BNA, INC.

CRIMINAL LAW REPORTER

BNA Employee-Owned Since 1947

SEARCH AND SEIZURE

Computer Search and Seizure Under the Fourth Amendment: The Dilemma of Applying Old-Age Principles To New-Age Technology

BY ALAIN LEIBMAN

Few provisions in the Bill of Rights illustrate the shortcomings of an ''original intent'' approach to constitutional interpretation better than the Fourth Amendment's guarantee against unreasonable searches and seizures. Eighteenth-century words must be given new meaning to maintain their currency in the 21st century. As recordkeeping has shifted from storing a few parchment documents in Colonial-era footlockers to housing millions of bytes of data on portable laptops, notebooks, and personal digital assistants, Fourth Amendment jurisprudence has struggled to balance legitimate law enforcement needs with modern expectations of privacy in electronic storage media. No consensus has yet been achieved on how to update the legal construct of the Fourth Amendment to encompass new means of maintaining information, as the courts of appeals have arrayed themselves at every imaginable point along the spectrum of possible interpretations.

The simple words of the Fourth Amendment, ratified in 1791, provide as follows:

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

Violations of the Fourth Amendment's warrant requirement have for nearly the last 100 years been remedied by excluding the use of illegally obtained materi-

als as evidence. *Weeks v. United States*, 232 U.S. 383, 398 (1914) (exclusionary remedy as applied to federal court proceedings).

Some of the most commonly applied exceptions to the warrant requirement were established and continue to be applied in the context of brick-and-mortar locations or physical containers and storage areas. For example, evidence of criminal activity in the plain view of a law enforcement officer who is lawfully entitled to be in a particular premises may be seized without a warrant. *See Coolidge v. New Hampshire*, 403 U.S. 443, 465 (1971) (plurality opinion). But applying the plain-view doctrine in regard to the contents of a computer has been described as ''intriguing.'' *United States v. Carey,* 172 F.3d 1268, 1273 (10th Cir. 1999).

In addition, an authorized and voluntary consent to search dispenses entirely with the warrant requirement, *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973), and a cohabitant of a residence may have authority to consent to a warrantless search of the place. *See Illinois v. Rodriguez*, 497 U.S. 177, 181-82 (1990). But does a single user among several of a computer hard drive have the same authority to consent to the search of folders/files used exclusively by another as does a co-resident of a premises to the search of a roommate's bedroom?

Several of the historically most contentious Fourth Amendment issues assume a different cast when posed in the electronic dimension. Recent court of appeals decisions in this area emphasize the fluidity of these issues, such as the requirement that a search be bounded by the terms of a particularized warrant to avoid becoming a general search for incriminating information; the meaning of ''plain view'' inside a computer; and the authority to consent to the search and seizure of computer media without a warrant. The problem that overarches them all is that of cross-millennial translation. As the Tenth Circuit has said, ''Analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.' '' *Carey,* 172 F.3d at 1275 (quotation omitted). ''One might speculate whether the Supreme Court would treat laptop computers, hard drives, flash drives or even cell phones as it has a briefcase or give those types of devices preferred status because of their unique ability to hold vast amounts of diverse personal information.'' *United States v. Burgess,* 576 F.3d 1078, 1090 (10th Cir.), *cert. den.,* 130 S. Ct. 1028 (2009). The lack of U.S. Supreme Court guidance has compelled the varying, and strikingly different, speculations of intermediate appellate judges in response to these matters.

Alain Leibman is a principal member of the White Collar Compliance and Defense group at Fox Rothschild LLP, based in its Princeton, N.J., office, where he also practices commercial litigation. Leibman was an Assistant U.S. Attorney in the U.S. Attorney's Office for the District of New Jersey from 1988-2004, where he served as a deputy chief and senior litigation counsel. He writes about criminal, evidentiary, and trial-related issues on his blog for Fox Rothschild at http://whitecollarcrime.foxrothschild.com.

Scope of the Warrant And of the Ensuing Search and Seizure

The particularity requirement of the Fourth Amendment serves to prevent law enforcement officers from engaging in a prohibited general search of a given location for any evidence of any crime. *Marron v. United States,* 275 U.S. 192, 196 (1927) (particularity requirement ''makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another . . . nothing is left to the discretion of the officer executing the warrant''). A warrant meets the Fourth Amendment's particularity requirement if it identifies the items to be seized by relation to specific crimes and through descriptions sufficiently specific to leave nothing to the discretion of the searching officer. *Stanford v. Texas,* 379 U.S. 476, 485 (1965).

Even as to a traditional documents search, though, law enforcement agents enjoy some latitude to review, if briefly, a broad swath of materials that may be outside the scope of the warrant in order to make that determination. *See Andresen v. Maryland,* 427 U.S. 463, 482 n.11 (1976). The assumption underlying this relaxation of the particularity requirement is that some perusal of a document—its author and recipient, date, letterhead, or form—is reasonably necessary to compare the document against the specific description contained in the warrant to make an informed seize/do not seize judgment.

However, the immediate ability to grasp the sense of a document from glancing at its usual components is normally lacking in digital evidence searches; the names of computer files often yield no reliable information about their content or, worse, files are deliberately misnamed to conceal their content. Unless coded in some fashion, a letter addressed to the target of the investigation from ABC Corp. concerning a particular subject is just what it appears to be. The names of electronic folders and files do not so readily demonstrate their pertinence. File types (e.g., Adobe Acrobat, Word document, Excel spreadsheet) provide some information but are not sufficient guideposts. For example, in the case of a warrant authorizing the search for and seizure of records of drug transactions, a target could set forth an inculpatory schedule of deliveries in a conveniently labeled Excel document, but could as easily record the same information in a .pdf, .jpeg, Word, or other format that obscures the nature of the file's content.

The Third Circuit, in the recent case of *United States v. Stabile,* 2011 WL 294036, 88 CrL 562 (3d Cir., Feb. 1, 2011), recognized the problem of how to properly organize a computer search:

> On one hand, it is clear that because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad expansive search of the hard drive may be required. On the other hand . . . granting the Government a carte blanche to search *every* file on the hard drive impermissibly transforms a ''limited search into a general one.''

2011 WL 294036, at *13 (internal quotations and citations omitted) (emphasis in original).

   ISSN 0011-1341

In *Stabile*, a detective examined several computer media that had been seized by consent from the defendant's residence and removed for examination, looking for evidence of financial crimes, such as check counterfeiting. On one hard drive, the detective located a folder containing video files and opened 12 of them because the folder name suggested to him that they might contain child pornography, and his limited viewing of the files confirmed that they did; he purportedly stopped his search without viewing the detailed contents of the image files. *Id.* at *3. Seeking suppression of the evidence from those hard drives, the defendant argued that the seizure, even if properly consented to, was overbroad since the detective could and should have segregated possibly pertinent data at the residence, subject to later viewing if an appropriate child pornography search warrant was obtained.

The Third Circuit rejected the idea of compelling the government to conduct detailed on-site examinations of computer media, because the ''practical realities of computer investigations precluded'' the approach, given that such searches were time-consuming and required trained examiners. *Id.* at *8.

The problem of whether to require on-site preliminary examinations of computers before their wholesale seizure and the protocol for conducting examinations of electronic data has divided and vexed the courts of appeals, leading to conflicting answers to this problem:

(a) ***Ninth Circuit: most restrictive requirements for conducting searches.*** The case of *United States v. Comprehensive Drug Testing Inc.*, 621 F.3d 1162, 85 CrL 647 (9th Cir. 2010) (en banc), involved the BALCO-Barry Bonds steroids investigation. Agents had obtained a warrant to search computer records related to 10 named ballplayers in a specimen-collection laboratory. Drawing on pre-computer Ninth Circuit precedent, the magistrate judge conditioned the warrant to require non-case agents with computer training to conduct preliminary data reviews on-site to limit the removal of computer media, and then to require the speedy return of nonpertinent data that had been removed. Nevertheless, these restrictions were ignored in executing the warrant, and the lead case agent broadly reviewed all computer files and directories at the laboratory site, searching for the files affecting the 10 players. He reviewed the drug tests of hundreds of other ballplayers and later used that information to secure additional search warrants in other districts within the circuit, leading to the seizure of additional evidence involving many other ballplayers.

Three district court orders that either ordered a return of seized property or quashed a follow-on subpoena were consolidated for appeal, and a mixed decision from a Ninth Circuit panel was taken up by an en banc panel of the court. The en banc decision upheld the lower court orders and severely criticized the government. The court rejected the argument that agents could permissibly review entire hard drive directories thought to contain the narrower data eligible to be seized under a warrant, mocking the argument in a series of rhetorical questions: ''Why stop at the list of all baseball players when you can seize the entire [directory in which they were found]? Why just that directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the Zip disks under the bed in the room where the computer once might have been. . . . Let's take everything back to the lab, have a good look around and see what we might stumble upon.'' *Id.* at 1170-71.

Updating long-standing Ninth Circuit restrictions against search procedures that failed to adequately protect against the prospect of over-seizing documents, the *Comprehensive Drug Testing* opinion endorsed the imposition of a series of steps to be followed by the government in all computer searches. These steps include performing an on-site review and segregation of data by trained law enforcement personnel not involved in the investigation; employing narrowly designed search procedures to cull only the data encompassed by the warrant; and returning within 60 days any data later determined not to fall within the warrant. *Id.* at 1168-70 (drawing upon *United States v. Tamura,* 694 F.2d 591 (9th Cir. 1982)).

(b) ***Fourth Circuit: no requirements at all for conducting computer searches.*** In *United States v. Williams*, 592 F.3d 511, 86 CrL 507 (4th Cir.), *cert. den.*, 131 S. Ct. 595 (2010), the defendant argued that the warrant that led to the seizure of child pornographic images on computers and related electronic media was impermissibly general; it described the items to be seized broadly as those ''indicative'' of the Virginia crimes of communicating threats to injure or kill and of communicating obscene, vulgar, or lewd language. Acknowledging that the particulars of the warrant necessarily define the permissible scope of a search, the Fourth Circuit upheld the seizure as proper. In doing so, the court of appeals employed a very government-friendly formula to determine whether the seized items were within a warrant that made no mention of child pornography. The seizure was proper, the *Williams* court held, since the child pornography images were ''sufficiently relevant'' to the listed crimes because they somehow demonstrated the authorship of threatening and lewd e-mails sent from the computers. 592 F.3d at 520-21.

The court's opinion accepts as true, without any discussion, the evidentiary connection between saved child pornographic images and the sending of e-mails threatening sexual assaults upon children whose families attended a particular church. Curiously, social scientists and defense lawyers have exerted great effort to examine whether there is indeed any connection between a propensity to view certain images and the likelihood that the same viewer would act in the real world to harm actual children, but the *Williams* court expended no effort at all on this thorny question in upholding the search on the basis of an assumed linkage between the two.

The opinion contains no description of the search methodology employed by the examiner, apparently because the Fourth Circuit was unconcerned with limiting the methods by which computers are searched. ''[T]he warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization . . . . To be effective, such a search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance,'' the court said. 592 F.3d at 522.

(c) ***Third, Seventh, and Tenth Circuits: Addressing broadly the search steps to be followed, with much discretion left to searching agents.*** Between the two extremes is the view typified by the Tenth Circuit's decision in

Burgess. In that case, authorities executed a search warrant for evidence of drug sales and seized a laptop and two hard drives from the defendant's motor home. An agent searching for photos of drugs and drug proceeds on the media found child pornography while previewing image files; he then stopped and obtained a new warrant for child pornography. Burgess moved unsuccessfully to suppress evidence of the child pornography images, and the Tenth Circuit affirmed the denial of his motion. The court held that it was ''unrealistic'' to expect a warrant to narrow the scope of a search by filename or extension, since names could be altered, and that keyword searches directed against an entire hard drive might miss evidence, and so the search process must be ''dynamic.'' 576 F.3d at 1093-94.

Although it dismissed as ''folly'' efforts to impose a detailed search protocol such as that of the Ninth Circuit, the Tenth Circuit did set forth some functional limits on computer searches: The officer must first look in the most obvious places on the computer, starting with file structure, then look for suspicious file folders, and then look for files and types of files most likely to contain the objects of the search, using keyword searches. ''But in the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files. It is particularly true with image files,'' the court said. *Ibid*.

The Seventh Circuit also places itself in the middle of the road, constitutionally speaking. The defendant in *United States v. Mann*, 592 F.3d 779, 86 CrL 507 (7th Cir.), *cert. den.*, 130 S. Ct. 3525 (2010), was a lifeguard who had secretly videotaped swimmers changing in the locker room. A state warrant to search for computer media showing the locker room images led to the seizure of multiple computers. They were examined offsite using a forensic device that catalogs all image files by their names and file types and that alerts on any known to be child pornography. On one computer, the police examiner actually opened and viewed four image files that had drawn an automated alert and determined those and many other files to comprise child pornography, leading to the federal offense of conviction. *Id.* at 781.

The *Mann* court affirmed the denial of the defendant's suppression motion. First, the court addressed the practical difficulty of observing the warrant's limitation on searching only for images relating to the locker room. ''[S]uch images could be nearly anywhere on the computers [and] [u]nlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents.'' *Id.* at 782. The court held that the examiner did observe the strictures of the warrant, since he credibly claimed never to have abandoned his search for locker room images and since the search for image files led inexorably to ''stumbling upon'' the pornography. *Id*. at 783. Second, the Seventh Circuit noted but eschewed the Ninth Circuit's elaborate search protocol, preferring instead to ''simply counsel'' examiners to employ searches ''narrowly tailored to uncover only those things described.'' *Id.* at 786. The court said the officer's opening and viewing of the four suspect files was ''troubling'' and that he should have suspended the search until he obtained a warrant authorizing the search for child pornography but that the overall search was reasonable and within the warrant's scope. *Ibid.*

The Third Circuit in *Stabile* refrained from setting forth a search template for all circumstances. The court approved of an approach where the examining detective first identified a suspicious folder, called ''Kazvid,'' highlighted the folder to reveal the constituent file names, and then opened 12 of the files to ''confirm'' that they contained child pornography before ceasing his review under the original warrant. 2011 WL 294036, at *3. These steps illustrate a ''focused search of the hard drives rather than a general search,'' the Third Circuit said. *Id.* at *15.

Plain View

In the world of documents and other physical evidence, the concept of ''plain view'' has a readily cognizable meaning tied to the scope of a human being's field of vision or range of motion. If, for example, the searching agent is permissibly reviewing a cabinet of documents under the terms of a warrant but glances over and sees a package of suspected cocaine at a nearby desk, then the contraband may be seized in the absence of a drug warrant because it fell within plain view. Inside a computer's hard drive, there is no similar field of vision to exercise, so ''plain view'' is a more limited and circular concept; the agent must already have a permissible basis to be examining certain electronic files in order to plainly view their unlawful content and thereby to justify their ''plain view'' seizure. The breadth of a permissible plain-view search is thus tied to the notion of what is an initially permissible search procedure pursuant to the warrant; that is, if an agent searching for visual evidence of drug caches stored on a computer may examine every image file to find it, then any child pornography images that turn up in that broad examination will be determined to fall within the ''plain view'' doctrine.

The Fourth Circuit in *Williams* relied on plain view as an alternative basis on which to conclude that the seizure of child pornography images was lawful, even though the warrant was limited to computer files ''indicative'' of threatening and lewd communications. To do so, the court conflated the separate concepts of the reasonableness of the search under the Fourth Amendment and the plain-view exception to its warrant requirement:

> Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied.

592 F.3d at 522 (citations omitted). Thus, in the Fourth Circuit, once agents secure a warrant allowing them to search a computer, they may rummage through its contents, serene in the knowledge that any evidence they find they may keep.

The Ninth Circuit in *Comprehensive Drug Testing* was justifiably alarmed at this routine conflation of doctrinally separate ideas, recognizing the risk that the exception could swallow the rule:

> Once a file is examined, however, the government may claim (as it did in this case) that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search *some* computer

   ISSN 0011-1341

> files therefore automatically becomes authorization to search all files in the same subdirectory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media. Where computers are not near each other, but are connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there.

621 F.3d at 1176. Five judges concurring in the en banc decision made explicit that the very first element of the search procedure to be followed by law enforcement is the requirement that the government agree to waive any reliance on the plain-view doctrine in digital evidence cases. *Id.* at 1180.

Other courts of appeals have positioned themselves between the extremes of the Ninth and Fourth circuits' positions on the plain-view doctrine. The Seventh Circuit in *Mann* expressed a preference for allowing the doctrine to develop ''incrementally through the normal course of fact-based case adjudication.'' 592 F.3d at 785 (citation omitted). The Third Circuit likewise observed in *Stabile* that the ''exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner,'' *id.* at *16, citing *Mann* with approval and rejecting the Ninth Circuit's absolutist rejection of the doctrine. *Ibid.* & n.16.

Consent, or Is a Computer More Like a Duffel Bag or a Footlocker?

The Third Circuit in *Stabile* also considered whether the cohabiting girlfriend of a target of a counterfeit-check investigation had the authority to consent to the seizure of six hard drives, either removed from computers or simply strewn about, from their home. The woman, Debbie Deetz, was held to enjoy the authority to consent generally to the search of the shared home by agents whom she had invited in, since she used the home with the defendant and exercised joint access and control over it. 2011 WL 294036, at *7. But the question whether she had authority to consent to the computer seizure was ''complicated because computers often contain segregated blocks of information'' and ''multiple people may use the same computer and store information on the same hard drive.'' *Id.* at *8-9.

Compelled to resort to cases involving physical locations or storage devices, the Third Circuit pondered the conceptual question whether ''a computer [is] more like a shared duffel bag'' (citing *Frazier v. Cupp,* 394 U.S. 731, 740 (1969) (holding that a joint user of a duffel authorized any user to consent)) ''or more like a locked footlocker under the bed'' (citing *United States v. Block,* 590 F.2d 535 (4th Cir. 1978) (holding that parent could not consent to search of child's locked footlocker)). The *Stabile* court's answer to this metaphysical inquiry: It ''depends'' on issues such as the identity of the users; the presence or absence of password protection on the computer or as to certain directories; and the location of the computer, in that placing a computer in a bedroom connotes a greater expectation of privacy than if it were maintained in the basement. In *Stabile,* the absence of any passwords and the location of the computer media in common areas meant that Ms. Deetz had the requisite authority to consent.

Conclusion

These markedly contrasting approaches illustrate the degree to which confusion will reign until the Supreme Court speaks to the matter. The tension inherent in updating a right created more than two centuries ago is illustrated by the very different views expressed, respectively, by the Ninth and Fourth circuits on the hazards of digital evidence searches:

> We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data that it has no probable cause to collect.

Comprehensive Drug Testing, 621 F.3d at 1177.

> At bottom, we conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents. . . . We have applied these rules [counseling care generally in executing a warrant for the seizure of private papers] successfully in the context of warrants authorizing the search and seizure of non-electronic files . . . and we see no reason to depart from them in the context of electronic files.

Williams, 592 F.3d at 524 (internal quotation omitted).