 (D. Me. 1999), *aff’d*, 256 F.3d 14 (1st Cir. 2001).
78. *State v. Grenning*, 174 P.3d 706 (Wash. Ct. App. 2008).
79. 18 U.S.C. § 983 (2008); 21 U.S.C. § 881; O.C.G.A. § 16-13-49 (2007).
80. *In re Search of 3817 W.W. End*, 321 F. Supp. 2d 953 (N.D. Ill. 2004).
81. 211 F.R.D. 31, 42-43 (D. Conn. 2002).
82. *United States v. Vilar*, No. S3 05-CR-621 (KMK), 2007 U.S. Dist. LEXIS 26993, at *71 (S.D.N.Y. Apr. 5, 2007).
83. 275 F.3d 391, 402 (4th Cir. 2001).
84. 473 F.3d 551, 555 (4th Cir.), *cert. denied*, 127 S. Ct. 2119 (2007).
85. 483 F.3d 711, 722 (10th Cir. 2007), *cert. denied*, 128 S. Ct. 1738 (2008).
86. *See Illinois v. Rodriguez*, 497 U.S. 177 (1990).