THE FOURTH AMENDMENT ASPECTS OF COMPUTER SEARCHES AND SEIZURES: A PERSPECTIVE AND A PRIMER

Thomas K. Clancy[*]

[*] Director, National Center for Justice and the Rule of Law, and Visiting Professor, University of Mississippi School of Law. I thank Don Mason and Marc Harrold for their comments on an earlier draft of this article. The National Center for Justice and the Rule of Law is supported by Grant No. 2000-DD-VX-0032 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this article are those of the author and do not represent the official position of the United States Department of Justice.

I. INTRODUCTION

This article is called a "primer" because it outlines the application of Fourth Amendment principles to the search and seizure of computers and the digital information that is stored in them. It does not purport to address every Fourth Amendment issue that may arise in the computer context because, for many issues, the mere fact that a computer is involved does not change the analysis. Instead, it focuses on situations that are influenced by the fact that the object to be searched and seized is a computer or the data stored on it. Like a traditional primer, this article reports how courts have addressed Fourth Amendment applicability and satisfaction issues in the computer context.

A primer is generally thought of as not espousing a point of view. This article, however, departs from that role in two important respects. First, in discussing the nature of computer and digital evidence searches and seizures, it rejects the view that those intrusions require a "special approach," that is, that unique Fourth Amendment rules are needed to regulate them; instead, this article adopts the view that computers are containers and the data they contain are mere forms of documents. This is to say that the principles applicable to document searches have equal application to electronic data searches. Second, it rejects expansion of the private search doctrine, used by some courts, which permits government agents to open data files that had not been opened during a preceding private party search and still not be a search within the meaning of the Fourth Amendment based on the theory that the "context" in which the file was found negated any reasonable expectation of privacy. Underlying both of these points of view is the perspective that a computer is a container of containers of documents, that is, each individual file is a separate container–just like each manila file in a filing cabinet is a container–that requires a separate opening to determine what is inside. This is to say that the mere fact that an item to be searched or seized is electronic evidence does not fundamentally change the Fourth Amendment analytical structure that governs.

II. THE NATURE OF COMPUTER SEARCHES: SEARCHES FOR DATA

There are two principal approaches to searches involving electronic data stored on computers. One view asserts that a computer is a form of a container and that the data in electronic storage are mere forms of documents. A second view maintains that searches for data require a "special approach," requiring unique procedures and detailed justifications. This article concludes that the first view is correct: computers are containers. As with all containers, they have the ability to hold

physical evidence, including such items as wires, microchips, and hard drives. They also contain electronic evidence, that is, a series of digitally stored 0s and 1s that, when combined with a computer program, yield such items as images, words, and spreadsheets. Accordingly, the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers.

A. Document Searches

In *Andresen v. Maryland*,[1] the Supreme Court outlined the broad parameters of a permissible records search. In upholding the search of an office for documents that sought evidence of the crime of false pretenses by an attorney involved in real estate settlement activity, the Court asserted:

> Under investigation was a complex real estate scheme whose existence could be proved only by piecing together many bits of evidence. Like a jigsaw puzzle, the whole "picture" of petitioner's false-pretense scheme . . . could be shown only by placing in the proper place the many pieces of evidence that, taken singly, would show comparatively little. The complexity of an illegal scheme may not be used as a shield to avoid detection when the State has demonstrated probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession.

Although authorizing a broad document search, the Court observed:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for

[1] 427 U.S. 463, 479-80 (1976).

[2] Id. at 480 n.10.

> papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a warrant for the "seizure" of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.[3]

Several of the themes articulated by *Andresen* have been applied by lower courts to searches of computers for data. Those considerations include the complexity of the crime, whether innocuous files can be examined, and minimization procedures to reduce the intrusion upon the individual's protected interests. Antecedent to those themes, however, is the debate whether *Andresen's* framework for document searches is applicable to computer searches.

[3] Id. at 482 n.11.

B. Views Whether Computer Data Are Documents

1. Data are Forms of Records/Container Analogy

Many courts view data in computer storage as a form of a document. Hence, a warrant that authorizes a search for "writings" or "records" permits a search of computer files.[4] This is to say that the government need not know the exact "form that records may take."[5] Indeed, this view asserts that there is "no principled distinction between records kept electronically and those in paper form"[6] and, hence, there is "no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records."[7] In both instances, consistent with *Andresen*, "innocuous documents may be scanned to ascertain their relevancy"[8] in "recognition of `the reality that few people keep documents of their criminal transactions in a folder marked `[crime] records.'"[9]

---

[4] See United States v. Hunter, 13 F. Supp. 2d 574, 581 (D. Vt. 1998) (warrant authorizing search for "records" permitted search of "computers, disks, and similar property"); United States v. Musson, 650 F. Supp. 525, 531 (D. Colo. 1986) (seizure of computer diskettes approved under a warrant authorizing the seizure of "any records or writings of whatsoever nature showing any business or financial transactions"); Frasier v. State, 794 N.E.2d 449, 454, 460 (Ind. Ct. App. 2003) (warrant that authorized search of "notes and or records" of marijuana sales permitted police to examine computer files); People v. Gall, 30 P.3d 145, 153 (Colo. 2001) (when warrant authorized seizure of "written and printed material" indicating an intent to do physical harm to a person or building pursuant to an investigation of a conspiracy to murder and use explosives against a facility, seizure of computers permissible because they were "reasonably likely to serve as `containers' for writings, or the functional equivalent of `written or printed material'"); People v. Loorie, 630 N.Y.S.2d 483, 486 (County Ct. 1995) (warrant authorizing search for "records" permitted search of computer files); cf. United States v. Triumph Capital Group, Inc., 211 F.R.D. 31 (D. Conn. 2002) (warrant authorizing search for "file records"

Courts adopting this view have often analogized computers to filing cabinets or to containers:

> [The police] may search the location authorized by the warrant, including any containers at that location that are reasonably likely to contain items described in the warrant. . . . This container rationale is equally applicable to nontraditional, technological "containers" that are reasonably likely to hold information in less tangible forms. Similarly a warrant cannot be expected to anticipate every form an item or repository of information may take, and therefore courts have affirmed the seizure of things that are similar to, or the "functional equivalent" of, items enumerated in a warrant, as well as containers in which they are reasonably likely to be found.[10]

Following this view, computers have been said to be "reasonably likely to serve as `containers' for writings, or the functional

included text, remnants, and fragments of deleted files); United States v. Harding, 273 F. Supp. 2d 411, 425 (S.D.N.Y. 2003) (because photographs may be taken by digital or film cameras and can be scanned if initially captured by film, a warrant authorizing the police to search for "photographs" allowed agents to open and inspect graphical image files on a zip disk).

[5] United States v. Gawrysiak, 972 F. Supp. 853, 861 (D.N.J. 1997) (approving of warrant to search business office for evidence of fraud), aff'd, 178 F.3d 1281 (3d Cir. 1999); accord United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988).

[6] United States v. Lievertz, 247 F. Supp. 2d 1052, 1063 (S.D. Ind. 2002).

[7] United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998).

[8] Id. at 582; accord United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999).

[9] United States v. Hunter, 13 F. Supp. 2d 574, 582 (D. Vt. 1998) (quoting United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990)); accord United States v. Maali M., 346 F. Supp. 2d 1226, 1265 (M.D. Fla. 2004).

[10] People v. Gall, 30 P.3d 145, 153 (Colo. 2001) (citations omitted); see also United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) (a computer is a form of a container); People v. Loorie, 630 N.Y.S.2d 483, 486 (County Ct. 1995) (same); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (same).

equivalent of `written or printed material.'"[11] This is despite the recognition that computer file searches present "a heightened degree" of intermingling of relevant and irrelevant material: "[t]oday computers and computer disks store most of the records and data belonging to businesses and attorneys."[12]

Accepting this view does not mean that wholesale searches of data on computers are permitted.[13] Instead, the courts look to traditional means to limit the scope of document searches, such as the nature of the criminal activity alleged[14] or the nature of

---

[11] People v. Gall, 30 P.3d 145, 153 (Colo. 2001).

[12] United States v. Hunter, 13 F. Supp. 2d 574, 581, 583 (D. Vt. 1998).

[13] The "container," however, must be properly defined. See infra notes 139-82 and accompanying text.

[14] See Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (warrants seeking subscriber information in obscenity investigation requiring that communications and computer records pertain to the listed offenses were as particular as circumstances permitted); United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (one way to make warrant particular is to specify suspected criminal conduct being investigated but warrant invalid when it authorized "the seizure of virtually every document and computer file" without indicating how items related to suspected crime); United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) ("Mere reference to `evidence' of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize."); Lafayette Academy, Inc. v. United States, 610 F.2d 1, 5-6 (5th Cir. 1979) (warrant that resulted in removal of four or five truckloads of documents and computer-related materials violated the particularity requirement when, inter alia, it did not specify type of fraud under investigation); United States v. Hunter, 13 F. Supp. 2d 574, 582-83 (D. Vt. 1998) (discussing limitations on scope of search involving money laundering scheme); In re Search Warrant for K-Sports Imports, Inc., 163 F.R.D. 594, 597-98 (C.D. Cal. 1995) (warrant for "all computer records and data," without limiting to crime under investigation, violated particularity requirement); State v. Askham, 86 P.3d 1224, 1227 (Wash. App. 2004) (warrant sufficiently particular when it names crime under investigation or when it describes in "some detail" suspected criminal activity; hence, when accused suspected of using computer to make threats and false accusations and warrant details the type of text files and web sites to be searched that could have been used to conduct that activity, it was sufficient); United States v. Longo, 70 F. Supp. 2d 225, 251 (W.D.N.Y.

the objects sought.[15] For example, searches of computers for evidence of child pornography and other sexual exploitation of children make up a shockingly large percentage of the decided cases; in response to particularity challenges in these cases, courts focus on the sufficiency of the allegations of criminal conduct[16] or the description of the objects[17] sought.

1999) (warrant that authorized search of hard drive and any data disks for "two documents, one a promissory note, entitled TGL-003, contained within the directory labeled MISC, and a purchase agreement entitled 911, contained in the directory entitled IMF" specifically described area to be searched); State v. Nuckolls, 617 So. 2d 724, 726 (Fla. App. 1993) (warrant seeking records of used car business charged with forgery, odometer tampering, and other criminal violations sufficient when it authorized seizure of "[d]ata stored on computer, including, but not limited to, magnetic media or any other electronic form, hard disks, cassettes, diskettes, photo optical devices and file server magnetic backup tapes" because it left nothing to discretion of officers executing warrant).

[15] See United States v. Thorn, 375 F.3d 679, 684-85 (8th Cir. 2004) (warrant that authorized search and seizure of electronic storage media containing images of minors engaged in sexual acts allowed examination of contents of various computer-related media); United States v. Wong, 334 F.3d 831, 837-38 (9th Cir. 2003) (warrant authorizing search of computer to "obtain data as it relates to this case" sufficiently particular when combined with warrant's list of items sought in house); State v. One Pioneer CD-ROM Changer, 891 P.2d 600, 604 (Okla. Ct. App. 1995) (seizure of computer system permissible under warrant authorizing seizure of "equipment . . . pertaining to the distribution or display of pornographic material in violation of state obscenity laws"); Schalk v. State, 823 S.W.2d 633, 644 (Tex. Crim. 1991) (in theft of trade secrets prosecution, "magnetic tapes" that contained or were reasonably believed to contain stolen data and/or files sufficiently described items to be seized).

[16] See United States v. Meek, 366 F.3d 705, 714-15 (9th Cir. 2004) (warrant sufficient to search for crime involving use of Internet when it listed numerous items relating to seduction and sexual exploitation of children: sexually explicit material or paraphernalia used to lower inhibition of children, sex toys, photography equipment, child pornography, as well as material related to past molestation such as photographs, address ledgers including names of other pedophiles, journals of sexual encounters with children, computer equipment, information on digital and magnetic storage devices, computer printouts, computer software and manuals, and documentation regarding computer use); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding validity of search of computer equipment and files because warrant limited search to evidence of crimes involving

sexual exploitation of children); United States v. Gleich, 293 F. Supp. 2d 1082, 1088 (D.N.D. 2003) (warrant authorizing search of computer for photographs, pictures, visual representations, or videos that included sexual conduct by minor, as defined by North Dakota statute, met particularity requirement), aff'd, 397 F.3d 608 (8th Cir. 2005); United States v. Hall, 142 F.3d 988, 996-97 (7th Cir. 1998) (when items listed in warrant qualified by phrases that items sought were related to child pornography, particularity requirement satisfied); United States v. Clough, 246 F. Supp. 2d 84, 87-88 (D. Me. 2003) (warrant in child pornography case authorizing search of "text documents" and "digital images" violated particularity requirement when there were "no restrictions on the search, no references to statutes, and no references to crimes or illegality"); State v. Wible, 51 P.3d 830, 837 (Wash App. 2002) (warrant particular when it limited search to images of children engaged in sexually explicit activity as defined by child pornography statute); cf. United States v. Maxwell, 45 M.J. 406, 420 (C.A.A.F. 1996) (rejecting challenge to warrant that included persons who could have unknowingly received child pornography in their email mailboxes because to narrow the field to only those who had knowingly received images would have required advance search of mailboxes to ascertain if files had been opened).

[17] See United States v. Gleich, 397 F.3d 608, 612 (8th Cir. 2005) (warrant authorizing search of home and personal computer for "photographs, pictures, visual representations or videos in any form that include sexual conduct by a minor" permitted search of all three computers in house); Thorn, 375 F.3d at 685 (warrant that authorized search and seizure of electronic storage media containing images of minors engaged in sexual acts sufficed to provide authority to examine contents of various computer-related media); United States v. Campos, 221 F.3d 1143, 1147-48 (10th Cir. 2000) (warrant particular when it authorized, inter alia, seizure of computer equipment that may be used to depict or distribute child pornography); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999), cert. denied, 527 U.S. 1011 (1999) (upholding warrant issued for "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in house of woman suspected of sending and receiving child pornography over Internet); Davis v. Gracey, 111 F.3d 1472, 1479 (10th Cir. 1997) ("equipment . . . pertaining to the distribution or display of pornographic material" was sufficiently precise to limit search to computer equipment connected with that criminal activity); United States v. Albert, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (warrant particular when it authorized search and seizure of computer, disks, software, and storage devices when there was probable cause to believe that the computer contained more than 1000 images of child pornography, given that the "search and seizure of the computer and its related storage equipment was the only practical way to obtain the

2. Rejection of the Document Search and Container Analogy: A "Special Approach"

Some authorities reject the container analogy and view searches for data on a computer much differently than paper document searches.[18] The leading case, *United States v. Carey,*[19] espouses the view that law enforcement officers must take a "special approach"[20] to the search of data contained on computers and that the "file cabinet analogy may be inadequate."[21] This position is premised on the fact that "electronic storage is likely to contain a greater quantity and variety of information than any previous storage method."[22] As one judge has argued:

---

images"); United States v. Allen, 53 M.J. 402, 407-08 (C.A.A.F. 2000) (warrant particular when it authorized search for computer files relating to nude photographs of juveniles, Internet locations of such material, or lists of such files); State v. Wible, 51 P.3d 830, 836-37 (Wash. App. 2002) (warrant for child pornography satisfies particularity requirement if it limits seizable items by specifying type of material that qualifies as child pornography); State v. Maxwell, 825 A.2d 1224, 1234 (N.J. Super. 2001) (in case involving use of telephone to call child victims of sexual assault, warrant that authorized search of computer for "computer address books" valid); State v. Patscheck, 6 P.3d 498, 500-01 (N.M. App. 2000) (in prosecution for sexual offenses against children, warrant that specified computer to be searched for "pornographic movies" valid); State v. Lehman, 736 A.2d 256, 260-61 (Me. 1999) (warrant not overbroad when it authorized seizure of all computer-related equipment in suspect's house when police knew only that the images of sexually exploited girls were taken by a digital camera and downloaded to a computer); cf. United States v. Lamb, 945 F. Supp. 441, 457-59 (N.D.N.Y. 1996) (warrant satisfied particularity requirement in child pornography case seeking subscriber information and electronic mail messages sent to and received by 78 individuals from Internet service provider when messages were instrumentalities of crime used by child pornography traffickers to locate and communicate with persons of like mind).

[18] See Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 H . J.L. & TECH. 75, 110 (1994) ("An analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage."); see also Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures:

> A computer is fundamentally different from a writing, or a container of writings, because of its capacity to hold a vast array of information in many different forms, to sort, process, and transfer information in a database, to provide a means for communication via e-mail, and to connect any given user to the internet. A computer may be comprised of a wide variety of personal information, including but not limited to word processing documents, financial records, business records, electronic mail, internet access paths, and previously deleted materials. Because of these differences, the seizure of a computer raises many issues beyond those that might pertain to mere writings. . . .
> A "writing" is simply not particular enough to warrant a reasonable person to conclude that it includes a computer because a writing and a computer are two fundamentally different things, both in degree and in kind. . . . Moreover, Fourth Amendment analysis regarding the search and seizure of computers must be approached cautiously and narrowly because of the important privacy concerns inherent in the nature of computers, and because the technology in this area is rapidly growing and changing.[23]

Some Unresolved Issues, 8 MICH. TELECOMM. TECH. L. REV. 39, 60-63, 81-82 (2002) (setting forth some of the differences between searches of "paper documents and computer-generated evidence" and maintaining that courts should impose restrictions on computer searches such as limiting the search by file types, by requiring a second warrant for intermingled files, and by imposing time frames for conducting the search).

[19] 172 F.3d 1268 (10th Cir. 1999).

[20] Id. at 1275 n.7; see also People v. Gall, 30 P.3d 145, 160 (Colo. 2001) (Martinez, J., dissenting) ("Because computers process personal information and effects, they require heightened protection under the Fourth Amendment against unreasonable searches or seizures.").

[21] Carey, 172 F.3d at 1275.

[22] Winick, supra note 18, at 105; see also In re Search of 3817 W. West End, 321 F. Supp. 2d 953, 958-59 (N.D. Ill. 2004) (asserting that searches of computers require "careful scrutiny of the particularity requirement" because, inter alia, of the "extraordinary volume of information that may be stored").

[23] People v. Gall, 30 P.3d 145, 162-65 (Colo. 2001) (Martinez, J.,

Other arguments that searches of computers are different include the assertion that computers "present the tools to refine searches in ways that cannot be done with hard copy files. When confronting a file cabinet full of papers, there may be no way to determine what to seize without doing some level of review of everything in the cabinet"; in contrast, computer technology affords a variety of methods by which the government may tailor a search to focus on documents that evidence the alleged criminal activity.[24] Those methods, it has been asserted, include limiting searches by date range, doing key word searches, limiting searches by file type, and "focusing on certain software programs."[25]

Under this "special approach," courts have imposed several unique requirements: a search warrant seeking to seize computers or computer equipment must specify that it covers such items and the warrant must "include measures to direct the subsequent search of a computer."[26] Police officers may also have to limit the search by "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[27]

---

dissenting).

[24] In re Search of 3817 W. West End, 321 F. Supp. 2d at 959.

[25] Id.

[26] People v. Gall, 30 P.3d 145, 164-65 (Colo. 2001) (Martinez, J., dissenting); see also In re Search of 3817 W. West End, 321 F. Supp. 2d at 957 (maintaining that an issuing magistrate had authority to require government to follow "search protocol that attempts to ensure that the search will not exceed constitutional bounds").

[27] United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999); see also People v. Carratu, 755 N.Y.S.2d 800, 807-09 (N.Y. Sup. Ct. 2003) (stating that police did or did not have right under warrant to open computer file folders based on name associated with that folder); In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (based on government's concession, asserting that key word search of information stored on computer would reveal information likely to be relevant to grand jury investigation); People v. Gall, 30 P.3d 145, 166 (Colo. 2001) (Martinez, J., dissenting) ("[S]earches may be limited to avoid searching files not included in the

To restrict the scope of a search of a computer that contains intermingled documents, those rejecting the premise that computer searches are just another form of a document search maintain that merely obtaining a warrant to search for specified items is insufficient.[28] Instead,

> [L]aw enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought.[29]

warrant by `observing files types and titles listed in the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory"); Winick, supra note 18, at 107 ("Once officers seize large quantities of computer memory, they have three methods of distinguishing relevant from irrelevant information. Officers can either read through portions of each file stored in the memory, conduct a key word search of the data stored on the disks, or print out a directory of the title and file type for each file on the disk.").

[28] The origin of the intermingled document doctrine can be traced to a non-computer case, which involved a large volume of material. See United States v. Tamura, 694 F.2d 591, 595-97 (9th Cir. 1982) (government can avoid violating Fourth Amendment rights by sealing documents pending issuance of search warrant detailing further search); see also United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987) (regarding file cabinets, government should adopt procedure outlined in Tamura and require subsequent search warrant). But see United States v. Hill, 322 F. Supp. 2d 1081, 1090 (C.D. Cal. 2004) (rejecting Tamura as applicable precedent because warrant permitted seizure of all storage media); David J.S. Ziff, Note, Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant, 105 COLUM. L. REV. 841, 858-61 (2005) (arguing inapplicability of Tamura to computer searches).

[29] Carey, 172 F.3d at 1275 (footnote omitted); accord United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000); Winick, supra note 18, at 105-07.

3. Discussion of the Premises of the "Special Approach"

As this section explains, I believe the "special approach" is misguided. It has no foundation in Fourth Amendment jurisprudence, even by analogy, given its essential postulate that computer technology is so fundamentally different from anything in the past. This postulate has been articulated to include several premises. First, technology not only creates a vastly different system of storage, information, and privacy concerns, it also affords ways to minimize intrusions. Because such methods are available, so the reasoning goes, they must be used. Second, computer abilities are fundamentally different than anything previously known to humankind, mandating rejection of the document and container doctrines that the Supreme Court has articulated to regulate those other types of searches. Third, because of the other premises, computer searches and seizures require the courts to create special search execution rules. Each of these premises and the underlying postulate, I believe, are flawed. Instead, the proper view is that computer and electronic data searches are properly governed by traditional Fourth Amendment rules regulating containers and document searches.

a. Should File Names or Types Limit the Scope of a Search?

An essential premise of the "special approach" is that file name labels or suffixes accurately indicate what the file contains.[30] As one commentator has asserted:

[30] See Carey, 172 F.3d at 1275 ("This is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer before discovering its contents."); People v. Carratu, 755 N.Y.S.2d 800, 807 (N.Y. Sup. Ct. 2003) ("[A] warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity."); Amy Baron-Evans, When the Government Seizes and Searches Your Client's Computer, 27 CHAMPION 18 (2003) ("Fortunately, the technical means

> Computer programs store information in a wide variety of formats. For example, most financial spreadsheets store information in a completely different format than do word processing programs. Similarly, an investigator reasonably familiar with computers should be able to distinguish database programs, electronic mail files, telephone lists and stored visual or audio files from each other. Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought.[31]

In *Carey*, the principal case espousing this "special approach," the police had a warrant allowing them to search computer files for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[32] During the course of the search, Detective Lewis came across files with sexually suggestive titles and the suffix "jpg."[33] Upon opening one of those files, Lewis observed child pornography. He subsequently downloaded numerous other "jpg" files and opened some of them, revealing additional child pornography. The "jpg" files featured sexually suggestive or obscene names, many including the word "teen" or "young."[34] Lewis testified that, until he

exist to search computers for particular information without rummaging through private information not described in a warrant. For example, in a typical white collar case, relevant files can be isolated and irrelevant ones avoided through keyword searches. In a child pornography case, the government can search for picture files without the need to look at any text file."). Cf. Commonwealth v. Hinds, 768 N.E.2d 1067, 1073 (Mass. 2002) (suggestive file names can create probable cause to search computer for child pornography).

31 See Winick, supra note 18, at 108.

32 Carey, 172 F.3d at 1270.

33 Id.

34 Id. at 1271 n.3.

opened each file, he really did not know its contents.[35] He claimed: "I wasn't conducting a search for child pornography, that happened to be what these turned out to be."[36] Although the trial court denied the motion without making any findings of fact, the appellate court reversed, imposing its own view of the evidence:

> [T]he case turns upon the fact that each of the files containing pornographic material was labeled "JPG" and most featured a sexually suggestive title. Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware—in advance of opening the remaining files—what the label meant. When he opened the subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant[.][37]

Putting aside the appellate court's disregard of its limited role in fact-finding, there are significant reasons to reject its position that a search be restricted by file names or file types. Professional investigators recognize that computer users attempt to conceal criminal evidence by storing it "in random order with deceptive file names," thus requiring a search of all the stored data to determine whether it is included in the warrant.[38] Indeed, others have asserted that "it is impossible to tell

---

[35] Id. at 1271. Lewis stated, however, that image files could contain evidence pertinent to a drug investigation such as pictures of "a hydroponic growth system and how it's set up to operate" and that drug dealers often obscure or disguise evidence of their drug activity. Id. at 1270 n.2.

[36] Id. at 1271.

[37] Id. at 1274.

[38] United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (quoting affidavit); see also United States v. Maali M., 346 F. Supp. 2d 1226, 1265 (M.D. Fla. 2004) (expert explained that he could not rely on file names to determine what was responsive to warrant); EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME (2d ed. 2004) (describing a methodical data filtering process that includes several different tools, id. at 632-43, and observing that digital evidence analysis requires examiners to employ filtering procedures to find potentially useful data and that "[l]ess methodical data reduction techniques, such as searching for specific keywords or extracting only certain file types, may not only miss important clues but

what a computer storage medium contains just by looking at it. Rather, one has to examine it electronically, using a computer that is running the appropriate operating system, hardware and software."[39] As one court has maintained:

> [Defendant] claims that the search should have been limited to certain files that are more likely to be associated with child pornography, such as those with a ".jpg" suffix (which usually identifies files containing images) or those containing the word "sex" or other key words.
>
> Defendant's proposed search methodology is unreasonable. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.
>
> Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised—whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated—forecloses defendant's proposed search

can still leave the examiners floundering in a sea of superfluous data", id. at 230); Michael G. Noblett, Mark M. Pollitt, & Lawrence A. Presley, Recovering and Examining Computer Forensic Evidence, 2 FORENSIC SCIENCE COMMUNICATIONS 7 (2000) at www.fbi.gov/hp/lab/fsc/backissue/oct2000/computer.htm (observing that there is "no such thing as generic computer science procedures" and that "evidence is likely to be significantly different every time a submission is received by the laboratory and will likely require an examination plan tailored to that particular evidence").

[39] United States v. Hill, 322 F. Supp. 2d 1081, 1088 (C.D. Cal. 2004).

methodology.[40]

Similarly, in *United States v. Gray*,[41] the court rejected the argument that an agent could not search files tagged with the "jpg" suffix, even though none of the materials covered by the warrant were believed to be pictures. The court reasoned:

> While the ".jpg" suffix generally denotes a picture file, there is no requirement that it do so, and, as a result, Agent Ehuan could not be certain that files with the ".jpg" suffix did not contain the materials for which he was authorized to search. Indeed, Agent Ehuan would have been remiss not to search files with a ".jpg" suffix simply because such files are generally pictures files, and he believed the NLM documents and hacker materials were more likely to be text files. He knew from his experience that computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories. Indeed, in the course of his search of defendant's computer files, Agent Ehuan found some text files mixed in with picture files. This serves to underscore the soundness of the conclusion that Agent Ehuan was not required to accept as accurate any file name or suffix and limit his search accordingly.
>
> Defendant further argues that Agent Ehuan, having been alerted by the names of the "Teen" and "Tiny Teen" subdirectories, was looking for child pornography when he opened the two subdirectories. Agent Ehuan testified persuasively to the contrary; he stated that, while the names of the subdirectories were suspicious to him, he opened the "Teen" and "Tiny Teen" subdirectories in the course of a systematic search of the BBS directory. In other words, Agent Ehuan did not target those particular subdirectories because of their names, and, at all times, he was searching for the materials that were the subject of the search warrant.[42]

---

[40] Id. at 1090-91.

[41] 78 F. Supp. 2d 524 (E.D. Va. 1999).

[42] Id. at 529-30; see also Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (agents could legitimately check contents of directories to see if contents corresponded with labels placed on directories; suspects "would otherwise be able to shield evidence from a search simply by `misfiling' it in directory labeled `e-mail'");

These authorities support the conclusion that *Carey's* limitations on search authority based on file names or types do not comport with the ability of computer users to hide data in innocuously labeled files. Instead, the more sound approach, consistent with *Andresen*, is that "innocuous [computer files] may be scanned to ascertain their relevancy"[43] in "recognition of `the reality that few people keep documents of their criminal transactions in a [computer file] folder marked `[crime] records.'"[44]

b. Do Technological Search Programs Make the File Cabinet Analogy Inadequate?

Another premise of authorities rejecting the file cabinet analogy is that technological searches can be employed by the government to scan data held in electronic storage to reliably sort relevant information from information for which the government does not have probable cause to search. This is a technical question and not a legal one.

There are a variety of software programs that government investigators now routinely employ when searching for electronic evidence.[45] It has been recognized that "automated

State v. Schroeder, 613 N.W.2d 911, 916 (Wis. App. 2000) (rejecting limitations on search based on file names and concluding that, during systematic search of all user-created files in executing search warrant for evidence of online harassment and disorderly conduct, opening file containing child pornography in plain view); United States v. Abbell, 963 F. Supp. 1178, 1201 (S.D. Fla. 1997) (upholding seizure of computer disks despite fact that they did not contain responsive name because seizing agents "were not required to accept labels as indicative of the disks' contents").

[43] United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998); accord United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999).

[44] Hunter, 13 F. Supp. 2d at 582 (quoting United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990)).

[45] One commonly used tool is Encase, designed by Guidance Software. See www.guidancesoftware.com.

search techniques have inherent strengths and weaknesses:"

> The usefulness [of automated keyword searches] is limited to situations where there is some precise textual identifier that can be used as the search argument. Keyword searches are context insensitive, and cannot employ the discrimination used by a human investigator. If either the data encoding or the alleged criminal activity is complex in nature, human judgment will be required to determine the evidentiary value of specific electronic documents and whether the documents fall within the scope of the warrant.
>
> The benefits of electronic search techniques are that they are fast, accurate, and within the narrow scope of their capabilities. If the officers are searching for very specific information and know one or two exact phrases or words to search for, a comprehensive electronic search can be conducted in a matter of hours. For example, if the officers were searching for a copy of specific insurance claims or accounting records, and the officers knew with certainty that these records would contain specific phrases, numbers, or names, these records could be located very quickly. Once the appropriate electronic records were located, they could be copied on a file-by-file basis, in effect allowing seizure of only the files that fall within the scope of the warrant.
>
> By contrast, if the officers conducting the search do not have specific information (names, numbers, phrases) sufficient to allow an accurate identification of all relevant documents, electronic searches are far less useful. The use of common words or phrases as keywords may still help locate relevant evidence, but such searches yield a high number of false hits. False hits are documents that contain the searched—for term, but have no evidentiary value and are beyond the scope of the warrant.
>
> The usefulness of keyword searches is further diminished by the fact that such searches are context insensitive. Computer data is encoded. Many computerized documents require specialized software to read or render their contents comprehensible. Such software provides the context required to interpret electronic data. For example, the medical records, accounting data, and medical appointment logs in our hypothetical would most probably contain

many abbreviations or coded values representing various medical procedures and associated charges. A record containing a patient's name, a numeric value of 1, a procedure code of 346 and a charge of 740000 might not seem suspicious. But if the numeric value 1 is a code that indicates that the patient is a male, and the medical procedure code of 346 identifies the operation as a hysterectomy, then the legitimacy of the $7400.00 charge is suspect. Without knowing the context of the numbers 1, 346, and 740000, the data represented cannot be evaluated for relevance.

The manner in which computer data is represented also limits the effective scope of automated search techniques. Many automated search tools are based on the detection of textual character strings embedded in documents. These techniques can only be applied to textual data, and not for pictures, diagrams, or scanned images. For example, a search for the word "submarine" would locate text that contained those characters, but it would fail to locate the scanned image of a submarine, a digital photo of the control tower, or even a scanned image or photo of the original document. The textual search would also fail to locate the desired document if it had been compressed, encrypted, or password protected. Depending on the software used for the search, it might or might not detect the word "submarine" in files that had been deleted.

Other types of searches depend on properly identifying documents by either document type or by file name. Searches by file name are unreliable because a user is free to name (or rename) files without regard to their content. Searches by file type, can be accomplished using specialized tools that identify files based on the "signature" associated with the program used to create the file. This technique can be used to identify or group files based on how data is represented. These tools can identify file format, but are not able to search content. Searches based on file type are not normally effective against files which have been encrypted, compressed, or password protected.[46]

[46] Brenner & Frederiksen, supra note 18, at 60-62; see also

This passage merely describes the current state of competition between criminal minds and government investigators. The ability to hide evidence in electronic storage constantly evolves and the government must keep pace or catch up.[47] There will always be a considerable amount of uncertainty at any given time whether any one search technique identifies with an acceptable degree of accuracy what a file contains without opening it.

A second question is a legal one: does the Fourth Amendment

SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 59 (rev. ed. 2002), at http://www.purl.access.gpo.gov/GPO/cps11361 [hereinafter CCIPS Manual] ("Even where a considerable amount is known about a system, the agents and technicians conducting a review of data often have to use a number of different techniques in order to thoroughly search a computer and its storage media. Sometimes, seemingly commonplace data or configurations cannot be copied, reviewed or analyzed by one search program or protocol, so another–or several different ones–must be tried. Keyword searches may not be possible until a careful review of a portion of the files is conducted; moreover, a careful data search may reveal other, otherwise unapparent aspects of how the system is used and data generated, accessed, transmitted and stored."); id. at 105 (discussing how it is necessary to have a "robust search strategy" that may require "a careful file-by-file review" because of, inter alia, the limitations of keyword searches, the use of code words in files, and unusual locations where the data may be stored on a computer); Orin Kerr, Digital Evidence and the New Criminal Procedure, 105 COLUM. L. REV. 279, 303 (2005) ("Existing technology simply gives us no way to know ahead of time where inside a computer a particular file or piece of information may be located."); EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME (2d ed. 2004) (describing a methodical data filtering process that includes several different tools, id. at 632-43, and observing that digital evidence analysis requires examiners to employ filtering procedures to find potentially useful data and that "[l]ess methodical data reduction techniques, such as searching for specific keywords or extracting only certain file types may not only miss important clues but can still leave the examiners floundering in a sea of superfluous data", id. at 230).

[47] See, e.g., EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 643 (2d ed. 2004) (discussing the challenges to investigators of compressed files, encrypted files, e-mails, and email attachments, which require a "combination of tools with different features").

mandate that advanced technological search engines be used? If technology is constantly evolving–and it is, then the inquiry is a moving target. This is to say that law enforcement must always stay on the cutting edge of technological change and continually invest money and resources for new training and new equipment. Such a mandate would be, in my view, a form of a least intrusive means analysis.[48] Recourse to a least intrusive analysis is a persistent minority view of the Fourth Amendment's requirements.[49] This is despite the clear mandate from the Supreme Court that it is not an element of reasonableness.[50] Indeed, there is no support for such an analysis in the language of the Amendment or in the historical regulation of search and seizure powers.[51] A least intrusive means analysis first appeared in opinions during the Warren Court era and its advocates do not rely on historical precedent to support it. Rather, they argue that it is necessary to achieve equivalence of protection between Fourth Amendment rights and other guarantees of the Bill of Rights.[52] For example, one commentator has argued that "the rationale which is commonly offered

---

[48] See Winick, supra note 18, at 108 ("[T]he government should bear a heavy burden in demonstrating that no less intrusive method is available to separate files falling within the scope of the warrant from files falling outside the scope of the warrant.").

[49] See Thomas K. Clancy, Protective Searches, Pat-Downs, or Frisks?: The Scope of the Permissible Intrusion to Ascertain if a Detained Person is Armed, 82 MARQ. L. REV. 491, 513-14 (1999) (collecting cases).

[50] See id. at 514-15 (collecting cases).

[51] See, e.g., United States v. Koyomejian, 970 F.2d 536, 546 (9th Cir.) (Kozinski, J., concurring) (finding no support for a least intrusive means requirement in either the language of the Fourth Amendment or in the "two centuries of search and seizure caselaw" interpreting it), cert. denied, 506 U.S. 1005 (1992).

[52] See Nadine Strossen, The Fourth Amendment in the Balance: Accurately Setting the Scales through the Least Intrusive Means Analysis, 63 N.Y.U. L. REV. 1173, 1242 (1988); Scott E. Sundby, A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry, 72 MINN. L. REV. 383, 436-37 (1988) (arguing that a strict scrutiny-least intrusive means standard would "bestow preferred status upon the fourth amendment as a fundamental right").

for according a special status to first amendment liberties—that they created the environment necessary for other freedoms to flourish–is equally applicable to the fourth amendment."[53] Such broad brush analysis ignores important historical differences in constitutional rights and the language of the constitution. For example, the First Amendment's Speech Clause utilizes absolute language: "Congress shall make *no* law . . . abridging the freedom of speech." Given that absolute bar, as a general matter, it is appropriate that restrictions on speech should be subjected to a requirement of necessity, that is, that the government have a compelling interest and that the restriction be narrowly tailored to effectuate that interest.[54] Such close tailoring analysis is, however, inappropriate in the Fourth Amendment context, which, instead of barring governmental intrusions, requires only that the intrusion be reasonable. This is to say that reasonableness is a more forgiving concept than a least intrusive means analysis allows. In accordance with that mandate, the means need be only reasonably related to the justification for the intrusion.[55]

The proper question for searches of data stored on a computer–as with all questions of reasonableness–is whether the means chosen by the government to execute the search are reasonably related to the purpose of the search. This inquiry, in my view, does not mandate that the police utilize any specific technology or procedures at any given time, particularly where the state of technology creates uncertainty that the search would be effective if limited to certain means. Indeed, there is no parallel in Supreme Court jurisprudence limiting intrusions

---

[53] Strossen, supra note 52, at 1241 (footnote omitted).

[54] See, e.g., Ashcroft v. American Civil Liberties Union, 542 U.S. 656 (2004) (looking to less restrictive alternatives to content-based restrictions on speech in context of Congressional attempts to protect minors from sexually explicit materials on Internet).

[55] See United States v. Gray, 78 F. Supp. 2d 524, 529 n.8 (E.D. Va. 1999) (police searching computers not obligated to conduct "the most technically advanced search possible"; instead, proper question is "whether the search, as conducted was reasonable").

to means that might permit evidence to go undetected once it is determined that the police have a warrant to search based on probable cause to believe that the place to be searched contains evidence of a crime.[56]

c. Does the Nature or Amount of Material Make Computers Different from Other Containers?

A fundamental premise of the "special approach," which asserts that computers should be treated differently than other containers of evidence, is the belief that "electronic storage is likely to contain a greater quantity and variety of information than any previous storage method."[57] The premise does not dispute that, at the most basic level, a computer is a container of a variety of items, ranging from wires to hard drives, some of which hold (contain!) digital evidence. The underlying rationale seems to be nothing more than the fact that computers store such a vast amount of information of all sorts that the particular container called a computer becomes distinct from any previous container.

The Supreme Court at one point attempted to distinguish among types of containers in ranking expectations of privacy.

---

[56] See generally Thomas K. Clancy, The Fourth Amendment's Concept of Reasonableness, 2004 UTAH L. REV. 977 (2004) [hereinafter Clancy, Concept of Reasonableness] (discussing the Supreme Court's reasonableness analysis). The Court has created a few unusual restrictions for probable-cause based intrusions due to heightened concerns for intrusions into the body and based on free-speech concerns. See id. at 1015-20. Certainly, the search of a computer is not analogous to a forced surgical procedure to remove a bullet from a person's chest. See Winston v. Lee, 470 U.S. 753, 755 (1985). Moreover, even in the area of free speech, the Court has held that a warrant based on probable cause is sufficient authority to search newspaper offices for evidence of a crime. See Zurcher v. Stanford Daily, 436 U.S. 547, 566-67 (1978). Congress, in response to Zurcher, has imposed several statutory obligations on law enforcement when there is reason to believe that First Amendment materials are involved. See, e.g., CCIPS Manual, supra note 46, at 44-47 (discussing the Privacy Protection Act).

[57] Winick, supra note 18, at 105.

Luggage had high expectations of privacy.[58] But other containers did not "deserve the full protection of the Fourth Amendment."[59] The bankruptcy of an analytical structure based on distinguishing between types of containers soon became evident, at least to a plurality of the Court: it had no basis in the language of the Amendment, which "protects people and their effects, . . . whether they are `personal' or `impersonal.'"[60] Thus, the contents of closed footlockers or suitcases and opaque containers were immune from a warrantless search because the owners "reasonably `manifested an expectation that the contents would remain free from public examination.'"[61] Moreover, the plurality believed that it would be "difficult if not impossible to perceive any objective criteria" to make any distinction between containers: "What one person may put into a suitcase, another may put into a paper bag."[62] A majority of the Court later adopted the view that there was no distinction between "worthy" and "unworthy" containers:

> the central purpose of the Fourth Amendment forecloses such a distinction. For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of

---

[58] See, e.g., United States v. Chadwick, 433 U.S. 1, 12-13 (1977) (contrasting reduced expectation of privacy surrounding an automobile with luggage and asserting: "Unlike an automobile, whose primary function is transportation, luggage is intended as a repository of personal effects. In sum, a person's expectations of privacy in personal luggage are substantially greater than in an automobile."); accord Florida v. Jimeno, 500 U.S. 248, 253-54 (1991) (Marshall, J., dissenting); see also Donald A. Dripps, The Fourth Amendment and the Fallacy of Composition: Determinacy Versus Legitimacy in a Regime of Bright-Line Rules, 74 MISS. L.J. 341, 379-87 (2004) (discussing the Court's inconsistent treatment of containers in vehicles).

[59] Arkansas v. Sanders, 442 U.S. 753, 765 n.13 (1979). Indeed, "some containers (for example a kit of burglar tools or a gun case) by their very nature [could not] support any reasonable expectation of privacy because their contents [could] be inferred from their outward appearance." Id.; accord Walter v. United States, 447 U.S. 649, 658 n.12 (1980).

[60] Robbins v. California, 453 U.S. 420, 426 (1981) (plurality opinion).

[61] Id.

[62] Id.

> privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attache case.[63]

Based on this reasoning, it seems clear that the Supreme Court would–and should–reject a special rule for electronic evidence containers. Otherwise, contrary to Supreme Court precedent and sound reasoning, filing cabinets, diaries, books, floppy drives, hard drives, paper bags, and other storage devices would all require different rules. Moreover, given the pace of technological change, which permits ever greater storage of information on ever smaller devices, such distinctions are illusory. Finally, the fact that some of the evidence in electronic storage is intermingled with other materials should not change the analysis. The same can be said of many other containers: diaries may contain evidence unrelated to the crime; filing cabinets often hold not only files of business-related paper but also miscellaneous other documents, ranging from personal tax records to family photographs.

---

[63] United States v. Ross, 456 U.S. 798, 822 (1982) (footnote omitted); accord Florida v. Jimeno, 500 U.S. 248, 253-54 (1991) (Marshall, J., dissenting); see also California v. Carney, 471 U.S. 386, 394 (1985) (rejecting distinction between worthy and unworthy motor vehicles); New Jersey v. T.L.O., 469 U.S. 325, 337-39 (1985) (student has protected privacy interest in her purse at school). But cf. California v. Greenwood, 486 U.S. 35, 40-41 (1988) (person leaving plastic trash bags for collection has no reasonable expectation of privacy as to the contents of the bags).

d. Limitations Based on Search Execution Procedures in Warrants

Based at least in part on the other premises of the "special approach," that is, computers are different than other containers, that there should be limitations on how the government may conduct a search based on file names or types, or that software search technology must be employed, some authorities require that the warrant set forth the police strategy for executing the search for electronic evidence.[64] Frankly, there is no basis in the language of the Fourth Amendment or Supreme Court caselaw[65] for such warrant requirements. As emphasized by the Supreme Court in *Dalia v. United States,*[66] the Warrant Clause contains three requirements for a search warrant to issue: an oath or affirmation; probable cause to search; and a particular description of the place to be searched.[67] Grounded in that language, the *Dalia* Court rejected the claim that a warrant must specifically authorize a covert entry in order for such a manner of execution of a warrant to be legal. The Court reasoned:

---

[64] See, e.g., In re Search of 3817 W. West End, 321 F. Supp. 2d at 958-63 (discussing the particularity requirements as applied to computer searches). The United States Department of Justice's manual on how to search computers may be partly to blame for this because it states that a computer search warrant should set forth a search strategy and the reasons for that strategy. See CCIPS Manual, supra note 46, 69-75. However, it has been noted that the CCIPS manual is not authoritative on what the Fourth Amendment requires and that, although "it may be preferable and advisable to set forth a computer search strategy in a warrant affidavit, failure to do so does not render computer search provisions unduly broad." Maali M., 346 F. Supp. 2d at 1246. Indeed, the CCIPS manual itself recognizes the inherent difficulty of mandating a predetermined search strategy: "Every computer and computer network is different, and subtle differences in hardware, software, operating systems, and systems configuration can alter the search plan dramatically." CCIPS Manual, supra note 46, at 39.

[65] In Andresen, the Court did assert that, for document searches and telephone conversation seizures, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwar-

> Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant-subject of course to the general Fourth Amendment protection "against unreasonable searches and seizures."
>
> . . . .
>
> It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth

---

ranted intrusions upon privacy." 427 U.S. at 482 n.11. Nothing in that language suggests that the manner in which a search is to be conducted was subject to pre-authorization by the judiciary. Also, Berger v. New York, 388 U.S. 41 (1967), properly understood, does not support pre-authorization procedures in a warrant beyond what the Warrant Clause requires. In striking down a statute that authorized wiretapping of telephone conversations, the Berger Court identified the statute's failures as noncompliance with the Fourth Amendment's particularity requirements of naming the crime that had been or was being committed and specifying the conversations to be searched. Id. at 55-60. The Court added that the statute had the vice of failing to place a termination date on the eavesdrop once the conversation targeted had been seized. Id. at 59-60. This latter minimization procedure stems not from Warrant Clause requirements regulating the issuance of a warrant but from the nature of reasonableness, the fundamental command of the first clause of the Amendment, which mandates that the scope of an intrusion must be reasonably related to its justification. See, e.g., New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (noting the twofold inquiry to assess the reasonableness of a search: initial justification for search and the subsequent scope of that search). Nothing in that reasonableness inquiry requires pre-authorization. Primarily in response to Berger, Congress created minimization requirements upon law enforcement officers seeking to intercept electronic communications, mandating that attempts be made to limit interceptions to those conversations that are relevant to the criminal activity that they are authorized to investigate. See 18 U.S.C. § 2518(5). Those broad prohibitions have significant application to computer-facilitated communications. See generally CCIPS Manual, supra note 46, at 164-96.

66 441 U.S. 238 (1979).

67 Id. at 255.

> Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers. Such an interpretation is unnecessary, as we have held . . . the manner in which a warrant is executed is subject to later judicial review as to its reasonableness.[68]

Indeed, in the computer context, some courts have recognized that a warrant need not specify the methods of recovery of the data or the tests to be performed because "[t]he warrant process is primarily concerned with identifying *what* may be searched or seized–not how–and *whether* there is sufficient cause for the invasion of privacy thus entailed."[69]

---

[68] Id. at 257-58 (footnote omitted).

[69] United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).

III. SELECTED FOURTH AMENDMENT APPLICABILITY ISSUES

A. Expectation of Privacy Analysis

1. In General

A person seeking to challenge the propriety of a governmental search must establish that she has a protected interest, which the Supreme Court measures by ascertaining whether she has a legitimate expectation of privacy that has been invaded by the government.[70] This expectation of privacy inquiry is two pronged: the individual must show that she has a subjective expectation of privacy; and that that subjective expectation of privacy is one that society is prepared to recognize as reasonable.[71] If either prong is missing, no protected interest is established.[72] The application of this doctrine in the computer context is not without critics;[73] nonetheless, it remains the frame-

[70] Rakas v. Illinois, 439 U.S. 128, 143 (1978). But see Thomas K. Clancy, What Does the Fourth Amendment Protect: Property, Privacy, or Security?, 33 WAKE FOREST L. REV. 307, 327-44 (1998) (discussing origins and development of the privacy expectations test and arguing that it inadequately describes the individual's interests protected by the Fourth Amendment).

[71] See, e.g., Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); California v. Ciraolo, 476 U.S. 207, 214 (1986) (stating that "Justice Harlan made it crystal clear that he was resting on the reality that one who enters a telephone booth is entitled to assume that his conversation is not being intercepted"); Smith v. Maryland, 442 U.S. 735, 740 (1979) (stating that the Harlan test "embraces two discrete questions").

[72] To support this privacy analysis, the Court has created a hierarchy of privacy interests. First, expectations of privacy that "society is `prepared to recognize as legitimate'" have, at least in theory, the greatest protection. New Jersey v. T.L.O., 469 U.S. 325, 338 (1985) (quoting Hudson v. Palmer, 468 U.S. 517, 526 (1984)). Second, diminished expectations of privacy are more easily invaded. See id. at 342 n.8 (discussing the individual suspicion requirement when privacy interests are minimal); accord Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624-25 (1989). Third, subjective expectations of privacy that society is not prepared to recognize as legitimate have no protection. See, e.g., Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978); United States v. Caymen, 404 F.3d 1196, 1200-01 (9th Cir. 2005) (no reasonable expectation of privacy in the contents of computers the person has stolen or obtained by fraud). See generally Clancy, Concept of Reasonableness, supra note 56, at 1005-13 (discussing the impact of the privacy hierarchy on the Court's reasonableness analysis).

[73] See, e.g., United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical `place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth

work to assess a person's ability to challenge the propriety of governmental searches. The following sections discuss the more common situations where the reasonable expectation of privacy analysis has been applied in the computer context.

2. The Location of the Computer—In General

Preliminarily, it is important to distinguish between the exterior of the computer (including what is visible on the monitor's screen) and its contents. As to locating a computer, the person seeking to challenge plain view[74] observations made upon observing the computer must establish an expectation of privacy in the place where the computer is stored.[75] Thus, for example, when computers are located in a common storage area accessible to hotel employees and tenants, a person does not have a reasonable expectation of privacy in the physical components of that computer.[76] In contrast, homeowners have a reasonable expectation of privacy in their belongings, including computers, in their home.[77] Equally true, however, is the principle that persons with no expectation of privacy in someone else's home or that home's contents cannot challenge the search or seizure of another's computer in that home.[78]

Amendment analysis. So long as the risk-analysis approach of Katz remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology.").

[74] See discussion infra at 262-64.

[75] See, e.g., United States v. Lyons, 992 F.2d 1029, 1031-32 (10th Cir. 1993) (no reasonable expectation of privacy in a stolen hard drive); United States v. Poulsen, 41 F.3d 1330, 1337 (9th Cir. 1994) (holding that a person who failed to pay rent had no reasonable expectation of privacy in the contents of storage locker, including computer tapes).

[76] United States v. Nettles, 175 F. Supp. 2d 1089, 1093-94 (N.D. Ill. 2001).

[77] Guest, 255 F.3d at 333; see also People v. O'Brien, 769 N.Y.S.2d 654, 656 (N.Y. App. Div. 2003) (defendant had reasonable expectation of privacy in computer in his bedroom).

[78] Guest v. Leis, 255 F.3d at 333.

3. Data on Work Computers—Governmental Employer

Government employees may have a legitimate expectation of privacy in their offices or parts of their offices.[79] However, office policies, practices, or regulations may reduce that expectation of privacy.[80] In the context of government computers used by employees, the assessment whether an employee has standing to challenge a search is made "`in the context of the employment relation,' after considering what access other employees or the public had to [the employee's] office"[81] and is done on a case-by-case basis.[82]

When the employer has no policy notifying employees that their computer use could be monitored and there is no indication that the employer directs others to routinely access the employees' computers, the employees' subjective beliefs that their computer files are private may be objectively reasonable.[83] Thus, for example, in *Leventhal v. Knapek*,[84] the court held that Leventhal had a reasonable expectation of privacy in a computer in a private office that he occupied.[85] He had exclusive use of the computer.[86] The agency did not have a general practice of routinely conducting searches of office computers nor had it placed Leventhal on notice that he should have no

---

[79] O'Connor v. Ortega, 480 U.S. 709, 716-18 (1987) (plurality opinion).

[80] Id. at 717.

[81] Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (quoting O'Connor, 480 U.S. at 717); cf. Voyles v. State, 133 S.W.3d 303, 306 (Tex. App. 2004) (teacher had no reasonable expectation of privacy in computer owned by school district that had been placed on teacher's desk in computer laboratory to teach students about computers).

[82] O'Connor, 480 U.S. at 718.

[83] United States v. Slanina, 283 F.3d 670, 676-77 (5th Cir.), remanded on other grounds, 537 U.S. 802 (2002), on appeal after remand, 359 F.3d 356 (5th Cir. 2004).

[84] 266 F.3d 64 (2d Cir. 2001).

[85] Id. at 73.

[86] Id.

expectation of privacy in the contents of his office computer.[87] Although agency technical support staff had access to all computers in the agency's offices, their maintenance of the computers was normally announced; the one unannounced visit to Leventhal's computer was only to change the name of a server.[88] Further, although agency "personnel might also need, at times, to search for a document in an unattended computer," those searches were not so frequent, widespread, or extensive as to constitute an atmosphere "`so open to fellow employees or the public that no expectation of privacy is reasonable.'"[89] The *Leventhal* court concluded that the "`[c]onstitutional protection against *unreasonable* searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer.'"[90]

On the other hand, agency policies and notices indicating that computer use is not private or is subject to inspection or audit have routinely served to defeat expectation of privacy claims.[91]

---

87 Id. at 74.

88 Id.

89 Id. at 74 (quoting O'Connor, 480 U.S. at 718 (plurality opinion)).

90 Id. (quoting O'Connor, 480 U.S. at 717-18 (plurality opinion) (emphasis in original)).

91 See United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002) (university policies and procedures, which inter alia reserved the right to randomly audit Internet use and to monitor individuals suspected of computer misuse, prevented employees from having reasonable expectation of privacy in data downloaded from the Internet and stored on university computers); United States v. Simons, 206 F.3d 392, 398-99 (4th Cir. 2000) (in light of agency's policy that permitted it to "audit, inspect, and/or monitor" employees' use of Internet, employee did not have reasonable expectation of privacy in files he transferred from the Internet or in the hard drive of computer he used); Wasson v. Sonoma Junior Coll. Dist., 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (no legitimate expectation of privacy in computer files by employee based on school district's policy that reserved right to "access all information stored on district computers"); United States v. Tanksley, 50 M.J. 609, 620 (N-M. Ct. Crim. App. 1999) (stating there is no reasonable expectation of privacy by military officer in office computer made available to him to perform official duties); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F.

For example, a public employee had no reasonable expectation of privacy in the contents of his government computer based on his written acknowledgement of the agency's policy, which prohibited personal use, expressly stated that employees had no privacy rights, and that the employee consented to inspection and audit of the computer.[92]

4. Data on Work Computers—Private Employer

A similar analysis has been applied to work computers owned by a private employer. For example, it has been held that there is no reasonable expectation of privacy in a laptop provided by an employer based on the employer's reserving the right to inspect.[93] Also, a person who has no ownership in a computer that has been assigned by a company to another user has no standing to challenge its search.[94]

2000) (no reasonable expectation of privacy in email messages and email box when government-owned email system had banner warning that user of system consented to monitoring); cf. Bohach v. Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (stating that there is no reasonable expectation of privacy in messages sent over computerized police paging system designed for official communications when all messages were recorded, and notice was given that all messages would be "logged on the network," and that certain messages were banned). But see United States v. Long, 61 M.J. 540, 545-47 (N-M. Ct. Crim. App. 2005) (despite banner warning user of possible monitoring of computer network system, the defendant had reasonable expectation in privacy of email on her computer because the system administrator discovered the evidence as a result of a request by law enforcement to locate evidence rather than as a result of routine monitoring).

92 Thorn, 375 F.3d at 683.

93 Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002). Cf. United States v. Bailey, 272 F. Supp. 2d 822, 824, 835-37 (D. Neb. 2003) (there was no reasonable expectation of privacy in work computer owned by employee's company when company required employee to assent to search every time employee accessed computer).

94 United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 54 (D. Conn. 2002). Cf. United States v. Wong, 334 F.3d 831, 839 (9th Cir. 2003) (defendant had no standing to challenge search of former employer's laptop computer).

5. Information Obtained from Third Parties

If a third party discloses information to the government that an individual has provided to that third party, the individual typically will not have an interest protected by the Fourth Amendment.[95] This is based on the Court's view that no Fourth Amendment protection exists where a wrongdoer has a misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.[96] Such a "risk," according to the Court, is "probably inherent in the conditions of human society."[97] This is consistent with the Supreme Court's view that voluntary exposure to the public eliminates Fourth Amendment protection.[98]

Thus, there is no Fourth Amendment protection[99] against the

---

[95] See, e.g., Miller v. United States, 425 U.S. 435, 443 (1976) (stating rule); United States v. Horowitz, 806 F.2d 1222, 1225-26 (4th Cir. 1986) (no reasonable expectation of privacy in computer data sold to and stored on another company's computer). There is a burgeoning amount of information held by third parties and used by law enforcement. See Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083, 1089-1101 (2002) (cataloguing this development). Numerous commentators have argued for Fourth Amendment protections extending to information held by third parties. See, e.g, Patricia I. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 GEO. WASH. L. REV. 1375, 1403-12 (2004) (arguing that there is a reasonable expectation of privacy in communications held by Internet service providers). Some, as has Professor LaFave, distinguish between the type of information given to the third party and the purposes for which the third party has been given the information and conclude that a person may retain a reasonable expectation of privacy in some circumstances. WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.6(f) at 717-19 (4th ed. 2004). There is a recent case, which is perhaps a mere aberration, that indicates that the Court may adopt a similar analysis. See Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (finding a reasonable expectation of privacy by a patient in information conveyed to medical personnel and stating: "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.").

[96] Hoffa v. United States, 385 U.S. 293, 302 (1966).

[97] Id. at 303.

[98] Katz, 389 U.S. at 351.

[99] Congress has provided some statutory protections for stored communications in the control of third parties. See, e.g., Orin S. Kerr, A User's

disclosure of subscriber information by Internet service providers.[100] This rule also applies to email recovered from a third party: once an email message has been received by another party, the sender has no reasonable expectation of privacy in its contents.[101] This risk of exposure analysis also has been uniformly applied to statements made in Internet chat rooms.[102] As

Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208 (2004). Similarly, the interception of communications in transit is largely governed by a statutory framework. See, e.g., Bellia, supra note 95, at 1383-96 (outlining the constitutional and statutory framework).

[100] See Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (noting that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) (holding that there is no reasonable expectation in subscriber information provided to Internet service provider); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (no reasonable expectation of privacy in subscriber information); United States v. Hambrick, 55 F. Supp. 2d 504, 507-09 (W.D. Va. 1999) (individual has no reasonable expectation of privacy in his name, address, social security number, credit card number, screen name, and proof of Internet connection obtained from Internet service provider); State v. Evers, 815 A.2d 432, 440-41 (N.J. 2003) (person had no standing to challenge warrant that obtained his subscriber information from Internet service provider); Hause v. Commonwealth, 83 S.W.3d 1, 10-12 (Ky. App. 2001) (no standing of subscriber to challenge warrant that obtained his name, address, and screen name from Internet service provider); United States v. Ohnesorge, 60 M.J. 946, 949-50 (N-M. Ct. Crim. App. 2005) (no reasonable expectation of privacy in subscriber information given to Internet service provider).

[101] See, e.g., United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received"); United States v. Maxwell, 45 M.J. 406, 418-19 (C.A.A.F. 1996) (no reasonable expectation of privacy in emails after being received by another person); Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. 2001) (no reasonable expectation of privacy in email messages sent to another person when that person forwarded email to police). Cf. United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (expressing doubt but declining to decide whether there was a reasonable expectation of privacy in email recovered from Internet service provider).

[102] See, e.g., Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (no expectation of privacy in material posted on bulletin board system that had disclaimer

one court has stated: "Clearly, when Defendant engaged in chat room conversations, he ran the risk of speaking with an undercover agent."[103]

6. Joint Users; Password Protected Files

The question also arises where there are joint users of a computer.[104] By creating password-protected files, the creator "affirmatively" intends to exclude the joint user and others from the files.[105] Under such circumstances, it has been reasoned, it cannot be said that the person has assumed the risk that the joint user would permit others to search the files.[106] On the other hand, for example, stating that there is "no generic expectation of privacy for shared usage on computers," one court has held that a student has no standing to suppress session logs, indicating when he used a computer, and evidence on hard drives of the university-owned computer that he used in a computer lab on campus.[107]

---

that personal communications were not private); State v. Evers, 815 A.2d 432, 439-40 (N.J. 2003) (person had no reasonable expectation of privacy in "pornographic material he unloosed into the electronic stream of commerce when he e-mailed two photographs . . . to fifty-one chat-room subscribers"); Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. 2001) (no reasonable expectation of privacy by suspect in his chat-room conversations). Cf. United States v. Meek, 366 F.3d 705, 712 n.7 (9th Cir. 2004) (chat room participant had no standing to assert privacy interest of minor's online identity).

[103] United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997) (no expectation of privacy in statements made in public chat room).

[104] Cf. United States v. Longo, 70 F. Supp. 2d 225, 256 (W.D.N.Y. 1999) (no reasonable expectation of privacy by lawyer in computer files accessed by employee in her status as legal secretary).

[105] Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

[106] Id.; see also United States v. Slanina, 283 F.3d 670, 676 (5th Cir.), remanded on other grounds, 537 U.S. 802 (2002), on appeal after remand, 359 F.3d 356 (5th Cir. 2004) (use of passwords and locking office doors to restrict employer's access to computer files is evidence of employee's subjective expectation of privacy in those files).

[107] United States v. Butler, 151 F. Supp. 2d 82, 84-85 (D. Me. 2001).

B. Private Searches and Seizures

1. In General

The Fourth Amendment is applicable only to governmental activity; hence, private searches and seizures are unregulated by it.[108] Caselaw has detailed three aspects of the private search doctrine that have significance when applied to searches of computers. They are: 1) determining who is a government agent; 2) ascertaining what constitutes replication of a private search; and 3) determining under what circumstances the "context" of a private search destroys any reasonable expectation of privacy in objects not searched by the private party. These latter two questions have been treated by the courts as analytically related and will, therefore, be treated together in this article.

[108] See, e.g., United States v. Jacobsen, 466 U.S. 109, 113 (1984) (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 government official.'").

2. Government Agents

The first difficulty is assessing when a person acts as a governmental agent. The Supreme Court has stated that the question whether a person is acting as an agent of the government "necessarily turns on the degree of the Government's participation in the private party's activities, [which] can only be resolved `in light of all of the circumstances.'"[109] Nonetheless, two considerations for determining when a private party is a government agent are often the focus of the inquiry used by lower courts: (1) whether the government knew or acquiesced in the private party's conduct; and (2) whether the private party's purpose was to assist law enforcement efforts or to further his or her own ends.[110]

Although a variety of factual instances have been litigated,[111] a

[109] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614-15 (1989) (citation omitted); see also Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (a private search may be converted into state action if the private actor is "regarded as having acted as an `instrument' or agent of the state").

[110] See, e.g., United States v. Soderstrand, 412 F.3d 1146, 1153 (10th Cir. 2005); United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003); United States v. Grimes, 244 F.3d 375, 383 (5th Cir. 2001); Jarrett v. Commonwealth, 594 S.E.2d 295, 300-01 (Va. App. 2004); see also United States v. Jarrett, 338 F.3d 339, 344-45 (4th Cir. 2003) (viewing the two parts not as a "test" but as "factors"), cert. denied, 540 U.S. 1185 (2004).

[111] See, e.g., United States v. Ellyson, 326 F.3d 522 (4th Cir. 2003) (woman living in defendant's house was not government agent when she turned over to government computer disks containing child pornography); United States v. Poulsen, 41 F.3d 1330, 1335 (9th Cir. 1994) (manager of self-storage unit not acting as government agent when he entered defendant's unit and seized, inter alia, computer tapes); United States v. Nettles, 175 F. Supp. 2d 1089, 1091-92 (N.D. Ill. 2001) (Fourth Amendment inapplicable to hotel clerk's moving of computer equipment from hotel room to common storage area when actions were not at behest of government agents); United States v. Longo, 70 F. Supp. 2d 225, 258-60 (W.D.N.Y. 1999) (legal secretary's observations of defendant's computer files were within scope of employment and not a search); State v. Lasaga, 848 A.2d 1149 (Conn. 2004) (private university employee responsible for monitoring computer use

common situation involves repairmen who report their findings to the police. Courts have consistently held that observations by private computer technicians made during their examination of a computer given to them to repair do not implicate the Fourth Amendment.[112] For example, in *United States v. Grimes*,[113] a repairman, during the course of his examination of a computer brought to the computer store for repair by Grimes' wife, opened 17 files that he believed contained child pornography.[114] After consultations with his supervisor, the technician called the police.[115] An officer then came to the store and viewed the same 17 images.[116] Without requesting the store employees to search the computer any further, the officer reported the findings to a FBI agent.[117] The repairman's supervisor, meanwhile, copied the 17 images onto a floppy disk, which he gave to the police officer; the officer copied them before faxing the images to the FBI agent, who later seized the computer after obtaining a search warrant.[118] Grimes claimed that the store's search went beyond the permission given by his wife,

not acting as government agent when he detected child pornography on school computer).

[112] See, e.g., United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998); United States v. Barth, 26 F. Supp. 2d 929, 932-35 (W.D. Tex. 1998) (Fourth Amendment inapplicable to computer repairman's examination of computer when performing repair work); People v. Phillips, 831 N.E.2d 574, 582 (Ill. 2005) (no search when police shown child pornography video on computer that had been previously viewed by computer repairman during course of repair efforts); People v. Emerson, 766 N.Y.S.2d 482, 486-87 (N.Y. Sup. Ct. 2003) (no reasonable expectation of privacy and hence, no search, when private computer repairman showed child pornography computer files to police that he had previously viewed). Cf. Rogers v. State, 113 S.W.3d 452, 457-48 (Tex. App. 2003) (finding no reasonable expectation of privacy in computer files that defendant had requested computer repairman to copy).

[113] 244 F.3d 375 (5th Cir. 2001).

[114] Grimes, 244 F.3d at 377-83.

[115] Id. at 378.

[116] Id.

[117] Id.

[118] Id.

thereby invalidating any evidence that flowed from the search.[119] The court found that the initial search, being private in nature, was not subject to Fourth Amendment applicability.[120] It reasoned that the government was not involved in the discovery of the 17 images nor were the private parties acting with the intent to assist law enforcement officials.[121] The court believed that the pre-warrant images viewed by the police officer and the FBI agent were "within the scope of the original private-party search" and "were in an area where Grimes no longer possessed a reasonable expectation of privacy."[122]

On the other hand, it has been held, when a repairman copied files based on a state trooper's request, a search within the meaning of the Amendment occurred.[123] Similarly, although a private computer repairman was acting in a private capacity when he observed the first file containing child pornography, after he related his observations to a FBI agent who asked him to copy the entire hard drive, his observations of additional files were as a government agent.[124]

Other common searches involve hackers.[125] An anonymous computer hacker, known as "Unknownuser," has generated several prosecutions for possession of child pornography stem-

---

119 Id. at 383.

120 Id.

121 Id.

122 Id.

123 United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998); see also United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (computer repairman's first viewing of child pornography not a search but his later viewing of additional files after reporting his observation to police was as government agent).

124 Barth, 26 F. Supp. 2d at 935-36. But see United States v. Peterson, 294 F. Supp. 2d 797, 800, 805 (D.S.C. 2003) (technician's observation of child pornography during repair of computer was not as agent of government, despite South Carolina statute requiring technician to report such observations and despite the fact that, after the technician's initial observations, he decided to open additional files because of that legal requirement).

125 See Monica R. Shah, Note, The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches, 105 COLUM. L. REV. 250 (2005) (discussing ability of private citizens to hack into computers of other persons).

ming from his hacking activities.[126] Unknownuser obtained access to the computers via a Trojan horse program that he attached to a picture he posted to a news group frequented by persons interested in pornography. When the picture was downloaded, the Trojan horse program was also downloaded, allowing Unknownuser to gain access to the computers.[127] After finding child pornography, Unknownuser reported those findings to law enforcement authorities.

Although Unknownuser was truly unknown to law enforcement prior to his first report, thus making the conclusion that he was not a government agent an easy one,[128] Unknownuser's subsequent efforts were preceded by an FBI agent's thanking him for his assistance in the first case and by the comment: "If you want to bring other information forward, I am available."[129] Several months later, Unknownuser produced information about another child molester.[130] Two different appellate courts subsequently rejected the claim that Unknownuser acted as a government agent based on the FBI agent's comments, reasoning that, although Unknownuser was motivated to aid law enforcement, the government did not involve itself in Unknownuser's search sufficiently to transform it into governmental action.[131] Those courts asserted that mere acquiescence was insufficient; rather, the government must either participate in or affirmatively encourage the search.[132] The mere expression of gratitude did not create an agency relationship; otherwise, as one court stated, "virtually any Government ex-

---

126 See United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003); United States v. Steiger, 318 F.3d 1039, 1042-46 (11th Cir. 2003) (no search when private hacker turned child pornography over to police that hacker found by accessing defendant's computer); Jarrett v. Commonwealth, 594 S.E.2d 295, 301-03 (Va. App. 2004) (same).

127 Jarrett, 338 F.3d at 341.

128 Steiger, 318 F.3d at 1045.

129 Jarrett, 338 F.3d at 341.

130 Id. at 342.

131 Id. at 345; Jarrett, 594 S.E.2d at 302-03.

132 Jarrett, 338 F.3d at 345.

pression of gratitude for assistance well prior to an investigation would effectively transform any subsequent private search by the party into a Government search."[133] The court noted that the government was under no affirmative obligation to discourage Unknownuser from hacking.[134]

Subsequent to Unknownuser's providing the information that formed the basis of the second and third prosecutions, an FBI agent began a series of e-mail exchanges with Unknownuser, which one appellate court has described as the "proverbial `wink and a nod.'"[135] The agent informed Unknownuser that she could not ask him to search for additional child pornographers because that would make him an agent of the government and make the information he obtained unuseable.[136] The agent further advised that Unknownuser should feel free to send any additional information he obtained and that he would not be prosecuted for hacking.[137] The Fourth Circuit viewed those exchanges as "probably" the type of government involvement that would create an agency relationship.[138]

133 Id. at 346.

134 Id. at 347.

135 Id. at 343.

136 Id.

137 Id.

138 Id. at 346.

3. Replication and "Context" Issues

A government search that merely replicates a previous private one is not a "search" within the meaning of the Fourth Amendment; rather, the Amendment applies only to the extent that the government has exceeded the scope of the private search.[139] The reasoning behind this rule, generally speaking, is that the original private party search extinguishes any reasonable expectation of privacy in the object searched.[140] The application of these principles in the computer context has sometimes led to questionable results. For example, although a computer repairman detained a computer for an extra day based on the FBI's request to do so to allow time for the FBI to obtain a search warrant, one court maintained that the detention was not attributable to the government.[141]

There are also situations where the "context" in which an object is found may lead some courts to the conclusion that there is no legitimate expectation of privacy in that object.[142] According to this view, due to the private search, there may not be any legitimate expectation of privacy remaining in aspects of the object that had not been examined during that private search. Under such circumstances, it might be concluded that the government expansion of the private intrusion does not invade any protected interest, which is to say that there is no

---

139 United States v. Jacobsen, 466 U.S. 109, 115 (1984).

140 Id. at 120-21.

141 United States v. Hall, 142 F.3d 988, 994-95 (7th Cir. 1998).

142 See, e.g., Jacobsen, 466 U.S. at 121 (although private party had not physically examined contents of package containing white powder, package could no longer support reasonable expectation of privacy); id. at 143 (Brennan, J., dissenting) (observing that the "context in which the white powder was found" under his view of the facts "could not support a reasonable expectation of privacy" and that there was a "`virtual certainty" that the DEA agent could identify it). Cf. Texas v. Brown, 460 U.S. 730, 743 (1983) (plurality opinion) (balloon had "distinctive character [that] spoke volumes as to its content–particularly to the trained eye of the officer").

search within the meaning of the Fourth Amendment. Frankly, the caselaw is less than clear whether this principle is firmly established–at least in Supreme Court jurisprudence.

The analysis of these principles begins with *Walter v. United States*.[143] In that case, 12 packages were delivered to the wrong company.[144] Employees opened the packages; inside the packages were 871 boxes of 8-millimeter film.[145] On one side of each box "were suggestive drawings, and on the other were explicit descriptions of the contents."[146] One employee attempt-

143 447 U.S. 649 (1980).

144 Id. at 651.

145 Id. at 652.

146 Id. The Supreme Court did not detail the information on the boxes. The lower court, however, stated that "[t]he top of each film box showed the name `David's Boys' and a drawing of two nude males embracing and kissing; on the back of each were the title of the individual movie and a detailed description, in explicit terms, of the bizarre homosexual acts depicted in the film." United States v. Sanders, 592 F.2d 788, 791 (5th Cir. 1979). The court detailed:

> The indictment listed five of the 25 "David's Boys" titles included in the shipment. The individual boxes containing "Look at the Birdie" said that Corbett really gets turned on when Rich comes over for a photo session. In the a—close-ups you won't believe ! The highlight of the movie happens when Corbett masturbates and—on Rich's face! This is a flick you will not forget.
>
> "The Clean Up (3 white)" boxes read that Lenny and Eric turn each other on and when you see these good looking studs you'll know why! ! ! The action gets heavy and then Les enters the picture. galore and Les cleans it up like you've never seen. Great close-ups!
>
> The "Black Rape" (1 blk. 1 wht.) boxes stated that Big Black Lance as 11—but it doesn't take long before the small slender Larry is taking it all right up the ! Good tongue action and a surprise that you won't believe. You will love the close-up action. The boxes containing "The Massage" explained that Angelo the masseur gets turned on as he gives Tommy a rubdown. Angelo's expert tongue & hands soon have Tommy's hard & excited. But he wants it the Greek way and Angie complies. Then he beautiful on Tommy's face! This is one of the best close-ups of french love you will ever see! !
>
> Finally, the "Loving Hands" boxes said that Murray and Carl are well into their love session when Ben enters the room. He will show you his loving hands as he shoves them with his arms (just short of his elbows!) right up

ed to hold one or two of the films up to the light, but was unable to observe the content of the films.[147] The recipients contacted federal agents, who viewed the films with a projector without first obtaining a warrant to search.

Although a majority of the Court concluded that the viewing of the films using a projector violated the Fourth Amendment, there was no majority opinion. In an opinion announcing the judgment of the Court, authored by Justice Stevens and joined by only one other Justice, Stevens asserted that the officers violated the Fourth Amendment because they exceeded the scope of the private search.[148] He reasoned that, because the private party had not actually viewed the films, projecting "the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search."[149] This was despite the fact that "the nature of the contents of these films was indicated by descriptive material on their individual containers."[150] Stevens maintained:

> [T]he labels on the film boxes gave [the federal agents] probable cause to believe that the films were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the labels were not sufficient to support a conviction and were not mentioned in the indictment. Further investigation–that is to say, a search of the contents of the films–was necessary in order to obtain

---

> his friends' ah ! ! While they masturbate! It is a true masterpiece for the avid connoisseur! ! (Certain particularly salacious words have been deleted by the writer of this opinion, as indicated.)

Id. at 793 n.5.

147 Walter, 447 U.S. at 651.

148 Id. at 657. Justice White, in a concurring opinion joined by Justice Brennan, believed the Fourth Amendment was violated because the agents had not obtained a warrant, regardless of whether the scope of the private search was exceeded. Id. at 660-62. Justice Marshall concurred in the judgment but did not write an opinion. Id. at 660.

149 Id. at 657.

150 Id. at 654.

the evidence which was to be used at trial.[151]

Stevens rejected the government's claim "that because the packages had been opened by a private party, thereby exposing the descriptive labels on the boxes, petitioners no longer had any reasonable expectation of privacy in the films."[152] He believed that "[t]he private search merely frustrated that expectation in part. It did not simply strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection."[153] In a curious footnote, however, Justice Stevens opined that "if a gun case is delivered to a carrier, there could then be no expectation that the contents would remain private, but if the gun case were enclosed in a locked suitcase, the shipper would surely expect that the privacy of its contents would be respected."[154] The gun case example indicates that Stevens would hold that, in at least some circumstances where the objects inside the container can be ascertained by information outside the container, there is no reasonable expectation of privacy inside the container. Stevens, however, made no attempt to reconcile the gun case example with the facts or his analysis in *Walter*.[155]

The four dissenters in *Walter* believed that no legitimate expectation of privacy remained in the contents of the packages by the time the FBI received them because the private search had "clearly revealed the nature of their contents."[156] Accordingly, the viewing of the films by the FBI did not change the nature of the search and was not an additional search.[157] The

151 Id.

152 Id. at 658.

153 Id. at 659.

154 Id. at 658 n.12 (citation omitted).

155 The gun case has been repeated several times to illustrate the situation where the "very nature" of the container "cannot support any reasonable expectation of privacy because [the] contents can be inferred from [the] outward appearance." Arkansas v. Sanders, 442 U.S. 753, 764-65 n.13 (1979); see also Jacobsen, 466 U.S. at 121 (repeating the gun case example).

156 Walter, 447 U.S. at 663 (Blackmun, J. dissenting).

157 Id. at 663-64 (citation omitted).

dissent also addressed Stevens' gun case hypothetical: "The films in question were in a state no different from Mr. Justice Stevens' hypothetical gun case when they reached the FBI. Their contents were obvious from `the condition of the package,' . . . and those contents had been exposed as a result of a purely private search that did not implicate the Fourth Amendment."[158]

A perplexing question involving searches of computers, which has led to contradictory results, involves whether the scope of the private party search has been exceeded when law enforcement agents open additional files that had not been opened in the preceding private search. This question is similar to the one that so divided the Court in *Walter*. Some courts have held that the determinative inquiry is not the mere opening of additional files.[159] On the other hand, in *United States v. Barth*,[160] the court rejected the government's contention that, once a private computer repairman opened a file containing an image of child pornography, Barth lost his reasonable expectation of privacy in the other files on the computer's hard drive, reasoning that the copying of the entire contents of the hard drive and the review of those files by law enforcement "far exceeded" the private viewings.[161]

In this context, *United States v. Runyan*[162] is particularly instructive. In that case, the defendant's estranged wife and

---

158 Id. at 665.

159 See, e.g., People v. Emerson, 766 N.Y.S.2d 482, 488 (N.Y. Sup. Ct. 2003) ("when an earlier, private search opens child pornography images on a hard drive in identified computer file folders which the private searcher found replete with file titles plainly suggesting images of like kind, defendant retains no reasonable expectation of privacy with respect to additional such image files in the same two computer file folders"). Cf. State v. Lasaga, 848 A.2d 1149 (Conn. 2004) (declining to determine if police exceeded scope of private search when they opened additional files because, even if those files were disregarded, warrant based on probable cause to search).

160 26 F. Supp. 2d 929 (W.D. Tex. 1998).

161 Id. at 935-37.

162 275 F.3d 449, 453-57 (5th Cir. 2001).

her companions removed from Runyan's ranch various data storage devices and turned them over to the police. The private parties had examined only a randomly selected assortment of the floppy disks and CDs and they did not view any of the ZIP disks. The government agents examined every one of the floppy disks, ZIP disks, and CDs.[163]

The *Runyan* court noted that there are two different analytical approaches to the problem posed by the facts. One line of authority holds that "a police search exceeds the scope of a prior private search when the police open a container that the private searchers did not open."[164] A second line, according to the court, is reflected in *United States v. Bowman*:[165]

> In Bowman, an airline employee opened an unclaimed suitcase and found five identical bundles wrapped in towels and clothing The employee opened one bundle and found a white powdery substance wrapped in plastic and duct tape. He contacted a federal narcotics agent, who identified the exposed bundle as a kilo brick of cocaine and then opened the other bundles, which also contained kilo bricks of cocaine. The court held that the agent did not act improperly in failing to secure a warrant to unwrap the remaining identical bundles, reasoning that the presence of the cocaine in the exposed bundle "`spoke volumes as to [the] contents [of the remaining bundles]—particularly to the trained eye of the officer.'"[166]

Runyan attempted to harmonize the two approaches:

> [C]onfirmation of prior knowledge does not constitute exceeding the scope of a private search. In the context of a search involving a number of closed containers, this suggests that opening a container that was not opened by private searchers would not necessarily be problematic if the police knew with substantial certainty, based on the statements of the private searchers, their replication of the

163 Id. at 461-62.

164 Id. at 462.

165 907 F.2d 63 (8th Cir. 1990).

166 275 F.3d at 462-63 (quoting Bowman, 907 F.2d at 65).

> private search, and their expertise, what they would find inside. Such an "expansion" of the private search provides the police with no additional knowledge that they did not already obtain from the underlying private search and frustrates no expectation of privacy that has not already been frustrated.[167]

Applying this guideline to the facts of the case before it, the *Runyan* court believed that the police's pre-warrant examination of the disks not opened by the private parties clearly exceeded the scope of the private search:

> The police could not have concluded with substantial certainty that all of the disks contained child pornography based on knowledge obtained from the private searchers, information in plain view, or their own expertise. There was nothing on the outside of any disk indicating its contents. . . . Indeed, [the private searchers] could not have known the contents of any of the ZIP disks, as [they] did not use hardware capable of reading these disks in their private search. The mere fact that the disks that [the private searchers] did not examine were found in the same location in Runyan's residence as the disks they did examine is insufficient to establish with substantial certainty that all of the storage media in question contained child pornography.[168]

Turning to the question whether the police exceeded the scope of the private search because they opened more files on each of the disks than examined by the private searchers, while the record was not entirely clear whether the police actually did so, the court concluded that it would not have been constitutionally problematic for the police to have examined more files than did the private searchers.[169] The court reasoned:

> [T]he police do not exceed the scope of a prior private search when they examine the same materials that were

---

167 Id. at 463 (citations omitted).

168 Id. at 464.

169 Id.

> examined by the private searchers, but they examine these materials more thoroughly than did the private parties. In the context of a closed container search, this means that the police do not exceed the private search when they examine more items within a closed container than did the private searchers. . . . [A]n individual's expectation of privacy in the contents of a container has already been compromised if that container was opened and examined by private searchers[.] Thus, the police do not engage in a new "search" for Fourth Amendment purposes each time they examine a particular item found within the container.[170]

Runyan's approach is open to criticism. One can take issue with the court's view of what the appropriate container is: should it be the computer; an individual disk; the directory; the file folders; or each individual file? *Runyan* seems to point to each disk as the container and, hence, once that disk is opened by the private party, anything within it that the police examine is within the scope of the private search. The basis for the court's analysis is far from clear: why is not the entire hard drive of a computer the container and, once that container is opened by a private party, all data would be within that search's scope; on the other hand, why is not each data file a container, given that each must be separately "opened" to view the file's contents?

One could draw an analogy to a filing cabinet in the physical world. Each filing cabinet may have one or more drawers and have a number of file folders in each drawer. For example, there may be a group of folders entitled tax records, each for a different year. If a private party opens "tax records 2004," under *Runyan* it would seem that the tax records for other years may be opened by government agents and not be labeled a search. This approach is undoubtedly incorrect. Nothing in previous Supreme Court caselaw supports viewing the entire filing cabinet as a container that permits wholesale searches of all the files therein once a private party opens one of them.[171] If

---

170 Id. at 464-65.

171 Cf. United States v. Knoll, 16 F.3d 1313, 1321 (2d Cir. 1994)

computers are containers that hold various forms of information,[172] then there is no principled distinction between them and a metal filing cabinet when applying the private search doctrine. This is to say that the rules regulating containers in the bricks and mortar world have equal applicability to computer searches. Accordingly, a computer should be viewed as a physical container with a series of electronic "containers"–that is, directories, folders, and files that must be each separately opened. Each separate opening is the examination of a new container.

Also, to the extent that *Runyan* grounds its analysis on the belief that the mere opening of additional files within a container already partially examined by a private party does not exceed the scope of that private search because the "container" no longer supports a reasonable expectation of privacy, there is little Supreme Court jurisprudence to support that view. Only in *United States v. Jacobsen*[173] has the Supreme Court held that the government activities were not a search, even though the government activity exceeded the private search. In that case, a Federal Express employee opened a damaged package and found several transparent plastic bags of white powder inside a closed tube wrapped in crumpled newspaper. The employee put the bags back in the tube, put the tube and the newspapers back in the box, and then summoned federal agents. The agent who responded opened the box, unpacked the bags of white powder, and performed a chemical field test confirming that the white powder was cocaine.[174] Putting aside the chemical testing, which raised a separate issue,[175] the Court found that the agent's actions did not implicate the Fourth Amendment because the agent's actions in removing the plastic bags from the tube and visually inspecting their contents "enabled the

(viewing each closed opaque file folder as closed container).

172 See discussion supra at 197-220.

173 466 U.S. 109 (1984).

174 Id. at 111-12.

175 See id. at 123.

agent to learn nothing that had not previously been learned during the private search."[176] Although the private party had not physically examined the contents of the package containing the white powder, the Court asserted that the package could no longer support a reasonable expectation of privacy.[177] The Court concluded that the visual inspection was not a "search" because it did not infringe "any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct."[178] By merely replicating the private party's actions, the agents in *Jacobsen* observed white powder in a *transparent* container. They learned nothing more from its mere removal, which is to say that no reasonable expectation of privacy was invaded by their actions. This is in marked contrast to *Runyan*, where the container did not disclose its contents prior to its opening and, as a result, the police did learn something new when the files were opened.

This leaves the difficult decision of *Walter* as possible support for the *Runyan* viewpoint. Clearly, the Court has changed since *Walter* and a majority might be willing to adopt the *Walter* dissent's view that context does sometimes destroy an expectation of privacy, even if the private party had not opened the same container as the governmental authorities. On the other hand, if Justice Stevens' view in *Walter* is adopted by a majority of the Court, it is difficult to envision a situation where the police could open a computer file unopened by the private party without exceeding the scope of that private search. The boxes in *Walter* certainly gave the police a high degree of confidence that they contained pornography.[179] So too would a private party search that opened some files with suggestive names that were in a folder with a series of other files.

---

176 Id. at 120.

177 Id. at 121; see also id. at 142 (Brennan, J., dissenting) (observing that the "context in which the white powder was found" under his view of the facts "could not support a reasonable expectation of privacy" and that there was a "`virtual certainty'" that the DEA agent could identify it).

178 Id. at 126.

179 See supra notes 143-47 and accompanying text.

Thus, for example, if a private party opened files labeled "preteen.female9.rape", "preteen.female10.rape", and preteen.female11.rape," and discovered images of young girls being raped, if there were additional files in the same folder labeled "preteen.female12.rape" and "preteen.female13.rape", I would think that most courts would easily conclude that the police had probable cause to believe that the "12" and "13" files also depicted images of child pornography. But under Stevens' view in *Walter*, mere probable cause–or even "substantial certainty"–does not eliminate Fourth Amendment applicability.

This, it seems to me, is the proper approach. Probable cause is the usual level of suspicion that justifies a search. Moving to a higher level of suspicion, such as "substantial certainty," does not somehow make the Amendment inapplicable. The opposing position would hold that, the more certain the police are, the less applicable the Amendment becomes. That position confuses Fourth Amendment applicability with Fourth Amendment satisfaction.[180] Underlying the private search doctrine is the view that the private party has already discovered what is in the container; in the Court's words, the private party has eliminated the owner's reasonable expectation of privacy in the contents of the container. Yet, when the governmental agent opens an opaque container that a private party has not opened, the agent does learn something that the private party did not learn. That is, the container does *in fact* hold a gun, drugs, or child pornography, or that the container *in fact* holds something else – despite all indications of what it held prior to its opening.

Finally, there remains the oft-stated gun case hypothetical. This is much different than the situation in *Jacobsen*, where the contents of the *transparent* package could be viewed without opening the container. The gun case hypothetical envisions a container that is specifically designed to hold a gun and

[180] Cf. Soldal v Cook County, 506 U.S. 56, 69 (1992) ("[T]he reason why an officer might enter a house or effectuate a seizure is wholly irrelevant to the threshold question whether the Amendment applies. What matters is the intrusion on the people's security from governmental interference.").

whose exterior shape informs the observer that it is a gun case.[181] However, putting aside transparent gun cases, the shape of the case does not disclose what is inside; instead, it informs the observer that it is a case designed to hold guns and perhaps–or even probably–that there is a gun inside. The police will not *know* what is inside until they open the case or use other means, such as an x-ray, to examine its contents. The dissent in *Walter* was correct in asserting that the viewing of the films in that case and the gun case hypothetical presented identical scenarios. Yet, in both situations, although the police may have had a high degree of confidence in what they would find when they opened the container, that confidence should not eliminate the applicability of the Amendment; instead, that confidence goes to the reasonableness of the police's actions.[182]

[181] Gun cases come in many forms: some are mere rectangular hard-sided boxes; others are soft-sided and in the shape of a rifle or a shotgun. Rectangular boxes disclose nothing of the contents of the box. Instead, the gun case hypothetical refers to those containers that have the unique shape that says to the viewer that is a container designed to hold a gun.

[182] Cf. Clancy, Concept of Reasonableness, supra note 57, at 1000-03 (discussing the Court's inconsistent treatment of containers as to application of warrant preference rule and arguing that there should be no warrant requirement for "effects").

IV. SELECTED SATISFACTION ISSUES

A. Probable Cause

The concept of probable cause–a familiar but fluid standard for a court to apply[183]–has created some unique difficulties in the computer context.[184] This article focuses on two nexus questions that have troubled the courts confronting them: 1) as to subscribers of child pornography sites, the amount of information needed in order to conclude that there is probable cause to search the subscriber's computer; and 2) as to distributors or recipients of child pornography, establishing the location of the computer used to distribute or receive the materials.[185] Both of these problems illuminate the difficulty of piercing through the layers of anonymity that the Internet affords.

---

[183] See generally Ronald J. Bacigal, Making the Right Gamble: The Odds on Probable Cause, 74 MISS. L.J. 279 (2004) (comprehensively examining the concept of probable cause). "In dealing with probable cause . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Brinegar v. United States, 338 U.S. 160, 175 (1949). The totality of the circumstances is taken into account to determine whether there is a "fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). In reviewing a warrant that had been issued by a magistrate, a court does not make a de novo determination of probable cause; instead, the proper question is whether a substantial basis exits for the magistrate's finding of probable cause. Id. at 236.

[184] As with other situations, probable cause determinations in the computer context are fact-bound. See, e.g., United States v. Hill, 322 F. Supp. 2d 1081, 1084-87 (C.D. Cal. 2004) (discussing when allegations of child pornography are sufficient); United States v. Scott, 83 F. Supp. 2d 187, 197 (D. Mass. 2000) (it is "reasonable to suppose that someone allegedly engaged in bank fraud and producing false securities on his computer would have records of the bank fraud and false securities on that computer"); Burnett v. State, 848 So. 2d 1170, 1173-75 (Fla.

There is a split of authority over the strength of the inference that can be drawn as to whether a person has child pornography on his computer based on membership in a child pornography web site. A few courts have indicated that mere membership in a child pornography site is sufficient.[186] Others

App. 2003) (no probable cause to support warrant to search computer for evidence of child pornography based on initial complaint that suspect had made lewd videotape of two children); State v. Staley, 548 S.E.2d 26, 28-29 (Ga. App. 2001) (although police had probable cause to believe that Staley had molested a specific child, that he had worked as a computer analyst, that he had been previously convicted of molesting a child and taking pictures of that child, and that the affiant detailed that pedophiles stored information relating to having sex with children, there was no nexus between either the crime of molesting that specific child or the propensities of child sex offenders and search of computer in Staley's apartment); State v. Lum, 998 P.2d 137, 139-42 (Kan. Ct. App. 2000) (affidavit in support of search warrant for computer insufficient because affiant failed to detail basis of knowledge); Williford v. State, 127 S.W.3d 309, 313 (Tex. App. 2004) (probable cause to seize computer based on repairman's viewing of thumbnail picture of two naked boys on bed); Burke v. State, 27 S.W.3d 651, 653-56 (Tex. App. 2000) (fact-bound question whether there was probable cause to issue warrant in child pornography case).

A persistent question concerns the circumstances under which file names establish probable cause to search or seize a computer; a finding of probable cause generally turns on the explicit nature of the names and the surrounding circumstances. See, e.g., State v. Wible, 51 P.3d 830, 833-34 (Wash. App. 2002) (file names "8 year old Rape" and "8 year old Smile" gave context and meaning to repairman's tip that computer contained child pornography).

[185] The number of child pornographers utilizing the Internet is truly shocking and law enforcement efforts to catch those criminals comprise a large portion of the published decisions dealing with computer-related search and seizures. See, e.g., Amy E. Wells, Comment, Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet, 53 OKLA. L. REV. 99, 100-01 (2000) (cataloguing reasons for explosion of Internet child pornography). The Internet has increasingly become a preferred vehicle to trade and distribute child pornography; websites are designed for that purpose and chat rooms are used to establish contacts, followed by transmission or trading of images. See, e.g., United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000). Because of a computer's ability to store images in digital form, it is an ideal repository for child pornography. Id. at 635-36.

[186] See United States v. Martin, 426 F.3d 3 (2d Cir. 2005) (finding

have rejected that view.[187] Those latter courts caution:

> If the Government is correct in its position that membership in the Candyman group [an Internet child pornography site] alone was sufficient to support a finding of probable cause, then probable cause existed to intrude into the homes of some 3,400 (or even 6,000) individuals merely because their e-mail addresses were entered into the Candyman website. Without any indication that any of these individuals downloaded or uploaded or transmitted or received any images of child pornography, without any evidence that these individuals did anything more than simply subscribe, the Government argues that it had the right to enter their

probable cause based on subscription to website that's essential purpose was to trade child pornography); United States v. Wagers, 339 F. Supp. 2d 934 (E.D. Ky. 2004) (probable cause existed that suspect's home computer contained child pornography based on membership in child pornography website); U.S. v. Bailey, 272 F. Supp. 2d 822, 824-25 (D. Neb. 2003) (holding that "knowingly becoming a computer subscriber to a specialized Internet site that frequently, obviously, unquestionably and sometimes automatically distributes electronic images of child pornography to other computer subscribers alone establishes probable cause for a search of the target subscriber's computer even though it is conceivable that the person subscribing to the child pornography site did so for innocent purposes and even though there is no direct evidence that the target subscriber actually received child pornography on his or her computer").

[187] See United States v. Gourde, 382 F.3d 1003, 1006, 1011-13 (9th Cir. 2004) (holding that merely because suspect was member of Internet child pornography site for at least two months was insufficient to establish that he had downloaded child pornography onto his home computer, despite a discussion of traits of child pornography collectors by affiant that included explanations that they "rarely if ever" dispose of pornography and that they use the Internet to share information and trade child pornography), reh'g granted, 416 F.3d 961 (9th Cir. 2005); United States v. Perez, 247 F. Supp. 2d 459, 483-84 (S.D.N.Y. 2003) (subscription to known child pornography website created a "chance, but not a fair probability, that child pornography would be found"). But see United States v. Corcas, 419 F.3d 151 (2d Cir. 2005) (although affirming denial of motion to suppress, the panel did so based on prior precedent finding probable cause stemming from membership in child pornography website, while criticizing that precedent as unsound).

> homes to conduct a search and seize their computers, computer files and equipment, scanners, and digital cameras. This cannot be what the Fourth Amendment contemplated.
> * * * * Here, the intrusion is potentially enormous: thousands of individuals would be subject to search, their homes invaded and their property seized, in one fell swoop, even though their only activity consisted of entering an e-mail address into a website from a computer located in the confines of their own homes. In fact, here the FBI sent out 700 or more draft search warrants across the country. . . . In light of the potential impact, care must be taken.[188]

To establish probable cause to search, courts often rely on additional information–beyond membership in a child pornography site–that substantiates the person's sexual interest in children or in child pornography.[189] That additional information has included such factors as evidence of actual downloading[190]–as opposed to mere viewing,[191] automatic transmis-

---

[188] Perez, 247 F. Supp. 2d at 483-84.

[189] See, e.g., United States v. Froman, 355 F.3d 882, 884-91 (5th Cir. 2004) (upholding search warrant for member of group whose "singular goal . . . was to collect and distribute child pornography and sexually explicit images of children," when members could choose to automatically receive emails with attached images and Froman's interest in child pornography was shown by his chosen screen names, "Littlebuttsue" and "Littletitgirly"); State v. Schaefer, 668 N.W.2d 760, 770 (Wis. App. 2003) (because computer files are common way of storing photographs, reasonable inference that computer contained child pornography when suspect actively cultivated friendship of teenage boys by inviting them to use his home computer, used his computer to communicate with others interested in stories about adults sexually assaulting children, and visited Internet sites where child pornography was available for downloading).

[190] Gourde, 382 F.3d at 1006, 1012 ("Requiring the government to buttress its affidavit with personalized information linking a website member to actual child pornography strikes a reasonable balance between safeguarding the important Fourth Amendment principles embodied in the probable cause requirement and ensuring that the government can effectively prosecute possessors and distributors of child pornography."); United States v. Perez, 247 F. Supp. 2d 459, 483-84 (S.D.N.Y. 2003) (rejecting finding of probable cause and noting, inter alia, that,

sions as part of the site's services,[192] use of suggestive screen names,[193] expert information on the retention habits of child pornography collectors[194] (which often serves to dispel allega-

unlike other cases where there was evidence of downloading, the affidavit contained "nothing concrete to suggest that Perez had transmitted or received images of child pornography").

[191] See Perez, 247 F. Supp. 2d at 483-84 n.12 ("The statute does not criminalize `viewing' the images, and there remains the issue of whether images viewed on the internet and automatically stored in a browser's temporary file cache are knowingly `possessed' or `received.'"); see also United States v. Zimmerman, 277 F.3d 426, 435 (3d Cir. 2002) (without evidence that pornography was specifically downloaded and saved to defendant's computer, offending images "may well have been located in cyberspace, not in [the defendant's] home"); United States v. Tucker, 305 F.3d 1193, 1198 (10th Cir. 2002) (upholding conviction for possession of files automatically stored in browser cache because defendant's habit of manually deleting images from cache files established his control over them).

[192] See Perez, 247 F. Supp. 2d at 485 (asserting that "the agents either had or could have had, before they requested the warrant, all the Yahoo logs, which provided extensive information—whether a subscriber was offered e-mail delivery options; whether he elected a delivery option; whether he uploaded or posted any images; when he subscribed; and whether he unsubscribed"). Cf. United States v. Froman, 355 F.3d 882, 884-91 (5th Cir. 2004) (upholding search warrant for member of group whose "singular goal . . . was to collect and distribute child pornography and sexually explicit images of children," when members could choose to automatically receive emails with attached images and Froman's interest in child pornography was shown by his chosen screen names, "Littlebuttsue" and "Littletitgirly").

[193] Gourde, 382 F.3d at 1006, 1011-13 (stating that screen name indicating sexual interest in children would add to probable cause determination).

[194] See, e.g., United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997) (probable cause found in child pornography case when affiant, based on her training and experience, explained that collectors and distributors of child pornography typically store it in their homes); United States v. Wagers, 339 F. Supp. 2d 934, 941 (E.D. Ky. 2004) ("In child pornography cases, courts have repeatedly recognized that collectors of child pornography tend to retain their materials."); United States v. Cox, 190 F. Supp. 2d 330, 333 (N.D.N.Y. 2002) (same); State v. Evers, 815 A.2d 432, 446, 448 (N.J. 2003) (probable cause to believe that pornographic images of children would be retained on computer due to retention habits of child pornographers); State v. Lindgren, 687 N.W.2d 60, 64-65 (Wis.

tions of staleness[195] and identifies the house as the place where

App. 2004) (when defendant took nude photographs of a 14 year old female employee at work, touched her vaginal area, and had allegedly taken pictures of other female employees, and affiant detailed habits and characteristics of child molesters, including, inter alia, that they collect sexually explicit materials, rarely dispose of them, and record diaries of their encounters on, inter alia, their computers, probable cause existed to search home computer for photographic evidence of underage children of sexually explicit nature). Cf. United States v. Gourde, 382 F.3d 1003, 1006, 1011-13 (9th Cir. 2004) (merely because suspect was member of Internet child pornography site for at least two months insufficient to establish he had downloaded child pornography onto home computer, despite discussion of traits of child pornography collectors by affiant that included explanations that they "rarely if ever" dispose of pornography and that they use the Internet to share information and trade child pornography), reh'g granted, 416 F.3d 961 (9th Cir. 2005).

The reason why child pornography collectors retain their collections for long periods of time was explained by the court in United States v. Lamb, 945 F. Supp. 441, 460 (N.D.N.Y. 1996):

> Since the [child pornographic] materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.

But see United States v. Greathouse, 297 F. Supp. 2d 1264, 1272 (D. Or. 2003) (even though agent indicated in affidavit that child pornography collectors routinely maintain their materials for long periods of time, rejecting that assertion as sufficient because it appeared "to be based upon a generalized sense developed through informal conversations with other agents").

[195] See, e.g., United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000) (probable cause that computer in suspect's home contained child pornography was not stale, even though information was six months old, due to affiant's explanation that collectors and distributors rarely if ever dispose of it and store it in secure place); United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997) (probable cause not stale in child pornography case when based on information 10 months old because affiant, based on her training and experience, explained that collectors and distributors of child pornography "rarely if ever" dispose of such material); United States v. Wagers, 339 F. Supp. 2d 934, 941 (E.D. Ky. 2004) (collecting cases);

the materials were viewed), and prior convictions involving sex offenses involving children or child pornography.[196]

Another significant question is ascertaining the location of the computer that has distributed or received the child pornography. This difficulty arises because many individuals use computers in a variety of locations, including in an office and at home.[197] Persons accessing the Internet are assigned an

Hause v. Commonwealth, 83 S.W.3d 1, 13-14 (Ky. App. 2002) (based on "hoarding" characteristics of child pornography collectors, information that was 178 days old not stale); United States v. Lamb, 945 F. Supp. 441, 460-61 (N.D.N.Y. 1996) (based, inter alia, on proposition that pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant period of time, five month delay from last transmission of child pornography to issuance of warrant did not render probable cause stale); State v. Schaefer, 668 N.W.2d 760, 767 (Wis. App. 2003) (information that suspect possessed child pornography in 1998, some of which went back to 1990, not stale based on protracted and continuous nature of habits of preferential child offenders, who rarely dispose of sexually explicit materials). But cf. United States v. Zimmerman, 277 F.3d 426, 433-34 (3d Cir. 2002) (probable cause based on viewing of pornographic video file on defendant's computer six months prior to execution of search warrant was stale, absent evidence that defendant had downloaded the video clip and absent evidence of continuous criminal activity); United States v. Greathouse, 297 F. Supp. 2d 1264, 1272-73 (D. Or. 2003) ("Carefully considering all of the factors present in this case, including the limited incriminating evidence, the absence of any evidence of intervening criminal activity, the absence of any evidence that [the suspect] was a pedophile, and the fact that computer equipment becomes obsolete very quickly, I find that the thirteen month delay in this case is simply too long. If a line must be drawn in internet child pornography cases, I find that the line is one year absent evidence of ongoing or continuous criminal activity.").

[196] See, e.g., United States v. Wagers, 339 F. Supp. 2d 934, 941 (E.D. Ky. 2004); United States v. Fisk, 255 F. Supp. 2d 694, 706 (E.D. Mich. 2003) (when the defendant had prior conviction for unlawful sexual involvement with a minor, had wired money to purveyor of child pornography, and when the purveyor sold that pornography over the Internet, there was probable cause to believe that computer contained child pornography).

[197] See, e.g., State v. Evers, 815 A.2d 432, 448 (N.J. 2003) ("Computers are in use in both homes and businesses, and, with the advent of the laptop, in almost every other conceivable place. Business people and students leave

Internet Protocol number, which does "*not directly* reflect the geographic street address of the office, residence, or building from which an individual accesses his email and/or the internet."[198] As a result, "law enforcement officials must conduct research and rely upon the addresses and data provided by internet providers, . . . as well as billing addresses for those service providers and/or credit card companies."[199]

Some courts will infer that the computer is located in the home from the Internet Protocol address assigned to the user's account. For example, in *United States v. Wagers*,[200] the court reasoned that, while the account holder

> had access to the internet from many locations . . . his residence and business locations are certainly the most likely and suspect locations through which he would have accessed the internet. The question, then, is not whether he did or did not access child pornography through the suspect sites from those physical addresses, but, rather, giving the Magistrate Judge's decision great deference, whether there is a "fair probability" that evidence or fruits of criminal wrongdoing would be found.[201]

As another example, in *State v. Brennan*,[202] although the suspect admittedly used his work laptop to view and store child

their homes with laptops, use them at other locations, and return home with them.").

198 United States v. Wagers, 339 F. Supp. 2d 934, 940 (E.D. Ky. 2004). Internet protocol (IP) numbers are owned by Internet service providers; each number is unique to each computer while it is online. Terrence Berg, Practical Issues in Searching and Seizing Computers, 7 T.M. COOLEY J. PRAC. & CLINICAL L. 27, 37 n.22 (2004). However, IP numbers can be either "dynamic" or "static." A dynamic number, typically used by persons who have dial-up Internet service, changes each time the user goes online: "it is only good for that transaction, and then returns to the pool of numbers after the transaction is over." Id. On the other hand, a static IP number, which is more commonly used with cable and DSL connections, is permanently assigned to a customer. Id.

199 Wagers, 339 F. Supp. 2d at 940.

200 Id.

201 Id.

202 674 N.W.2d 200 (Minn. Ct. App. 2004).

pornography, the court found that there was a substantial basis for the magistrate's determination that probable cause existed to search the suspect's home computer based on the training and expertise of the affiant, who asserted that persons with an interest in child pornography tend to view it in their home. The court reasoned, in part, that "viewing and possessing child pornography is, by its nature, a solitary and secretive crime."[203] It accordingly believed that a "court could reasonably draw an inference that the suspect would keep the illicit images in a place considered safe and secret, like the home."[204] The court also relied on the transportable nature of laptops and stated that it was reasonable to infer "that the illicit images found on the laptop would also be found on [the suspect's] home computer."[205]

Screen names also help to identify who the person is. A "screen name" is an identity created by a user and may or may not have any correlation with the user's real name; an individual typically gains access to a screen name by supplying a password that is associated with that screen name.[206] Some courts will find probable cause to search the billing address associated with the screen name.[207] As one court has reasoned:

> The billing address of an account tied to a computer screen name may not be an absolute guarantee that the holder of the computer screen name used the computer at the billing address to commit criminal activity, but there is a fair and logical inference that the computer will probably be found at that address and, if not, at least evidence of the identity of the holder of the screen name will be found there.[208]

---

[203] Id. at 206.

[204] Id.

[205] Id.

[206] United States v. Grant, 218 F.3d 72, 73 n.1 (1st Cir. 2000).

[207] See, e.g., Evers, 815 A.2d at 446 ("[T]he billing address of the Internet screen name–a screen name that had e-mailed photographs of child pornography–was the logical place to search for evidence of the identity of the holder of the screen name and evidence of the crime.").

[208] Evers, 815 A.2d at 446; see also United States v. Campos, 221

Nonetheless, the court cautioned that it would prefer that law enforcement officials take additional steps to verify that the computer from which offending images were sent is located in the defendant's residence.[209]

Other courts have rejected the view that a registered screen name is sufficient to establish probable cause to search the subscriber's computer.[210] Instead, it has been suggested that additional information is needed, such as the fact that the suspect maintained a computer or computer-related equipment at the place to be searched that was capable of transmitting child pornography, the screen name required a particular password, the transmission of child pornography was to a unique Internet or ethernet address assigned to a particular computer at the location to be searched, or the person occupying the place to be searched had an "extreme" interest in young children or had access to Internet sites operated by entities that required those having access to maintain Internet-accessible child pornography.[211] Also relevant to the probable cause determi-

F.3d 1143, 1145 (10th Cir. 2000) (upholding validity of search warrant for defendant's residence after "[l]aw enforcement agents determined that AOL subscriber who used the name `IAMZEUS' was [defendant]"); Hause v. Commonwealth, 83 S.W.3d 1, 4-5, 11-12 (Ky. Ct. App. 2001) (upholding validity of search warrant for residence that was supported by subscriber information obtained from Internet service provider through California search warrant and verification of address by Kentucky law enforcement officials).

[209] Evers, 815 A.2d at 446.

[210] See, e.g., Taylor v. State, 54 S.W.3d 21 (Tex. App. 2001) (no probable cause to search computer for child pornography in Taylor's home when affidavit merely alleged that one image of child pornography sent over the Internet had been traced to screen name registered to Taylor).

[211] See, e.g., Taylor v. State, 54 S.W.3d 21, 25-26 (Tex. App. 2001) (collecting cases); see also United States v. Bach, 400 F.3d 622, 627-28 (8th Cir. 2005) (probable cause existed to search defendant's home computer, even in absence of cross references of IP addresses provided by the ISP and his telephone records based, inter alia, on the fact that the user name employed to correspond to the minor was registered to defendant at his address), cert. denied, 2005 U.S. LEXIS 6585 (U.S., Oct. 3, 2005); United States v. Grant, 218 F.3d 72, 75 (1st Cir.

nation would be the habits of child pornography collectors, their propensity to collect child pornography and maintain the collection at home, and whether the suspect was a pedophile.[212]

B. Consent

1. In General

Consent to search is a question of fact and is determined based on the totality of the circumstances.[213] The ultimate question turns on the voluntary nature of the conse[214] The principles regulating the permissibility of a search or seizure based on a claim of consent do not change in the context of computer searches.[215] However, computers present several challenges to the application of those principles.

2000) (because use of password-protected account requires that user know password associated with account, fair probability that person using account is registrant).

[212] See, e.g., Taylor v. State, 54 S.W.3d 21, 25-26 (Tex. App. 2001); see also Berg, supra note 198, at 42-45 (arguing that there are "good reasons" to follow the Taylor court's approach, including the fact that email headers can be forged, that the information given to an ISP regarding the user's billing address does not mean that a computer is present at that address, and that, with current technology, ISPs can determine the phone numbers and times when the account was accessed).

[213] Ohio v. Robinette, 519 U.S. 33, 40 (1996).

[214] See, e.g., Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (viewing consent as an exception to warrant and probable cause requirements); United States v. White, 401 U.S. 745, 752 (1971); Alderman v. United States, 394 U.S. 165, 179 n.11 (1968); Hoffa v. United States, 385 U.S. 293, 302-03 (1966). Underlying consent principles is the Court's assumption of risk analysis. See, e.g., United States v. Katz, 389 U.S. 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); United States v. Jacobsen, 466 U.S. 109, 118 (1984) (when individual reveals information to another, he assumes the risk that his con-

2. Scope of Consent

fidant will reveal that information). Voluntariness–meaning the lack of coercion by the government agents—must be established. However, the consent need not be an informed one, which is to say that the person giving the consent need not know that he or she has the right to refuse, which is the essential holding of Schneckloth. The Amendment regulates the reasonableness of governmental actors, not the knowledge of private individuals. Hence, it is reasonable for a law enforcement officer to rely on the apparent consent of a person who seems authorized and competent to consent, regardless of whether or not the person is in fact authorized, competent, or otherwise making an informed choice. See Illinois v. Rodriguez, 497 U.S. 177, 183-89 (1990) (consent by person whom police reasonably believe to have common authority over premises validated search); United States v. Matlock, 415 U.S. 164, 171 (1974) (third party may consent to search if party has common authority or other sufficient relationship to premises or effects).

[215] See, e.g., United States v. Mabe, 330 F. Supp. 2d 1234, 1240 (D. Utah 2004) (rejecting assertion that defendant consented to search of computer after police falsely stated that they had search warrant); People v. Yuruckso, 746 N.Y.S.2d 33, 34-35 (N.Y. App. Div. 2002) (consent to search home computer valid, based on defendant's maturity, education, and other factors, even though police stated that, if he did not consent, they would obtain a search warrant and seize his work computer).

A person may "delimit as he chooses the scope of the search to which he consents."[216] The government, in performing a search, cannot exceed the scope of the consent given. This is an objective inquiry: "what would the typical reasonable person have understood by the exchange between the officer and the suspect?"[217] Moreover, the scope of a consensual search is generally defined by its expressed object.[218] This is to say that consent "extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search."[219] Thus, for example, troopers exceeded the scope of

[216] Florida v. Jimeno, 500 U.S. 248, 252 (1991). Cf. United States v. Lemmons, 282 F.3d 920, 924-25 (7th Cir. 2002) (although suspect gave limited consent initially, his later consent to search computer made search valid); United States v. Greene, 56 M.J. 817, 822-23 (N-M. Ct. Crim. App. 2002) (when suspect signed form agreeing that agents could remove and retain his property or papers "which are desired for investigative purposes," agents did not exceed scope of consent when they seized his computer and discs and held them for three months).

[217] Jimeno, 500 U.S. at 251.

[218] Id; see also United States v. Raney, 342 F.3d 551, 558 (7th Cir. 2003) (seizure of "homemade" adult pornography within scope of consent to search for "`materials [that] are evidence in the nature of' child abuse, child erotica, or child exploitation" as it showed ability and intent to manufacture pornography depicting himself in sexual acts); United States v. Turner, 169 F.3d 84, 88-89 (1st Cir. 1999) (scope of defendant's permission to search apartment in connection with intruder's assault on neighbor exceeded when police accessed files on his computer because the police request would have been reasonably understood to be that they intended to search for physical evidence of the assault); State v. Brown, 813 N.E.2d 956, 960 (Ohio Ct. App. 2004) (scope of defendant's consent exceeded when police seized two computers from his home when he had merely given consent to look at computers); People v. O'Brien, 769 N.Y.S.2d 654, 656 (N.Y. App. Div. 2003) ("[T]he fact that the defendant's written consent was expressly limited to only the Comp USA computer and monitor located in his bedroom reveals defendant's intent to maintain his privacy in all other contents of his bedroom," including another computer).

[219] United States v. Ross, 456 U.S. 798, 820-21 (1982); see also Jimeno, 500 U.S. at 251 (consent to search car included closed paper bag on floor of car); Commonwealth v. Hinds, 768 N.E.2d 1067, 1071 (Mass. 2002) (when

the driver's consent to search his vehicle for guns, drugs, money, or illegal contraband when they accessed the computer memory of a cellular phone to retrieve its electronic contents.[220] This is because a reasonable person would have understood the driver's consent to be limited to "search any containers inside the vehicle which might reasonably contain those specific items" and none of the objects sought would be found by accessing the phone's electronic contents.[221]

On the other hand, when a graduate student in computer science agreed to allow agents to search his entire home and to take his computer back to the FBI office for further examination, it was held that the student "would have realized that the examination of his computer would be more than superficial when the agents explained that they did not have the skills nor the time to perform the examination at his home."[222] Moreover, according to the court, "a graduate student in computer science would clearly understand the technological resources of the FBI and its ability to thoroughly examine his computer."[223] Given the lack of limitations put on the search by the student, his cooperation, and his expertise, the court believed it was reasonable for the agents to conclude that they had unlimited access to the computer.[224]

defendant consented to search of his computer for electronic mail, valid search not limited to specific directories or locations on computer).

220 Smith v. State, 713 N.E.2d 338, 343-44 (Ind. Ct. App. 1999).

221 Id.

222 United States v. Al-Marri, 230 F. Supp. 2d 535, 539-40 (S.D.N.Y. 2002).

223 Id. at 540.

224 Id.

3. Third Party Consent

The validity of third party consent depends on whether the person giving consent has either actual authority or apparent authority to consent.[225] In general, a third party may consent to a warrantless search when that party possesses "common authority over or other sufficient relationship to the premises or effects sought to be inspected."[226]

> Common authority is . . . not to be implied from the mere property interest a third party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.[227]

The issue frequently arises in the context of shared computer use. The question, as with consent generally, turns on the person's access or control of the computer, regardless of whether the person is a spouse,[228] parent,[229] other family mem-

---

[225] See, e.g., United States v. Smith, 27 F. Supp. 2d 1111, 1115 (C.D. Ill. 1998).

[226] United States v. Matlock, 415 U.S. 164, 171 (1974); see also Frazier v. Cupp, 394 U.S. 731, 740 (1969) (rejecting inquiry into "metaphysical subtleties" of argument that, because joint user of duffle bag only had actual permission to use one compartment, he could not consent to search of whole bag).

[227] Matlock, 415 U.S. at 171 n.7.

[228] See Walsh v. State, 512 S.E.2d 408, 411-12 (Ga. Ct. App. 1999) (defendant's wife had authority to consent to search of computer that she purchased and was available for use by family).

[229] See People v. Blair, 748 N.E.2d 318, 324-25 (Ill. App. Ct. 2001) (father, who had no actual or apparent ownership of computer, could not validly

ber,[230] house mate,[231] bailee,[232] systems administra-tor,[233] or other third party,[234] such as a computer repair person.[235]

The presence of password-protected files is an important consideration in assessing a third party's authority to consent. For example, in *Trulock v. Freeh*,[236] the court held that a resi-

consent to seizure of son's computer).

[230] See State v. Guthrie, 627 N.W.2d 401 (S.D. 2001) (son-in-law possessed common authority over computer and could validly consent to its seizure when he had unconditional access and control over it).

[231] See United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998) (housemate had authority to consent to search of defendant's computer, to which she had joint access and was located in common area of house; alternatively, government agents reasonably believed housemate could consent to search).

[232] See United States v. James, 353 F.3d 606, 614-15 (8th Cir. 2003) (bailee, who agreed to store disks and who had been later directed to destroy them, did not have actual or apparent authority to permit police to take and examine them).

[233] A "systems administrator" is the person "whose job is to keep [a computer] network running smoothly, monitor security, and repair the network when problems arise." CCIPS Manual, supra note 46, at 22. Those administrators "have `root level' access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems." Id. As the CCIPS manual emphasizes, "the primary barrier to searching a network account pursuant to a system administrator's consent is statutory, not constitutional. Systems administrators typically serve as agents of `provider[s] of electronic communication service' under the Electronic Communications Privacy Act (`ECPA'), 18 U.S.C. §§ 2701-2712." Id. Any attempt by law enforcement to obtain a system administrator's consent must comply with those provisions. Id. at 22-23. Regarding the Fourth Amendment, it is doubtful that a person using networks will be found to have a reasonable expectation of privacy in remotely stored files. See CCIPS Manual, supra note 46, at 23.

[234] See United States v. Meek, 366 F.3d 705, 711 (9th Cir. 2004) ("Like private phone conversations, either party to a chat room exchange has the power to surrender each other's privacy interest to a third party.").

[235] United States v. Barth, 26 F. Supp. 2d 929, 938 (W.D. Tex. 1998) (computer repair person does not have actual authority to consent to search of customer's hard drive, having "possession of the unit for the limited purpose of repair" and did not have apparent authority when police knew his status).

[236] 275 F.3d 391 (4th Cir. 2001).

dent of a townhouse, Conrad, could not authorize the search of password-protected files of another resident, Trulock, on a computer that was jointly used when Conrad did not have access to the passwords. The court reasoned by analogy to the case of a mother who was found not to have authority to consent to the search of a locked footlocker in her son's room, which was located in a home they shared, and added: "By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files."[237] On the other hand, the lack of passwords to protect files has been held to defeat a claim that the defendant had exclusive control of a computer and that his housemate did not have authority to consent to search.[238]

[237] Id. at 403.

[238] United States v. Smith, 27 F. Supp. 2d 1111, 1116 (C.D. Ill. 1998).

C. Particularity Claims

1. In General

The Fourth Amendment requires that a search warrant describe with particularity "the place to be searched, and the persons or things to be seized."[239] The particularity requirement prevents a "general, exploratory rummaging in a person's belongings"[240] and the seizure of one thing under a warrant describing another.[241] It also "`assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.'"[242] Although the Supreme Court has observed that, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant,"[243] this admonition has not been applied strictly by courts.[244] A warrant satisfies the particularity requirement if it enables the executing officer to identify with reasonable certainty those items that the issuing magistrate has authorized him to seize.[245] This is determined, *inter alia*,[246] by the nature of the activity charged[247] and the nature of the objects to be seized.[248] Without a sufficiently specific warrant, the search is considered warrantless.[249]

---

239 U.S. CONST. amend. IV.

240 Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

241 Marron v. United States, 275 U.S. 192, 196 (1927); see also LAFAVE, supra note 95, § 4.6(a) at 605 (underlying purposes of the particularity requirement are to prevent general searches and to prevent the "seizure of objects under the mistaken assumption that they fall within the magistrate's authorization").

242 Groh v. Ramirez, 540 U.S. 551, 561 (2004) (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977)).

243 Marron, 275 U.S. at 196.

244 See, e.g., Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997) (a "warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the

2. Varieties of Computer Searches

activity under investigation permit"); United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("Once a category of seizable papers has been adequately described, with the description delineated in part by an illustrative list of seizable items, the Fourth Amendment is not violated because the officers executing the warrant must exercise some minimal judgment . . . .").

245 Maryland v. Garrison, 480 U.S. 79, 84 (1987).

246 See LAFAVE supra note 95, § 4.6(a) at 609-13 (summarizing many of the general principles that can be distilled from the decided cases).

247 See, e.g., Andresen v. Maryland, 427 U.S. 463, 479-80 (1976) (phrase seeking all evidence was not general when modified by sentence referring to specific crime); United States v. Johnson, 541 F.2d 1311, 1314 (8th Cir. 1976); United States v. Abbell, 963 F. Supp. 1178, 1196 (S.D. Fla. 1997).

248 LAFAVE, supra note 95, § 4.6(a) at 609-11; see also State v. Wible, 51 P.2d 830, 836 (Wash. App. 2002) ("Courts evaluating alleged particularity violations distinguish between inherently innocuous items, such as [a] computer, and inherently illegal property, such as controlled dangerous substances. . . . Innocuous items require greater particularity.").

249 Groh, 546 U.S. at 558.

There are two varieties of computer searches: one is to seize the equipment, that is, the computer hardware and software; the other is to obtain the data contained in the computer equipment, including on hard drives and various storage devices, such as floppy disks. Helpful analysis in recognizing this distinction is contained in *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*.[250] Although decided under Federal Rule of Procedure 17(c) rather than under the Fourth Amendment, the court was presented with a subpoena that demanded that X Corporation provide the grand jury with the central processing unit, including the hard drive, of any computers supplied by the corporation to specified employees. The subpoena also demanded all computer-accessible data, including floppy diskettes created by those employees or their assistants. The court noted that, not only were corporate records within the scope of the subpoena, so were personal documents. The grand jury was investigating securities trading activities and obstruction of justice. The court observed:

> The subpoena at issue here is not framed in terms of specified categories of information. Rather, it demands specified information storage devices–namely, particular computer hard drives and floppy disks that contain some data concededly irrelevant to the grand jury inquiry. . . . If the categories of materials properly are seen to be hard disk drives and floppy disks, then . . . it is highly probable that these devices will contain some relevant information. If, on the other hand, the categories of materials properly are seen to be the various types of documents contained on these devices, then the subpoena would be unreasonably broad because there are easily separable categories of requested documents that undoubtedly contain no relevant information.[251]

Concluding that the grand jury was actually seeking documents and not the devices that stored them, the court held that the

---

250 846 F. Supp. 11 (S.D.N.Y. 1994).

251 Id. at 12.

subpoena was too broad.[252] Similarly, under the Fourth Amendment, it must be determined whether the computer is a mere storage device for data[253] or whether the equipment[254] is the object sought.

a. Searches for Computer Equipment

In the context of warrants issued to seize computer software and hardware,[255] the courts have often found fairly generic descriptions of the items to be seized to be sufficient.[256] For example, merely labelling the objects to be seized as evidence of, or an instrumentality[257] of, a crime as "computer equipment"[258] or even "equipment"[259] relating to a specific crime has sufficed. Of course, if computer equipment has been stolen and that specific equipment is the object of the search, it would have to be described with sufficient particularity to identify it.[260]

---

[252] Id. at 13-14.

[253] See, e.g., United States v. Gawrysiak, 972 F. Supp. 853, 860-61 (D.N.J. 1997) (approving warrant to search for documents related to wire fraud investigation, including records stored in magnetic or electronic forms), aff'd, 178 F.3d 1281 (3d Cir. 1999).

[254] See, e.g., Arkansas Chronicle v. Easley, 321 F. Supp. 2d 776, 793 (E.D. Va. 2004) (comparing seizure of computer equipment in child pornography cases, where those devices are considered instrumentalities of crime, with computers that are tools of journalist's trade that may or may not contain evidence); United States v. Hunter, 13 F. Supp. 2d 574, 584-85 (D. Vt. 1998) (warrant authorizing wholesale seizure of computers and related devices, without specifying crime for which computers were sought, violated particularity requirement).

[255] See, e.g., CCIPS Manual, supra note 46, at 63-64 (discussing that, under Fed. R. Crim. P. 41(b), agents may obtain search warrants to seize computer hardware if the hardware is contraband, evidence, or an instrumentality or fruit of a crime).

[256] See, e.g., State v. Lehman, 736 A.2d 256, 260-61 (Me. 1999) (collecting cases).

[257] See, e.g., Arkansas Chronicle v. Easley, 321 F. Supp. 2d 776, 793 (E.D. Va. 2004) (comparing seizure of computer equipment in child pornography cas-

b. Searches for Data

es, where those devices are considered instrumentalities of crime, with computers that are tools of a journalist's trade).

[258] See United States v. Lacy, 119 F.3d 742, 745-47 (9th Cir. 1997), cert. denied, 523 U.S. 1101 (1998) (upholding warrant issued for search of "computer equipment and records" that resulted in seizure of computer, more than 100 computer disks, and documents when government knew that suspect had downloaded child pornography but did not know where the images had been stored, with the court concluding that "this type of generic classification is acceptable `when a more precise description is not possible'"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999), cert. denied, 527 U.S. 1011 (1999) (observing that warrant issued for "[a]ny and all computer software and hardware, . . . computer disks, disk drives" is easily administered by seizing officer based on objective criteria whether item is computer equipment).

[259] Davis v. Gracey, 111 F.3d 1472, 1478-79 (10th Cir. 1997) (computers, monitors, keyboards, modems, CD-ROM drives, and changers were within the meaning of warrant that directed officers to search for "equipment . . . pertaining to the distribution or display of pornographic material").

[260] See, e.g., State v. Tanner, 534 So. 2d 535, 537 (La. App. 1988) (when defendant illegally copied software and other materials belonging to First Page Beeper Services, warrant not overbroad that authorized seizure of "all other computer related software" that bore the name "First Page Beepers"). But cf. State v. Wade, 544 So. 2d 1028, 1029-30 (Fla. App. 1989) (warrant, which resulted in seizure of 53 items, that authorized seizure of "computer equipment and business records" that had been stolen from Controlled Data Corporation was sufficiently particular when it incorporated by reference exhibit listing three specific items but was not limited to those items).

As discussed at the beginning of this article,[261] there are two principal approaches to searches involving electronic data stored on computers, that is, whether a computer is a form of a container and the data in electronic storage mere forms of documents or whether such searches for data require a "special approach." Perhaps the most significant consequence of those competing views is in the application of the Fourth Amendment's particularity requirement. If data is considered a form of a document and the computer is just a container holding that document, the traditional limitations on document searches apply.[262] On the other hand, if the court rejects such an analogy and adopts the "special approach" to searches of data on computers, then unique limitations are likely to be imposed.[263]

D. Plain View

The permissible scope of a search is usually determined by the objects sought under the warrant. If small objects (such as fibers or bullets) are the target of the search, law enforcement officials can look anywhere such an object may be hidden; if only large objects are sought, the officials can only look where that size of object can be concealed. In executing a search, it is not uncommon for the police to encounter objects that are incriminating or have evidentiary value for which they did not have prior authority to search or seize. Under such circumstances, the plain view doctrine may justify seizure of the object. That doctrine has three requirements: a prior valid intrusion; observing an object in plain view; and the incriminating character of the object must be immediately apparent.[264]

---

261 See discussion supra at 197-205.

262 See discussion supra at 197-201.

263 See discussion supra at 202-20.

264 Horton v. California, 496 U.S. 128, 136-37 (1990). There is no requirement that the spotting of the object be inadvertent. Id.; see also Ivatury v. State, 792 S.W.2d 845, 851 (Tex. Ct. App. 1990) (based on warrant to search safety

In the context of searches of computers for electronic evidence, if the police are otherwise validly in position to observe a computer screen, their observations of what is depicted on the screen will be considered in plain view.[265] As to observations of the contents of unopened files, what is in plain view is determined by whether the court accepts the view that data are mere types of document searches,[266] and hence the official can look at all data to ascertain its value when executing a warrant to search for documents,[267] or whether the court takes a special

deposit box during espionage investigation, discovery of special type of computer tape in box used in defense industry in plain view).

[265] See State v. Mays, 829 N.E.2d 773, 779 (Ohio Ct. App. 2005) (observations of information on computer screen during consent search of home in plain view); United States v. Tanksley, 50 M.J. 609, 620 (N-M. Ct. Crim. App. 1999) (observations of information on computer screen made during search of office were in plain view); People v. Blair, 748 N.E.2d 318, 323 (Ill. App. 2001) (when police observed `bookmarks with references to teenagers and so forth,' they did not have probable cause to believe that computer contained child pornography); State v. One Pioneer CD-ROM Changer, 891 P.2d 600, 604-05 (Okla. Civ. App. 1995) (during execution of search warrant based on allegations that suspect was distributing pornographic material, police observations of computer monitor "displaying the words `viewing' and/or `copying' with descriptions such as `lesbian sex' and/or `oral sex'" established that the equipment and its possible criminal use were in plain view). Cf. United States v. Turner, 169 F.3d 84, 88 (1st Cir. 1999) (observation of officer during consensual search of apartment of photograph of a nude woman on computer screen did not justify search of computer for other incriminating files); State v. Brown, 813 N.E.2d 956, 960-62 (Ohio Ct. App. 2004) (incriminating nature of computers and their contents not immediately apparent based on mere observation of two computers in defendant's house, with no pornography displayed on screen, when police merely knew that pornographic material had been printed from some computer). Of course, if there is no prior intrusion at all, that is, no prior search or seizure within the meaning of the Fourth Amendment, then an officer's use of her sight to observe something is not a search. See, e.g., United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (agent's looking over defendant's shoulder to see password for defendant's computer not search).

[266] See discussion supra at 198-206.

[267] See, e.g., United States v. Gray, 78 F. Supp. 2d 524, 531 n.11 (E.D. Va. 1999) (when agent is engaged in "systematic search" of computer files pursuant to warrant, any evidence discovered could be seized under plain view

approach[268] to computer searches and imposes limitations on the search by, for example, file name or file type.[269] It also depends on how the court defines the relevant container.[270]

doctrine); Commonwealth v. Hinds, 768 N.E.2d 1067, 1072 (Mass. 2002) (police had right to open file that officer believed contained child pornography based on file's name during search of computer for email; accordingly, child pornography was in plain view); State v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000) (rejecting limitations on search based on file names and concluding that, during systematic search of all user-created files in executing search warrant for evidence of online harassment and disorderly conduct, opening file containing child pornography in plain view); Frasier v. State, 794 N.E.2d 449, 462-66 (Ind. Ct. App. 2003) (rejecting limitations on a search based on file names and extensions, and concluding that plain view doctrine applied when police opened file and observed child pornography during execution of warrant permitting police to examine notes and records for evidence of drug trafficking). Cf. United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003) (under warrant permitting search of graphic files for evidence of murder, observations of files containing child pornography in plain view); United States v. Tucker, 305 F.3d 1193, 1202-03 (10th Cir. 2002) (parole agreement authorized search of computer; upon viewing child pornography on it, plain view permitted seizure).

[268] See discussion supra at 202-20.

[269] See United States v. Carey, 172 F.3d 1268, 1272-75 (10th Cir. 1999) (opening of files containing child pornography, at least after first file was opened, during execution of search warrant for documentary evidence relating to drug dealing, not justified by plain view doctrine because files were "closed" and "unambiguously" named). Cf. United States v. Abbell, 914 F. Supp. 519, 520-21 (S.D. Fla. 1995) (in criminal prosecution where large volume of computer generated data seized from defendant's law office, special master would determine whether documents and data were responsive to warrant or fell within exception to warrant requirement); United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996) (where officer used personal computer to transport obscenity and child pornography, plain view doctrine inapplicable to search of computer files under screen name not listed in warrant); see also Brenner & Frederiksend, supra note 18, at 89-106 (advocating significant restrictions on application of plain view doctrine to computer searches).

[270] See discussion supra at 233-44.

E. Execution Issues

1. On-site/Off-site Searches; Intermingled Documents

One question that has often arisen is whether the government may remove the computer, including its hard drive and disks, to the police station for detailed forensic examination. Answering this question, courts have fairly consistently held that, due to the intermingling of legitimate and illegitimate items, the technical difficulty of examination, and the volume of information seized, temporary seizures of the computer and removal off site for examination are permitted.[271] Underlying the courts' analysis is the fundamental premise that "current technology does not permit proper on-site examination of computer files."[272] For example, in *United States v. Hill*,[273] the court concluded that the police were not required to bring with them equipment capable of reading computer storage media and an officer competent to operate it; the court observed:

---

[271] See, e.g., United States v. Walser, 275 F.3d 981, 985 (10th Cir. 2001) (observing that seizure is appropriate in variety of circumstances, including "the impracticality of on-site sorting" and because "computer evidence is vulnerable to tampering or destruction"); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (due to "technical difficulties of conducting a computer search in a suspect's home," permissible to seize computers and their contents and remove to allow police to locate relevant data); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding, in child pornography case, warrant authorizing seizure of computer system because of the "time, expertise, and controlled environment required for a proper analysis"); Upham, 168 F.3d at 535 ("As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs."); United States v. Sissler, 966 F.2d 1455 (6th Cir. 1992), cert. denied, 506 U.S. 1079 (1993) (police permitted to remove

computers from defendant's residence to continue search off-site); Mahlberg v. Mentzer, 968 F.2d 772, 775 (8th Cir. 1992) (seizure of 160 computer disks permissible when searching for two computer files because of possibility that computer was `bobby-trapped' to erase itself and because it was unknown which disks contained the files); United States v. Schandl, 947 F.2d 462, 465-66 (11th Cir. 1991), cert. denied, 504 U.S. 975 (1992) (in tax evasion case, which requires "careful analysis and synthesis of a large number of documents," it might be more disruptive to conduct thorough search of each individual document and computer disk before removing it; to insist on such a practice would substantially increase time to conduct search, thereby aggravating its intrusiveness); United States v. Maali, 346 F. Supp. 2d 1226, 1246 (M.D. Fla. 2004) ("Warrants authorizing seizure of computer equipment for later off-site search of their contents for evidence . . . have been upheld, especially where, as here, the supporting affidavit explained the reason such off-site analysis was necessary."); United States v. Leveto, 343 F. Supp. 2d 434, 449-50 (W.D. Pa. 2004) (in large tax fraud scheme, involving many documents and computer files, off-site inspection permissible); United States v. Albert, 195 F. Supp. 2d 267, 278-79 (D. Mass. 2002) (upholding off-site search because "the mechanics of searching a hard drive by viewing all of the information it contains cannot be readily accomplished on site"); United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("Often it is simply impractical to search a computer at the search site because of the time and expertise required to unlock all sources of information."); United States v. Yung, 786 F. Supp. 1561, 1569 (D. Kan. 1992) (computer files "clearly could not be individually reviewed prior to completion of the search"); People v. Gall, 30 P.3d 145, 154-55 (Colo. 2001) (seizure of computers and later search off site upheld). Cf. United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) ("A reasonable-search of computer files may include copying those files on to a disk on the scene, for later time-consuming review of the index of documents to cull the relevant time periods and subject matters while returning the remainder."), aff'd, 178 F.3d 1281 (3d Cir. 1999); CCIPS Manual, supra note 46, at 64-66 (discussing possible search strategies where the hardware is a mere storage device for electronic evidence). But see Brenner & Frederiksen, supra note 18, at 45-89 (extensively analyzing the off/on site issue and advocating the view that an off-site search "should be treated as an "unusual measure" and specifically authorized by a magistrate, id. at 76, and that computer hardware cannot be seized absent explanation in warrant application of technical reasons why the search cannot be conducted on-site or conducted off-site using forensic back-up copies of data, id. at 75).

[272] United States v. Al-Marri, 230 F. Supp. 535, 541 n.3 (S.D.N.Y. 2002); see also United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000)

> Doing so would have posed significant technical problems and made the search more intrusive. . . . Because computers in common use run a variety of operating systems—various versions or flavors of Windows, Mac OS and Linux, to name only the most common—police would have had to bring with them a computer (or computers) equipped to read not only all of the major media types, but also files encoded by all major operating systems. Because operating systems, media types, file systems and file types are continually evolving, police departments would frequently have to modify their computers to keep them up-to-date. This would not be an insuperable obstacle for larger police departments and federal law enforcement agencies, but it would pose a significant burden on smaller agencies.
>
> Even if the police were to bring with them a properly equipped computer, and someone competent to operate it,

(quoting FBI agent's explanation as to why it was not usually feasible to search for particular computer files in person's home, which included the volume of information, user attempts to conceal criminal evidence, need for an expert examiner, controlled environment, wide variety of computer hardware and software, and vulnerably of evidence to tampering or destruction); United States v. Greene, 56 M.J. 817, 823-24 (N-M. Ct. Crim. App. 2002) (discussing expert witness testimony on effective forensic analysis, including danger of destruction of evidence when conducting on-site examinations and need for off-site analysis to protect evidence); Gall, 30 P.3d at 154-55 ("In addition to the problems of volume and commingling, the sorting of technological documents may require a search to be performed at another location `because that action requires a degree of expertise beyond that of the executing officers,' not only to find the documents but to avoid destruction or oversearching."). Cf. United States v. Greathouse, 297 F. Supp. 2d 1264, 1269, 1275 (D. Or. 1275) (although acknowledging that numerous cases have upheld the "wholesale seizure of computers and computer disks and records for later review for particular evidence as the only reasonable means of conducting a search," observing "that this may not always be true due to technological developments" and stating that, in the appropriate situation, "there may well be an obligation" to use a computer forensics program "to more narrowly tailor the search and seizure"); Hunter, 13 F. Supp. 2d at 583 ("until technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur").

[273] 322 F. Supp. 2d 1081 (C.D. Cal. 2004).

> using it would pose two significant problems. First, there is a serious risk that the police might damage the storage medium or compromise the integrity of the evidence by attempting to access the data at the scene. As everyone who has accidentally erased a computer file knows, it is fairly easy to make mistakes when operating computer equipment, especially equipment one is not intimately familiar with. The risk that the officer trying to read the suspect's storage medium on the police laptop will make a wrong move and erase what is on the disk is not trivial. Even if the officer executes his task flawlessly, there might be a power failure or equipment malfunction that could affect the contents of the medium being searched. For that reason, experts will make a back-up copy of the medium before they start manipulating its contents. Various other technical problems might arise; without the necessary tools and expertise to deal with them, any effort to read computer files at the scene is fraught with difficulty and risk.
>
> Second, the process of searching the files at the scene can take a long time. To be certain that the medium in question does not contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress, and this would necessarily interfere with the suspect's access to his home or business. If the search took hours or days, the intrusion would continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible.[274]

Because of these considerations, the court concluded that the police were not required to examine the electronic storage media at the scene to determine which contained child pornography and which did not but were, instead "entitled to seize all

[274] Id. at 1088-89.

such media and take them to the police station for examination by an expert."[275]

Nonetheless, courts have expressed concerns about such wholesale seizures due to the disruption of businesses, professional practices, and personal lives that such seizures entail.[276] Accordingly, courts have been cautious in their approval of such practices.[277] Some urge that the government copy the data and return the equipment as soon as possible.[278] A few courts appear to require a second warrant before searching when the government seizes intermingled documents.[279]

---

[275] Id. at 1089.

[276] Hunter, 13 F. Supp. 2d at 583.

[277] See, e.g., Upham, 168 F.3d at 535.

[278] Hunter, 13 F. Supp. 2d at 583. Cf. Leveto, 343 F. Supp. 2d at 441 (in large tax fraud scheme, involving many documents and computer files, factually describing how executing officials took "considerable steps" to minimize "upheaval" of veterinarian's business, including copying computer files rather than removing computers). But cf. Malapanis v. Regan, 335 F. Supp. 2d 285, 291 (D. Conn. 2004) (failure of police to return computer equipment does not implicate Fourth Amendment; it is, instead, analyzed under procedural due process); LM Bus. Assoc. v. Ross, No. 04-CV-612CJS 2004 WL 2609182, at *5 (W.D.N.Y. Nov. 17, 2004) (same).

[279] See, e.g., United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999). This requirement is based on precedent requiring a second warrant when the police seize intermingled documents. See United States v. Shilling, 826 F.2d 1365, 1369-70 (4th Cir. 1987) (although stating that "we cannot easily condone the wholesale removal of file cabinets and documents not covered by the warrant," concluding that there were legitimate practical concerns that prompted the removal of file cabinets and observing that seizure not based on intent to engage in fishing expedition); United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982) (suggesting that when documents are so intermingled that sorting on site is not feasible, Fourth Amendment violations can be avoided by sealing documents and obtaining additional search warrant). Other courts reject that requirement for document searches. See, e.g., United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (seizure of entire file cabinet permissible, including intermixed warrant-specified and unspecified documents). Some courts have raised these concerns in the computer context but have not specifically addressed the issue. See, e.g., Upham, 168 F.3d at 536 ("This problem arises in a variety of different contexts and in many permutations; matters of degree are involved and there is probably no single

2. Use of Experts

Because of the complicated nature of the evidence and equipment that computer-related searches give rise to, governmental authorities sometimes use computer experts to facilitate the execution of a search warrant. Challenges to the use of such experts, although few, have been consistently rejected.[280] The civilian, of course, must be "serving a legitimate investigative function,"[281] including using his or her special expertise to identify "property of a technical nature not generally familiar to law enforcement officers."[282] Approval has even extended to situations where the private experts performed the search outside of the presence of law enforcement officials.[283]

---

rule that resolves all such situations."). Cf. Hill, 321 F. Supp. 2d at 1090 ("The warrant here authorized precisely such a seizure of intermingled materials that are difficult and time-consuming to separate on-site. That the officer seeking the warrant did not make a specific showing to this effect is of no consequence: The difficulties of examining and separating electronic media at the scene are well known. It is doubtless with these considerations in mind that the state court judge authorized seizure of all of defendant's storage media, not merely those containing contraband or evidence of crime."); Gall, 30 P.3d at 154-55 (observing that the problem of "properly limiting a search of the contents of a lawfully seized computer" was not at issue because search pursuant to second, more detailed warrant).

[280] See, e.g., Belleville v. Town of Northboro, 375 F.3d 25, 32 (1st Cir. 2004) ("Federal constitutional law does not proscribe the use of civilians in searches."); Hill, 322 F. Supp. 2d at 1088 n.10 (recognizing that experts may be advisable to limit search); United States v. Schwimmer, 692 F. Supp. 119, 126-27 (E.D.N.Y. 1988) (summarily rejecting challenge to use of computer expert).

[281] Belleville, 375 F.3d at 32.

[282] Wade, 544 So. 2d at 1030-31 (computer experts from company from which computer equipment was stolen assisted in identifying equipment); accord Belleville, 375 F.3d at 32.

[283] See United States v. Bach, 310 F.3d 1063, 1066-68 (8th Cir. 2002) (private Internet service provider employees searched suspect's email), cert. denied, 538 U.S. 993 (2003).

3. Deleted Files

When a computer user "deletes" a file, the data that was contained in that file may remain in the computer memory:

> Most word processing programs use some form of a recycle bin, into which documents are transferred when deleted. Thus, a computer is also like a wastebasket of discarded material. In order to attempt to permanently delete such documents, the recycle bin must be emptied. However, even emptying the recycle bin may not actually delete the document or file because the information may still remain on the computer's hard drive.
>
> The intentional deletion of a file does not permanently erase the file. Instead, the computer internally marks the file as not needed, and clears space for storage of other files. The erasure of information only occurs when the computer overwrites the file with another file. Even then, fragments of information may be retrievable if the entire file is not overwritten. Furthermore, word processing programs may have saved portions or versions of documents regardless of whether the user intentionally saves the final version.
>
> Thus, in general, a file or document may not be removed from the hard drive of a computer until it is reformatted. However, even then, it may be possible to partially recover documents or files removed from a hard drive, depending on how the drive was reformatted. Further, the potential for deleted material to be stored on a hard drive, with or without intentional saving by the user, is not limited to word processing documents, but applies to other programs and functions of a computer as well.[284]

Because technicians can often recover much of that data using electronic search technology, courts have confronted a variety of

---

[284] Gall, 30 P.3d at 161 (Martinez, J., dissenting) (citations omitted). See, e.g., Upham, 168 F.3d at 537 (rejecting scope argument and asserting that recovery of deleted files no different than "pasting together scraps of a torn-up ransom note").

issues regarding the admissibility of such "deleted" data. Some courts have addressed–and rejected–the government claim that the files have been abandoned.[285] The analogy of deletion of a file to putting one's trash out in the street is flawed, according to one court, because in the latter situation, but not the former, every passerby can search the trash.[286]

On the other hand, defendants have claimed that the recovery of deleted files is outside the scope of a warrant;[287] the assertion is that a second warrant is required or the scope of the original warrant has been exceeded because the "deletion" of the documents creates a new and legally different expectation of privacy protected by the Amendment.[288] Rejecting such a claim, one court has reasoned that an "attempt to secrete evidence of a crime is not synonymous with a legally cognizable expectation of privacy."[289] The court analogized the situation to a paper tablet and a diary recorded in a private code, both of which may be subjected to scientific analysis after seizure pursuant to a warrant; the court concluded that no second warrant was required "before subjecting legally seized physical evidence to scientific testing and analysis to make it divulge its secrets."[290]

V. CONCLUSION

Courts are increasingly confronting the problems associated with adapting Fourth Amendment principles to modern

---

285 See, e.g., Upham, 168 F.3d at 537 n.3. Cf. United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002) (when defendant did not have access to data he previously attempted to delete on university owned computer, he had no reasonable expectation of privacy in that data).

286 Upham, 168 F.3d at 537 n.3.

287 See, e.g., id. at 537 (recovery of deleted files no different than "pasting together scraps of a torn-up ransom note").

288 Commonwealth v. Copenhefer, 587 A.2d 1353, 1356 (Pa. 1991).

289 Id.

290 Id.

technology.[291] Supreme Court jurisprudence, developed to regulate traditional search and seizure practices, presents conceptual problems when applied to the world of cyber-space and electronically stored evidence. Some authorities are reluctant to accept–or outright reject–analogies to physical world searches and seizures. This article concludes, however, that there is nothing "special" in the nature of computer searches that differentiate them in any principled way from other document and container searches. Assuming the validity of the document/container analogy, however, also requires recognition of what the relevant container is, which has significance for application of the plain view and private search doctrines. Traditional Fourth Amendment principles can be translated to the search of electronic evidence. Although one may dispute the correctness of some of the Supreme Court's development of Fourth Amendment principles, as I have elsewhere, there is nothing *sui generis* where the target of the search or seizure is a computer or other device that contains electronic evidence.

[291] See generally Symposium: The Effect of Technology on Fourth Amendment Analysis and Individual Rights, 72 MISS. L.J. 1 (2002).