H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director, OLE

Nathan Judish
Computer Crime and Intellectual Property Section

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

Computer Crime and
Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 741 (1979).

Chapter 2
Searching and Seizing Computers With a Warrant

A. Introduction

This Chapter discusses the legal and practical rules governing the use of warrants to search for and seize evidence stored in computers and electronic media. Section B discusses the strategic considerations any investigator or attorney should bear in mind before applying to the court for a warrant. Section C discusses the issues that arise in drafting a computer search warrant and affidavit. Section D addresses forensic analysis of the media. Section E discusses challenges to the search process. Finally, Section F discusses the limited circumstances in which statutes or other rules prohibit the government from using search warrants to obtain computers or electronic media. A sample computer search warrant appears in Appendix F.

B. Devising a Search Strategy

Before drafting a warrant application and affidavit, careful consideration should be given to what sort of evidence a search might reveal. A search of a computer's hard drive can reveal many different types of evidence. A search strategy should be chosen after considering the many possible roles of the computer in the offense:

> 1) A computer can be *contraband*—either because the computer is a repository of data that is contraband (such as child pornography) or because the computer is stolen property;
>
> 2) a computer can be a repository of data that is *evidence of a crime*—such as a spreadsheet showing illegal drug transactions, a letter used in an ongoing fraud, or log files showing IP addresses assigned to the computer and websites accessed; or

3) a computer can be an *instrumentality of a crime*—for example, the computer was used as a tool to hack into websites, distribute copyrighted videos, or produce illegal pornography.

Additionally, in devising a search strategy, investigators should bear in mind both the elements that must be proven should the prosecution go to trial and also the sources of electronic evidence that are relevant to those elements.

The typical computer user thinks of the contents of a hard drive in terms of what the computer's user interface chooses to reveal: files, folders, and applications, all neatly arranged and self-contained. This, however, is merely an abstraction presented to make the computer easier to use. That abstraction hides the evidence of computer usage that modern operating systems leave on hard drives. As computers run, they leave evidence on the hard drive—considerably more evidence than just the files visible to users. Remnants of whole or partially deleted files can still remain on the drive. Portions of files that were edited away also might remain. "Metadata" and other artifacts left by the computer can reveal information about what files have recently been accessed, when a file was created and edited, and sometimes even how it was edited. Virtual memory paging systems can leave traces of information on the hard drive that the user might have believed were stored only in volatile computer memory such as RAM and expected to disappear when the computer was shut down. Browsers, mail readers, chat clients, and other programs leave behind configuration files that might reveal online nicknames and passwords. Operating systems and applications record additional information on the hard drive, such as records of Internet usage, the attachment of peripherals and flash drives, and the times the computer was in use. Collectively, this information can reveal to an investigator not just what a computer happens to contain at the time of the search, but also evidence of who has used a computer, when, and how.

Obviously, discovering contraband or substantive evidence of a crime on the hard drive will be a frequent goal of a computer search. However, investigators should consider other goals that a computer search might meet. Consider the following examples:

1) It may be necessary to prove that a particular individual put contraband on the hard drive, rather than someone else with access to the computer. This might be shown through evidence that a particular user was logged on, or by evidence

that the computer was used shortly after the offense to check the individual's bank account or email account.

2) It may be necessary to satisfy the investigator that a virus or other piece of malware was not responsible for the offense. Often, an investigator can establish this by running a simple virus-checking program on an image of the hard drive.

3) It may be necessary to show that a defendant had knowledge of some particular subject. Web browsing history, for example, might reveal that an individual was researching how to build a methamphetamine laboratory.

A prosecutor or investigator should carefully consider the appropriate goals in drafting the warrant so as to ensure that sufficient evidence may be collected pursuant to the warrant.

C. Drafting the Affidavit, Application, and Warrant

An affidavit and application for a warrant to search a computer are in most respects the same as any other search warrant affidavit and application: the affiant swears to facts that establish that there is probable cause to believe that evidence of crime (such as records), contraband, fruits of crime, or instrumentalities of crime is present in a private space (such as a computer's hard drive, or other media, which in turn may be in another private space, such as a home or office), and the warrant describes with particularity the things (records and other data, or perhaps the computer itself) to be searched and seized. The process of drafting an affidavit and application, then, falls into two general steps: establishing probable cause to search the computer, and describing with particularity the data to be taken from the computer or the computer hardware itself.

1. Include Facts Establishing Probable Cause

The probable cause necessary to search a computer or electronic media is probable cause to believe that the media *contains* or *is* contraband, evidence of a crime, fruits of crime, or an instrumentality of a crime. *See* Fed. R. Crim. P. 41(c). Evidence of crime can include evidence of ownership and control. *See, e.g.*, *United States v. Horn*, 187 F.3d 781, 787-88 (8th Cir. 1999) (approving in child pornography case a warrant provision authorizing seizure of "[r]ecords, documents, receipts, keys, or other objects showing access to, and control of,

the residence"). According to the Supreme Court, the probable cause standard is satisfied by an affidavit that establishes "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). This requires a practical, common-sense determination of the probabilities, based on a totality of the circumstances. *See id.* Of course, probable cause will not exist if the agent can only point to a "bare suspicion" that criminal evidence will be found in the place searched. *See Brinegar v. United States*, 338 U.S. 160, 175 (1949). Once a magistrate judge finds probable cause and issues the warrant, the magistrate's determination that probable cause existed is entitled to "great deference," *Gates*, 462 U.S. at 236, and will be upheld so long as there is a "substantial basis for concluding that probable cause existed." *Id.* at 238-39 (internal quotations omitted).

Often, no special facts in the affidavit are necessary to establish probable cause to search a computer. As a general rule, "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately; the individual's interest in privacy must give way to the magistrate's official determination of probable cause." *United States v. Ross*, 456 U.S. 798, 823 (1982). Thus, if a warrant authorizes a search of a premises (for example, a doctor's office) for a particularized list of records (for example, false Medicare bills), then the warrant should authorize agents to search a computer they encounter on the premises if they reasonably believe the warrant describes records that might be stored on that computer. *See, e.g.*, *United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008) (agents were justified in searching a computer "where there was ample evidence that the documents authorized in the warrant could be found" on that computer); *United States v. Rogers*, 521 F.3d 5, 9-10 (1st Cir. 2008) (holding that "videotape is a plausible repository for a photo," such that a warrant authorizing seizure of "photos of DW" allowed seizure and review of videotape for such photos). In such a case, it is necessary to establish probable cause to believe that the records will be found on the premises, but it is no more necessary to establish that a computer or other electronic storage media will be found there than it is necessary to establish that file cabinets, piles of paper, or other record storage systems will be found there. In short, the probable cause requirement should not require agents to be clairvoyant in their knowledge of the precise forms of evidence or contraband that will exist in the location to be searched. *See United States v. Reyes*, 798 F.2d 380, 382 (10th Cir. 1986) (noting that "in the age of modern technology . . . , the warrant could not be expected to describe with exactitude the precise forms the records would take").

However, in *United States v. Payton*, ___ F.3d ___, 2009 WL 2151348 (9th Cir. July 21, 2009), the Ninth Circuit held that law enforcement is not necessarily entitled to examine a computer that may contain evidence that falls within the scope of a warrant. *See id.* at * 3. In *Payton*, an officer executing a search warrant that authorized a seizure of drug sales records and other financial records searched a computer capable of storing such records. The court held that because the warrant did not specifically authorize a search of the computer, and because nothing else present at the scene of the search suggested that records falling within the scope of the warrant would be found on the computer, the search violated the Fourth Amendment. *See id.* Under *Payton*, it is good policy for prosecutors and agents seeking a warrant in the Ninth Circuit to always seek specific authorization to search computers, though failure to do so will not necessarily invalidate the search.

Probable cause will look different in every case, but in the computer search context a few common scenarios have emerged. They are discussed below.

a. Probable Cause Established Through an Internet Protocol Address

In a common computer search scenario, investigators learn of online criminal conduct. Using records obtained from a victim or from a service provider, investigators determine the Internet Protocol ("IP") address used to commit the crime. Using a subpoena or other process discussed in Chapter 3, investigators then compel the Internet Service Provider ("ISP") that has control over that IP address to identify which of its customers was assigned that IP address at the relevant time, and to provide (if known) the user's name, street address, and other identifying information. In some cases, investigators confirm that the person named by the ISP actually resides at that the street address by, for example, conducting a mail cover or checking utility bills.

Affidavits that describe such an investigation are typically sufficient to establish probable cause, and the probable cause is strengthened if the affidavit corroborates with some additional facts the association of an IP address with a physical address. *See, e.g.*, *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) (probable cause established through IP address used to access child pornography and ISP records of physical address); *United States v. Grant*, 218 F.3d 72, 76 (1st Cir. 2000) (evidence that an Internet account belonging to the defendant was involved in criminal activity on several occasions, and that the defendant's car was parked at his residence during at least one such occasion, created probable cause to search the defendant's residence); *United States v.*

Carter, 549 F. Supp. 2d 1257, 1261 (D. Nev. 2008) (probable cause established through IP address, ISP records, and utility records); *United States v. Hanson*, 2007 WL 4287716, at *8 (D. Me. Dec. 5, 2007) (finding probable cause based on IP address and physical address despite "no direct knowledge whether any computer hardware . . . was physically located at the" residence); *United States v. Huitt*, 2007 WL 2355782, at *4 (D. Idaho Aug. 17, 2007) (probable cause established through IP address and separate email address both linked to same physical location).

Defendants sometimes will argue that the mere association of an IP address with a physical address is insufficient to establish probable cause because it is technologically possible for individuals not residing at that address to use the defendant's Internet connection. Most often, this argument takes the form of a defendant arguing that he has, or could have had, an open wireless Internet connection, which would have allowed any nearby person with commonly available equipment to use the defendant's Internet connection and IP address. Courts have consistently rejected this argument because the probable cause standard for warrants requires only a fair probability that evidence or contraband will be found. *See, e.g.*, *Perez*, 484 F.3d at 740 (probable cause standard met by the association of an IP address with a physical address despite defendant's argument that he could have had an "unsecure wireless connection" allowing others to use his IP address); *Carter*, 549 F. Supp. 2d at 1267-69 (rejecting argument that affidavit for search warrant should have mentioned the possibility of an open wireless connection); *United States v. Latham*, 2007 WL 4563459, at *11 (D. Nev. Dec. 18, 2007) (finding probable cause even though "[i]t was possible that someone other than Larry Latham or a resident of his household had accessed the internet either through his wireless router or by 'spoofing' his address in order to engage in the exchange of child pornography"). Indeed, this argument is particularly weak because the wireless access point itself will typically contain evidence within the scope of the warrant. For similar reasons, courts have rejected challenges to a finding of probable cause based on the failure of an affidavit to rule out "hacking, 'spoofing', tampering, theft, destruction, or viral infections by others." *United States v. Hibble*, 2006 WL 2620349, at *4 (D. Ariz. Sept. 11, 2006) (citing *United States v. Gourde*, 440 F.3d 1065, 1073 n.5 (9th Cir. 2006) (en banc)). As the Fifth Circuit explained, "though it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained likely that the source of the transmissions was inside that residence." *Perez*, 484 F.3d at 740. Alternative explanations "are

more suited to being raised as a defense at trial." *Hibble*, 2006 WL 2620349, at *4.

b. Probable Cause Established Through Online Account Information

In another scenario, a defendant establishes an account with an online service—such as a Web-based email service or a pornography site—and the credit card information or contact information associated with that account is used to identify the defendant and support probable cause to search computer media in the defendant's home. For example, in *United States v. Kelley*, 482 F.3d 1047, 1053 (9th Cir. 2007), an affidavit established probable cause through the real name and physical address associated with several America Online "screen names" used to receive child pornography. Similarly, in *United States v. Terry*, 522 F.3d 645, 648 (6th Cir. 2008), probable cause to search a home was established by demonstrating that an AOL email account was used to send child pornography, that the account's owner lived in that home, and that the account's owner had a computer in that home that he had used to send email through that account in the past. *See also United States v. Wilder*, 526 F.3d 1, 6 (1st Cir. 2008) ("it was a fair inference from his subscription to the Lust Gallery website, as described in the affidavit, that downloading and preservation in his home of images of child pornography might very well follow").

Frequently, this scenario arises when investigators have discovered a child pornography website or email group and have successfully obtained its membership list. In *United States v. Gourde*, 440 F.3d 1065, 1070-71 (9th Cir. 2006) (en banc), the affidavit established probable cause through the defendant's membership in a known child pornography website, without independent evidence such as an IP address. Several other courts have also held that it is reasonable to infer from a defendant's voluntary membership in a child pornography website or "e-group" (a hybrid of an email discussion list and web forum) that the defendant downloaded or kept child pornography, although many of these courts pointed to corroborating evidence as well. *See, e.g.*, *United States v. Wagers*, 452 F.3d 534, 539-40 (6th Cir. 2006); *United States v. Shields*, 458 F.3d 269, 279 (3d Cir. 2006) (membership in on-line child pornography Yahoo group, combined with "suggestive" email address of "LittleLolitaLove" supported probable cause); *United States v. Martin*, 426 F.3d 68, 77 (2d Cir. 2005) ("those who view are likely to download and store child pornography"); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004) (considering factors of joining a group, remaining a member for a month, and using screen names "that reflect his interest in child pornography").

Not all courts, however, have agreed that membership alone supports probable cause. In *United States v. Coreas*, 419 F.3d 151 (2d Cir. 2005), a Second Circuit panel sharply disagreed with the panel in *Martin*. *Coreas* involved an affidavit that, after false accusations were excised, contained "[s]imply" the allegation that the defendant, "by clicking a button, responded affirmatively to a three-sentence invitation … to join [a child pornography] e-group." *Coreas*, 419 F.3d at 156. The court held that this allegation "does not remotely satisfy Fourth Amendment standards" because "a 'person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.'" *Id*. (quoting *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979)). Similarly, in *United States v. Falso*, 544 F.3d 110, 121 (2d Cir. 2008), the Second Circuit held that there was no substantial basis for probable cause in a warrant that alleged only that it "appear[ed]" that the defendant "gained access or attempted to gain access" to a child pornography site.

c. Probable Cause Established Through Off-Line Conduct

In some cases, the defendant's name and address are known through traditional investigative techniques, and agents wish to search the individual's computer for evidence related to the crime. These cases are no different from any other computer search case: the objective of the affidavit is to establish "a fair probability that contraband or evidence of a crime would be found in computers at" the place to be searched. *United States v. Adjani,* 452 F.3d 1140, 1145 (9th Cir. 2006) (internal quotation marks and brackets omitted). For example, in *United States v. Khanani,* 502 F.3d 1281, 1290 (11th Cir. 2007), the court found probable cause to search an accountant's computer because the affidavit identified him as accountant for an employer of illegal aliens, stated that a tax return for that employer was found in the trash outside the office, and stated that an agent saw computers inside the office. *See also United States v. Flanders,* 468 F.3d 269, 271 (5th Cir. 2006) (probable cause to search a computer supported by defendant's "past sexual abuse of his daughter, coupled with his decision to take a digital photograph of that child naked").

d. Staleness

Defendants often claim that the facts alleged in the warrant affidavit were too stale to establish probable cause at the time the warrant was issued. Most such challenges have occurred in child pornography cases, and the courts have generally found little merit in these arguments: "When a defendant is suspected

of possessing child pornography, the staleness determination is unique because it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes." *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006) (internal quotations marks omitted); *see also United States v. Paull*, 551 F.3d 516, 522 (6th Cir. 2009) ("because the crime is generally carried out in the secrecy of the home and over a long period, the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography"); *United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007) (crediting affidavit saying that child pornographers "keep and collect items containing child pornography over long periods of time"); *United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) ("[i]nformation a year old is not necessarily stale as a matter of law, especially where child pornography is concerned"); *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005) (five-year old information that defendant sought to convert a Polaroid photograph to a digital format was not stale); *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000); *United States v. Horn*, 187 F.3d 781, 786-87 (8th Cir. 1999); *United States v. Lacy*, 119 F.3d 742, 745-46 (9th Cir. 1997). Courts have also noted that advances in computer forensic analysis allow investigators to recover files even after they are deleted, casting greater doubt on the validity of "staleness" arguments. *See Hay*, 231 F.3d at 636; *United States v. Cox*, 190 F. Supp. 2d 330, 334 (N.D.N.Y. 2002). *But see United States v. Doan*, 2007 WL 2247657, at *3 (7th Cir. Aug. 6, 2007) (seventeen-month-old information, combined with a lack of information about "the duration of the website subscriptions, the download capability accompanying those subscriptions, the last date Doan accessed the websites, whether Doan downloaded images from these sites, whether Doan owned a computer, or whether Doan had internet access at his home" insufficient to establish probable cause); *United States v. Zimmerman*, 277 F.3d 426, 433-34 (3d Cir. 2002) (distinguishing retention of adult pornography from retention of child pornography and holding that evidence that adult pornography had been on computer at least six months before a warrant was issued was stale); *United States v. Frechette*, 2008 WL 4287818, at *4 (W.D. Mich. Sept. 17, 2008) (sixteen-month-old information stale in a child pornography case).

2. Describe With Particularity the Things to be Seized

a. The Particularity Requirement

The Fourth Amendment requires that every warrant "particularly describ[e]" two things: "the place to be searched" and "the persons or things

to be seized." U.S. Const. Amend. IV; *see United States v. Grubbs,* 547 U.S. 90, 97 (2006). Describing with particularity the "things to be seized" has two distinct elements. *See United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999). First, the warrant must describe the things to be seized with sufficiently precise language so that it tells the officers how to separate the items properly subject to seizure from irrelevant items. *See Marron v. United States*, 275 U.S. 192, 296 (1927) ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); *Davis v. Gracey*, 111 F.3d 1472, 1478 (10th Cir. 1997). Second, the description of the things to be seized should be limited to the scope of the probable cause established in the warrant. *See In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853, 857 (9th Cir. 1997). Considered together, the elements forbid agents from obtaining "general warrants" and instead require agents to conduct narrow seizures that attempt to "minimize[] unwarranted intrusions upon privacy." *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).

b. Seizing Hardware vs. Seizing Information

The most important decision agents must make when describing the property in the warrant is whether the seizable property is the computer *hardware* or merely the *information* that the hardware contains. If computer hardware is contraband, evidence, fruits, or instrumentalities of crime, the warrant should describe the hardware itself. If the probable cause relates only to information, however, the warrant should describe the information to be seized, and then request the authority to seize the information in whatever form it may be stored (whether electronic or not).

c. Hardware seizures

Depending on the nature of the crime being investigated, computer hardware might itself be contraband, an instrumentality of a crime, or fruits of crime and therefore may be physically seized under Rule 41. For example, a computer that stores child pornography is itself contraband. *See United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) (upholding seizure of entire computer as contraband in child pornography case). A computer may also be used as an instrumentality of crime, as when it is used to commit a hacking offense or send threats. *See, e.g.*, *United States v. Adjani,* 452 F.3d 1140, 1145-46 (9th Cir. 2006) (computer used to send extortive threat is instrumentality); *Davis v. Gracey,* 111 F.3d 1472, 1480 (10th Cir. 1997) (computer used to operate bulletin board distributing obscene materials is instrumentality); *United States*

v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (computer used to send or receive child pornography is instrumentality). Although it could be argued that any computer that is used to store evidence of crime is an instrumentality, the reasoning in *Davis* suggests that in order for a computer to qualify as an instrumentality, more substantial use of the computer in the crime is necessary. *See Davis*, 111 F.3d at 1480 (stating that "the computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime").

If the computer hardware is itself contraband, an instrumentality of crime, or fruits of crime, the warrant should describe the hardware and indicate that the hardware will be seized. In most cases investigators will simply seize the hardware during the search, and then search through the defendant's computer for the contraband files back at a computer forensics laboratory. In such cases, the agents should explain clearly in the supporting affidavit that they plan to search the computer for evidence and/or contraband after the computer has been seized and removed from the site of the search. Courts have generally held that descriptions of hardware can satisfy the particularity requirement so long as the subsequent searches of the seized computer hardware appear reasonably likely to yield evidence of crime; in many of these cases, the computers contain child pornography and are thus contraband. *See, e.g.*, *United States v. Hay*, 231 F.3d 630, 634 (9th Cir. 2000) (upholding seizure of "computer hardware" in search for materials containing child pornography); *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir. 2000) (upholding seizure of "computer equipment which may be, or is used to visually depict child pornography," and noting that the affidavit accompanying the warrant explained why it would be necessary to seize the hardware and search it off-site for the images it contained); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (upholding seizure of "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in a child pornography case because "[a]s 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 [sought after] images"); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (warrant permitting "blanket seizure" of computer equipment from defendant's apartment not insufficiently particular when there was probable cause to believe that computer would contain evidence of child pornography offenses); *United States v. Henson*, 848 F.2d 1374, 1382-83 (6th Cir. 1988) (permitting seizure of "computer[s], computer terminals, . . . cables, printers, discs, floppy discs, [and] tapes" that could hold evidence of the defendants' odometer-tampering scheme because such language "is directed toward items

likely to provide information concerning the [defendants'] involvement in the . . . scheme and therefore did not authorize the officers to seize more than what was reasonable under the circumstances"); *United States v. Albert*, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (upholding warrant for seizure of computer and all related software and storage devices where such an expansive search was "the only practical way" to obtain images of child pornography).

d. Information seizures

☞ When electronic storage media are to be searched because they store information that is evidence of crime, the items to be seized under the warrant should usually focus on the content of the relevant files rather than the physical storage media.

Many investigations seek to search computers for evidence of a crime only; the computer might contain business records relevant to a white-collar prosecution, for example, but the computer itself does not store contraband and was not used to commit the crime. The computer is "evidence" only to the extent that some of the data it stores is evidence. *See United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008) ("Computers, like briefcases and cassette tapes, can be repositories for documents and records.").

When probable cause to search relates in whole or in part to information stored on the computer, rather than to the computer itself, the warrant should identify that information with particularity, focusing on the content of the relevant files rather than on the storage devices which may happen to contain them. *See, e.g.*, *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (stating that the ability of a computer to store "a huge array" of information "makes the particularity requirement that much more important"); *United States v. Vilar,* 2007 WL 1075041, at *36 (S.D.N.Y. Apr. 4, 2007) ("underlying information must be identified with particularity and its seizure independently supported by probable cause"); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (stating that a warrant to seize evidence stored on a computer should specify "which type of files are sought"); *United States v. Gawrysiak*, 972 F. Supp. 853, 860 (D.N.J. 1997), *aff'd*, 178 F.3d 1281 (3d Cir. 1999) (upholding seizure of "records [that] include information and/or data stored in the form of magnetic or electronic coding on computer media . . . which constitute evidence" of enumerated federal crimes). In cases where the computer is merely a storage device for evidence, failure to focus on the relevant files may lead to a Fourth Amendment violation. For example, in *United States v.*

Riccardi, 405 F.3d 852, 862 (10th Cir. 2005), which involved an investigation into harassing phone calls, the court held that a warrant authorizing seizure of all storage media and "not limited to any particular files" violated the Fourth Amendment.

Agents should be particularly careful when seeking authority to seize a broad class of information. This sometimes occurs when agents plan to search computers at a business. *See, e.g.*, *United States v. Leary*, 846 F.2d 592, 600-04 (10th Cir. 1988). Agents cannot simply request permission to seize "all records" from an operating business unless agents have probable cause to believe that the criminal activity under investigation pervades the entire business. *See United States v. Ford*, 184 F.3d 566, 576 (6th Cir. 1999) (citing cases); *In re Grand Jury Investigation Concerning Solid State Devices*, *Inc.*, 130 F.3d 853, 857 (9th Cir. 1997). A similarly dangerous phrase, "any and all data, including but not limited to" a list of items, has been held to turn a computer search warrant into an unconstitutional general warrant. *United States v. Fleet Management Ltd.*, 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007); *see also Otero*, 563 F.3d at 1132 (warrant authorizing seizure of "any and all information and/or data" fails the particularity requirement).

Instead, the description of the files to be seized should be limited. One successful technique has been to identify records that relate to a particular crime and to include specific categories of the types of records likely to be found. For example, the Ninth Circuit upheld such a warrant that limited the search for evidence of a specific (and specified) crime. *See United States v. Adjani*, 452 F.3d 1140, 1148 (9th Cir. 2006). It is sometimes helpful to also specify the target of the investigation (if known) and the time frame of the records involved (if known). *See, e.g.*, *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (invalidating warrant for failure to name crime or limit seizure to documents authored during time frame under investigation); *Ford*, 184 F.3d at 576 ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad."); *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (concluding that warrant to seize "[a]ll computers" was not sufficiently particular where description "did not indicate the specific crimes for which the equipment was sought, nor were the supporting affidavits or the limits contained in the searching instructions incorporated by reference.").

Thus, one effective approach is to begin with an "all records" description; add limiting language stating the crime, the suspects, and relevant time period

if applicable; include explicit examples of the records to be seized; and then indicate that the records may be seized in any form, whether electronic or non-electronic. For example, when drafting a warrant to search a computer at a business for evidence of a drug trafficking crime, agents might describe the property to be seized in the following way:

> All records relating to violations of 21 U.S.C. § 841(a) (drug trafficking) and/or 21 U.S.C. § 846 (conspiracy to traffic drugs) involving [the suspect] since January 1, 2008, including lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information); any information recording [the suspect's] schedule or travel from 2008 to the present; all bank records, checks, credit card bills, account information, and other financial records.
>
> The terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

Mentioning that records might appear in electronic form is helpful for agents and lawyers who read the warrant. However, the courts have generally permitted agents to seize computer equipment when agents reasonably believe that the content described in the warrant may be stored there, regardless of whether the warrant states expressly that the information may be stored in electronic form. *See, e.g.*, *United States v. Giberson*, 527 F.3d 882, 888 (9th Cir. 2008) ("[t]he format of a record or document should not be dispositive to a Fourth Amendment inquiry"); *United States v. Pontefract*, 2008 WL 4461850, at *3 (W.D. La. Oct. 1, 2008) (warrant that specified photographs but not computers allowed the search of a computer for photographs because "in today's digital world, a laptop computer is as likely a place to find photographs as a photo album"). As the Tenth Circuit explained in *United States v. Reyes*,

798 F.2d 380, 383 (10th Cir. 1986), "in the age of modern technology and commercial availability of various forms of items, the warrant c[an] not be expected to describe with exactitude the precise form the records would take." Accordingly, what matters is the substance of the evidence, not its form, and the courts will defer to an executing agent's reasonable construction of what property must be seized to obtain the evidence described in the warrant. *See United States v. Hill*, 19 F.3d 984, 987-89 (5th Cir. 1994); *Hessel v. O'Hearn*, 977 F.2d 299 (7th Cir. 1992); *United States v. Word*, 806 F.2d 658, 661 (6th Cir. 1986); *United States v. Gomez-Soto*, 723 F.2d 649, 655 (9th Cir. 1984) ("The failure of the warrant to anticipate the precise container in which the material sought might be found is not fatal."). *See also United States v. Abbell*, 963 F. Supp. 1178, 1997 (S.D. Fla. 1997) (noting that agents may legitimately seize "[a] document which is implicitly within the scope of the warrant – even if it is not specifically identified"). This approach is consistent with a forthcoming amendment to Rule 41(e) (which, assuming no contrary congressional action, is scheduled to take effect on December 1, 2009) specifying that a "warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information."

Of course, agents do not need to follow this approach in every case; judicial review of search warrants is "commonsensical" and "practical," rather than "overly technical." *United States v. Ventresca,* 380 U.S. 102, 108 (1965). When agents cannot know the precise form that records will take before the search occurs, a generic description must suffice. *See United States v. Logan*, 250 F.3d 350, 365 (6th Cir. 2001) (approving a broadly worded warrant and noting that "the warrant's general nature" was appropriate in light of the investigation's circumstances); *Davis v. Gracey*, 111 F.3d 1472, 1478 (10th Cir. 1997) ("Even 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 activity under investigation permit.") (internal quotations omitted); *United States v. Lacy*, 119 F.3d 742, 746-47 (9th Cir. 1997) (holding that the general description of computer equipment to be seized was sufficient as there was "no way to specify what hardware and software had to be seized to retrieve the images accurately"); *United States v. London,* 66 F.3d 1227, 1238 (1st Cir. 1995) (noting that where the defendant "operated a complex criminal enterprise where he mingled 'innocent' documents with apparently-innocent documents which, in fact, memorialized illegal transactions, ... [it] would have been difficult for the magistrate judge to be more limiting in phrasing the warrant's language, and for the executing officers to have been more discerning

in determining what to seize."); *United States v. Scharfman*, 448 F.2d 1352, 1354-55 (2d Cir. 1971); *Gawrysiak*, 972 F. Supp. at 861. Warrants sometimes authorize seizure of all records relating to a particular criminal offense. *See London*, 66 F.3d at 1238 (upholding search for "books and records . . . and any other documents . . . which reflect unlawful gambling"); *United States v. Riley*, 906 F.2d 841, 844-45 (2d Cir. 1990) (upholding seizure of "items that constitute evidence of the offenses of conspiracy to distribute controlled substances"); *United States v. Wayne*, 903 F.2d 1188, 1195 (8th Cir. 1990) (upholding search for "documents and materials which may be associated with . . . contraband [narcotics]"). Even an "all records" search may be appropriate in certain circumstances. *See also United States v. Hargus*, 128 F.3d 1358, 1362-63 (10th Cir. 1997) (upholding seizure of "any and all records relating to the business" under investigation for mail fraud and money laundering); *United States v. Lamb*, 945 F. Supp. 441, 458-59 (N.D.N.Y. 1996) (not insufficiently particular to ask for "[a]ll stored files" in AOL network account when searching account for obscene pornography, because as a practical matter all files need to be reviewed to determine which files contain the pornography).

3. Establishing the Necessity for Imaging and Off-Site Examination

☞ With limited exceptions, a search of a hard drive or other media requires too much time to conduct on-site during the execution of a warrant. The search warrant affidavit should explain why it is necessary to image an entire hard drive (or physically seize it) and later examine it for responsive records.

Examining a computer for evidence of crime is nearly always a time consuming process. Even if the agents know specific information about the files they seek, the data may be mislabeled, encrypted, stored in hidden directories, or embedded in "slack space" that a simple file listing will ignore. *See United States v. Hill*, 322 F. Supp. 2d 1081, 1089-90 (C.D. Cal. 2004) (Kozinski, J.), *aff'd* 459 F.3d 966 (9th Cir. 2006); *United States v. Gray,* 78 F. Supp. 2d 524, 530 (E.D. Va. 1999) (noting that agents executing a search for computer files "are not required to accept as accurate any file name or suffix and [to] limit [their] search accordingly," because criminals may "intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories."). Moreover, evidence of a crime will not always take the form of a file. It may be in a log, operating system artifact, or other piece of recorded data that can be difficult to locate and retrieve without the appropriate tools and time.

It may take days or weeks to find the specific information described in the warrant because computer storage devices can contain extraordinary amounts of information. *See United States v. Hill,* 459 F.3d 966, 974-75 (9th Cir. 2006) ("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.").

Because examining a computer for evidence of crime is so time consuming, it will be infeasible in almost every case to do an on-site search of a computer or other storage media for evidence of crime. Agents cannot reasonably be expected to spend more than a few hours searching for evidence on-site, and in some circumstances (such as executing a search at a suspect's home) an extended search may be unreasonable. *See United States v. Santarelli,* 778 F.2d 609, 615-16 (11th Cir. 1985). In cases involving large quantities of paper documents, courts traditionally have allowed investigators to remove the documents to an off-site location to review the documents to determine which documents fall within the scope of the warrant. *See Santarelli*, 778 F.2d at 616; *United States v. Hargus,* 128 F.3d 1358, 1363 (10th Cir. 1997) (upholding seizure of an entire file cabinet when such seizure was motivated by the impracticability of on-site sorting); *United States v. Tamura,* 694 F.2d 591, 595-96 (9th Cir. 1982).

For similar reasons, courts have approved removal of computers to an off-site location for review. *See United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (the "narrowest definable search and seizure reasonably likely to obtain" the evidence described in a warrant is, in most instances, "the seizure and subsequent off-premises search of the computer and all available disks"); *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) (seizure of entire computer reasonable because affidavit "justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis"); *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) ("[b]ecause of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files"); *cf. United States v. Giberson*, 527 F.3d 882, 886 (9th Cir. 2008) (holding that a warrant that "clearly limited the types of documents and records that were seizable" permitted the seizure of an entire computer); *United States v. Grimmett*, 439 F.3d 1263, 1269 (10th Cir. 2006) ("we have adopted a somewhat forgiving stance when faced with a 'particularity' challenge to a warrant authorizing the seizure of computers"). Moreover, attempting to search storage media on-site may even risk damaging the evidence itself in some cases. Modern operating

systems continually read from and write to the hard disk, changing some of the information recorded there; thus, the simple act of using a computer might alter the evidence recorded on the hard drive. Internet-connected computers are additionally vulnerable, because someone at a remote location might be able to access the computer and delete data while investigators are examining it on-site. Thus, the best strategy will generally be to review storage media off-site where forensic examiners can ensure the integrity of the data.

In many cases, rather than seize an entire computer for off-site review, agents can instead create a digital copy of the hard drive that is identical to the original in every relevant respect. This copy is called an "image copy"—a copy that "duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." *United States v. Vilar,* 2007 WL 1075041, *35 n.22 (S.D.N.Y. Apr. 4, 2007), quoting Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L. Rev. 531 (2005); *see also United States v. Stierhoff,* 477 F. Supp. 2d 423, 439 & n.8 (D.R.I. 2007). An image copy cannot be created by simply dragging and dropping icons or running conventional backup programs; the process of making one usually involves opening the computer case and connecting the investigator's own hardware directly to the hard drive. In some cases, investigators will make the image copy on-site; in others, investigators will seize the computer hardware from the premises and make the image copy off-site.

To justify the possible imaging and/or removal for off-site review of a computer or other storage media, the Ninth Circuit requires the affidavit to explain why practical constraints might require the seizure of the entire computer system for off-site examination. *See United States v. Hill,* 459 F.3d 966, 975-76 (9th Cir. 2006) (stating that the affidavit must "demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand"). As imaging and/or removal is necessary in nearly every computer search warrant case, it is doubtful that failure to include such a statement in the affidavit constitutes a Fourth Amendment violation. Nevertheless, although explicitly required only by the Ninth Circuit, it is a good practice for every search warrant affidavit to explain why it is necessary to image an entire hard drive (or physically seize it) and later examine it for responsive records. Including these facts in the affidavit provides a considerable degree of reassurance that the Fourth Amendment will be satisfied. *See United States v. Hill*, 459 F.3d 966, 976 (9th Cir. 2006); *United States v. Hay*, 231

F.3d 630, 637 (9th Cir. 2000) ("the affidavit explained why it was necessary to seize the entire computer system" and "justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis"); *United States v. Adjani*, 452 F.3d 1140, 1149 n.7 (9th Cir. 2006). As noted below, these facts justifying removal of storage media for off-site review should *not* commit the agents to any particular "protocol" for reviewing the media to find evidence that falls within the scope of the warrant. Instead, the affidavit will simply note that off-site review might be required.

4. Do Not Place Limitations on the Forensic Techniques That May Be Used To Search

Limitations on search methodologies have the potential to seriously impair the government's ability to uncover electronic evidence. "[A] search can be as much an art as a science," *United States v. Brooks*, 427 F.3d 1246, 1252 (10th Cir. 2005), and the forensic process can require detective work, including intuition and on-the-spot judgment in deciding, based on what the examiner has just seen, what is the best step to take next. One particularly burdensome restriction that could be placed on a forensic investigator is the requirement that the investigator limit the search to files containing particular keywords. Forensic analysis may include keyword searches, but a properly performed forensic analysis will rarely end there, because keyword searches will fail to find many kinds of files that fall within the scope of a warrant. For example, at the time of this writing, a number of file types, such as TIFF files and some PDF files, cannot be searched for keywords. *See, e.g.*, *United States v. Evanson*, 2007 WL 4299191, at *5 (D. Utah Dec. 5, 2007) (noting that in the search at issue some files "were in 'tiff' format," a "'digital picture of a hard copy document' that has been scanned," and that these files "had numbers as file names, rather than recognizable file names that purportedly described the data in the files"). In addition, keyword searches can also be thwarted through the use of code words or even unintentional misspellings. Law and investment firms—not to mention individuals involved in criminal activity—often use code words to identify entities, individuals, and specific business arrangements in documents and communications; sometimes the significance of such terms will not be apparent until after a careful file-by-file review has commenced. Every Westlaw or LEXIS user is familiar with the difficulty of crafting search terms that find the correct case on the first try; requiring a forensic investigator to find crucial evidence with a keyword search specified prior to forensic analysis is just as impractical.

Court-mandated forensic protocols are also unnecessary because investigators already operate under significant constitutional restrictions. As with any search, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979); *United States v. Ramirez*, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis … governs the method of execution of the warrant."); *Hill*, 459 F.3d at 978 ("reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials remains subject to judicial review"). Unreasonable conduct can be remedied after the fact, including, as a "last resort," with suppression of evidence. *Hudson v. Michigan*, 547 U.S. 586, 591 (2006).

A few magistrate judges issue warrants to search computers only subject to limitations on the way that the seized media may later be examined. For example, some magistrates require that the forensic analysis of the computer be completed within a set time period; issues related to the timing of forensic analysis are discussed in Section D.5 below. In addition, some magistrates may refuse to sign a warrant that does not include a protocol specifying how the government will examine seized media to find evidence that falls within the scope of the warrant. *See, e.g.*, *In re Search of 3817 W. West End,* 321 F. Supp. 2d 953, 962-63 (N.D. Ill. 2004). Neither Rule 41 nor the Fourth Amendment requires magistrates to impose such restrictions, and prosecutors should oppose such restrictions whenever they significantly interfere with the government's ability to obtain evidence that falls within the scope of the warrant. While it might be helpful for the affidavit to contain background information that might justify particular steps taken during the search—such as describing the ease with which evidence can be concealed in a computer, explaining the need to search off-site, or justifying the seizure of commingled records—neither the search warrant application nor the affidavit need contain special restrictions on how agents search for the things described in the warrant.

Any significant limitation (such as a restriction to keyword searches) on the techniques the government may use to find evidence that falls within the scope of a warrant is inconsistent with Supreme Court precedent. The Supreme Court has held that "[n]othing in the language of the Constitution or in [the Supreme Court's] decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they

are to be executed." *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (quoting *Dalia*, 441 U.S. at 255). "It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth 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." *Dalia*, 441 U.S. at 258. Furthermore, any limitation on the government's ability to find evidence that falls within the scope of a warrant is inconsistent with the rule that "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately; the individual's interest in privacy must give way to the magistrate's official determination of probable cause." *United States v. Ross*, 456 U.S. 798, 823 (1982).

Magistrates requiring the government to set forth a protocol for forensic analysis have typically cited the Supreme Court's decision in *Andresen v. Maryland*, 427 U.S. 463 (1976), in which the Court noted that when search warrants authorize the seizure of documents, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Id.* at 482 n.11. Under *Andresen*, it is surely appropriate for magistrates to strictly enforce the Particularity Clause in computer cases involving commingled records. However, nothing in *Andresen* authorizes magistrates to control the manner in which a warrant is *executed*, and such control was rejected by the Court in *Dalia* and *Grubbs*. In addition, the *Andresen* Court recognized that it is necessary to look at "innocuous documents . . . in order to determine whether they are, in fact, among those papers authorized to be seized." *Andresen*, 427 U.S. at 482 n.11.

Circuit courts have upheld computer search warrants that included neither a protocol (a list of steps the investigator is required to undertake in examining the computer) nor an explanation for the lack of a protocol. In *United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008), the court upheld a seizure of a computer and a search through it for particularly described records, even though the records were intermingled with other files, without requiring any protocol. The court held that "the potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's reasonableness requirement." *Id.* at 889. In *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006), the defendant challenged the search of his computer, arguing, among other things, that the warrant was invalid because "it did not include a search protocol to limit the officer's discretion as to what they could examine when searching the defendant's computer media."

Id. at 977. The court held that no search protocol was necessary, and that it also was not necessary to explain the absence of a search protocol in the warrant application. *Id.* at 978. The Tenth Circuit emphasized in *United States v. Brooks*, 427 F.3d 1246 (10th Cir. 2005), that while warrants must describe "with particularity the objects of their search," the methodology used to find those objects need not be described: "This court has never required warrants to contain a particularized computer search strategy." *Id.* at 1251. In *United States v. Khanani*, 502 F.3d 1281, 1290-91 (11th Cir. 2007), the Eleventh Circuit rejected the argument that a warrant should have included a search protocol, pointing in part to the careful steps agents took to ensure compliance with the warrant. *See also United States v. Cartier*, 543 F.3d 442, 447-48 (8th Cir. 2008) ("While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se"); *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) ("The warrant process is primarily concerned with identifying what may be searched or seized—not how"). *But see United States v. Payton*, ___ F.3d ___, 2009 WL 2151348, at *3-5 (9th Cir. July 21, 2009) (holding that search of computer without explicit authorization violated Fourth Amendment where nothing present at the residence searched suggested that records falling within the scope of the warrant would be found on the computer, and suggesting in dicta that judges issuing computer search warrants "may place conditions on the manner and extent of such searches").

If a search strategy is described in the affidavit, the affidavit should clearly state that the strategy is an illustration of a likely strategy that will be employed, but not "a specification of the precise manner in which [the warrant is] to be executed." *Grubbs*, 547 U.S. at 98. Indeed, one court has held that "search protocols and keywords are not 'material' for purposes of Rule 16(a)(1)(E)," and thus are not discoverable. *United States v. Fumo*, 2007 WL 3232112, at *7 (E.D. Pa. Oct. 30, 2007).

Finally, if a magistrate judge refuses to issue a warrant without conditioning its execution on certain requirements, and if law enforcement officials choose to execute the warrant anyway, the officials should not ignore the requirements. *See, e.g.*, *United States v. Brunette*, 76 F. Supp. 2d 30, 42 (D. Maine 1999), *aff'd*, 256 F.3d 14 (1st Cir. 2001) (suppression appropriate because the government failed to comply with time limits for reviewing seized computers when those time limits were required by the warrant). Instead, law enforcement officials

should follow the requirements of the warrant unless they obtain relief from the issuing magistrate or an appropriate higher court. Prosecutors encountering such issues should contact CCIPS at (202) 514-1026 for further assistance.

5. Seeking Authorization for Delayed Notification Search Warrants

If certain conditions are met, a court may authorize so-called "surreptitious entry" or "sneak-and-peek" warrants that excuse agents from having to notify at the time of the search the person whose premises are searched. Neither the Fourth Amendment nor Rule 41 requires an officer executing a search warrant to present the property owner with a copy of the warrant before conducting his search. *United States v. Grubbs,* 547 U.S. 90, 98-99 (2006). In addition, under 18 U.S.C. § 3103a, a court may grant the delay of notice associated with the execution of a search warrant if it finds "reasonable cause" to believe that providing immediate notification of the execution of the warrant may have one of the adverse effects enumerated in 18 U.S.C. § 2705 (except for unduly delaying a trial): endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation.

Under § 3103a, law enforcement authorities must provide delayed notice within a "reasonable period not to exceed 30 days after the date of [the warrant's] execution" or, alternatively, "on a later date certain if the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(b)(3). This initial period can be extended "for good cause" upon "an updated showing of the need for further delay;" such extensions are "limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(c).

Section 3103a distinguishes between delaying notice of a *search* and delaying notice of a *seizure*. Indeed, unless the court finds "reasonable necessity" for a seizure, warrants issued under this section must prohibit the seizure of any tangible property, any wire or electronic communication, or any stored wire or electronic information (except as expressly provided in chapter 121). Congress intended that if investigators intended to make surreptitious copies of information stored on a suspect's computer, they would obtain authorization from the court in advance. For more information regarding section 3103a, prosecutors and investigators should contact the Office of Enforcement Operations ("OEO") at (202) 514-6809.

6. Multiple Warrants in Network Searches

☞ Agents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations.

Fed. R. Crim. P. 41(a) states that a magistrate judge located in one judicial district may issue a search warrant for "a search of property . . . within the district," or "a search of property . . . outside the district if the property . . . is within the district when the warrant is sought but might move outside the district before the warrant is executed." Rule 41 defines "property" to include "information," *see* Fed. R. Crim. P. 41(a)(2)(A), and the Supreme Court has held that "property" as described in Rule 41 includes intangible property such as computer data. *See United States v. New York Tel. Co.*, 434 U.S. 159, 170 (1977). Although the courts have not directly addressed the matter, the language of Rule 41 combined with the Supreme Court's interpretation of "property" may limit searches of computer data to data that resides in the district in which the warrant was issued. *Cf. United States v. Walters*, 558 F. Supp. 726, 730 (D. Md. 1980) (suggesting such a limit in a case involving telephone records).

A territorial limit on searches of computer data poses problems for law enforcement because computer data stored in a computer network can be located anywhere in the world. For example, agents searching an office in Manhattan pursuant to a warrant from the Southern District of New York may sit down at a terminal and access information stored remotely on a computer located in New Jersey, California, or even a foreign country. A single file described by the warrant could be located anywhere on the planet, or could be divided up into several locations in different districts or countries. Even worse, it may be impossible for agents to know when they execute their search whether the data they are seizing has been stored within the district or outside of the district. Agents may in some cases be able to learn where the data is located before the search, but in others they will be unable to know the storage site of the data until after the search has been completed.

When agents can learn prior to the search that some or all of the data described by the warrant is stored in a different location than where the agents will execute the search, the best course of action depends upon where the remotely stored data is located. When the data is stored remotely in two or more different places within the United States and its territories, agents should obtain additional warrants for each location where the data resides to ensure

compliance with a strict reading of Rule 41(a). For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts.

When agents learn before a search that some or all of the data is stored remotely outside of the United States, matters become more complicated. The United States may be required to take actions ranging from informal notice to a formal request for assistance to the country concerned. Further, some countries may object to attempts by U.S. law enforcement to access computers located within their borders. Although the search may seem domestic to a U.S. law enforcement officer executing the search in the United States pursuant to a valid warrant, other countries may view matters differently. Agents and prosecutors should contact the Office of International Affairs at (202) 514-0000 for assistance with these difficult questions.

When agents do not and even cannot know that data searched from one district is actually located outside the district, evidence seized remotely from another district ordinarily should not lead to suppression of the evidence obtained. The reasons for this are twofold. First, courts may conclude that agents sitting in one district who search a computer in that district and unintentionally cause intangible information to be sent from a second district into the first have complied with Rule 41(a). *Cf. United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir. 1997) (Posner, C.J.) (adopting a permissive construction of the territoriality provisions of Title III); *United States v. Denman*, 100 F.3d 399, 402 (5th Cir. 1996) (same); *United States v. Rodriguez*, 968 F.2d 130, 135-36 (2d Cir. 1992) (same).

Second, even if courts conclude that the search violates Rule 41(a), the violation will not lead to suppression of the evidence unless the agents intentionally and deliberately disregarded the Rule, or the violation leads to "prejudice" in the sense that the search might not have occurred or would not have been so "abrasive" if the Rule had been followed. *See United States v. Burke*, 517 F.2d 377, 386 (2d Cir. 1975) (Friendly, J.); *United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988) (citing cases); *cf. Herring v. United States*, 129 S. Ct. 695, 702 (2009) (exclusionary rule is applied in Fourth Amendment cases only if police conduct is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system"). Under the widely-adopted *Burke* test, courts generally deny motions to suppress when agents executing the search cannot know whether it violates Rule 41 either legally or factually. *See Martinez-Zayas*, 857 F.2d at 136

(concluding that a search passed the *Burke* test "[g]iven the uncertain state of the law" concerning whether the conduct violated Rule 41(a)). Accordingly, evidence acquired from a network search that accessed data stored in multiple districts should not lead to suppression unless the agents intentionally and deliberately disregarded Rule 41(a) or prejudice resulted. *See generally United States v. Trost*, 152 F.3d 715, 722 (7th Cir. 1998) ("[I]t is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression.").

D. Forensic Analysis

1. The Two-Stage Search

In the vast majority of cases, forensic analysis of a hard drive (or other computer media) takes too long to perform on-site during the initial execution of a search warrant. Thus, as discussed in Section C.3 above, investigators generally must remove storage media for off-site analysis to determine the information that falls within the scope of the warrant. This process has two steps: *imaging*, in which the entire hard drive is copied, and *analysis,* in which the copy of the hard drive is culled for records that are responsive to the warrant.

Imaging is described in Section C.3 above. It results in the creation of an "image copy" of the hard drive—a copy that "duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." *United States v. Vilar,* 2007 WL 1075041, at *35 n.22 (S.D.N.Y. Apr. 4, 2007), quoting Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L. Rev. 531 (2005).

After imaging, the second step of the forensic review process begins: the hard drive image is examined, and data that falls within the scope of the warrant is identified. In computer search cases, where the purpose for the off-site analysis is to determine whether information stored on computer media falls within the scope of a warrant, courts have treated the off-site forensic analysis of computer media seized pursuant to a warrant as a continuation of the search, still bound by the Fourth Amendment. *See United States v. Syphers*, 426 F.3d 461, 468 (1st Cir. 2005) (referring to a forensic review of a seized computer as a "search"); *United States v. Mutschelknaus*, 564 F. Supp. 2d 1072, 1076 (D.N.D. 2008) (referring to forensic analysis as a "subsequent search");

United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002) (referring to an examination of a hard drive image as a "search").

Once a computer seized pursuant to a warrant has been reviewed and items within the computer determined to fall within the scope of the warrant, subsequent review of those items should not implicate the Fourth Amendment. As the Ninth Circuit has explained, "once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant." *United States v. Turner*, 28 F.3d 981, 983 (9th Cir. 1994) (quoting *United States v. Burnette*, 698 F.2d 1038, 1049 (1983)).

2. Searching Among Commingled Records

Few computers are dedicated to a single purpose; rather, computers can perform many functions, such as "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more." *United States v. Andrus,* 483 F.3d 711, 718 (10th Cir. 2007). Thus, almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation. The Fourth Amendment governs how investigators may search among the commingled records to isolate those records that are called for by the warrant.

The Supreme Court has noted that in a search of commingled records, "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." *Andresen v. Maryland,* 427 U.S. 463, 482 n.11 (1976). Therefore, "responsible officials, including judicial officials, must take care to assure that [these searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Id.*

Following on the acknowledgement in *Andresen* that "innocuous" documents can be "cursorily" examined, courts have set forth guidelines for agents review of commingled records to find documents that fall within the scope of a warrant. The leading case is *United States v. Heldt*, which allows a "brief perusal" of each document, and requires that "the perusal must cease at the point of which the warrant's inapplicability to each document is clear." *United States v. Heldt*, 668 F.2d 1238, 1267 (D.C. Cir. 1982); *see also United States v. Rude*, 88 F.3d 1538, 1552 (9th Cir. 1996); *United States v. Giannetta*, 909 F.2d 571, 577 (1st Cir. 1990) ("the police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the

documentary items to be seized"); *United States v. Slocum*, 708 F.2d 587, 604 (11th Cir. 1983); *United States v. Ochs*, 595 F.2d 1247, 1258 (2d. Cir. 1979) ("some perusal, generally fairly brief."). If a document falls outside the warrant but nonetheless is incriminating, *Heldt* allows that document's "seizure" only if during that brief perusal the document's "otherwise incriminating character becomes obvious." *Heldt*, 668 F.2d at 1267.

Similar reasoning has been applied to computer searches. *See United States v. Khanani*, 502 F.3d 1281, 1290 (11th Cir. 2007) (endorsing a search in which "a computer examiner eliminated files that were unlikely to contain material within the warrants' scope"); *Manno v. Christie*, 2008 WL 4058016, at *4 (D.N.J. Aug. 22, 2008) (finding it "reasonable for [Agent] to briefly review each electronic document to determine if it is among the materials authorized by the warrant, just as he could if the search was only of paper files"); *United States v. Potts*, 559 F. Supp. 2d 1162, 1175-76 (D. Kan. 2008) (warrant did not authorize an overbroad search when it allowed the investigator "to search the computer by . . . opening or cursorily reviewing the first few 'pages' of such files in order to determine the precise content" (internal quotation marks removed)); *United States v. Fumo*, 2007 WL 3232112, at *6 (E.D. Pa. Oct. 30, 2007) ("search protocols and keywords do not mark the outer bounds of a lawful search; to the contrary, because of the nature of computer files, the government may legally open and briefly examine each file when searching a computer pursuant to a valid warrant"); *United States v. Scarfo*, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) (in holding that a key stroke logger could be used to obtain a passphrase even though it would capture other keystrokes, noting that "law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant"). When it becomes necessary for an investigator to personally examine a computer file to determine whether it falls within the scope of the warrant, the investigator should take all necessary steps to analyze the file thoroughly, but the investigator should cease the examination of that file as soon as it becomes clear that the warrant does not apply to that file.

Some older cases appear to suggest that when agents executing a search encounter commingled records, they should seize the records, and then seek additional approval from the magistrate before proceeding. For example, the Ninth Circuit, writing about a search of paper files in an age before computer searches were common, suggested that in the "comparatively rare instances"

where "documents are so intermingled that they cannot feasibly be sorted on site," law enforcement "can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search." *United States v. Tamura,* 694 F.2d 591, 595-596 (9th Cir. 1982). The Tenth Circuit suggested in dicta that the same procedure might be followed for computer searches. *See United States v. Carey,* 172 F.3d 1268, 1275 (10th Cir. 1999) ("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"). Both courts, however, have subsequently clarified that a procedure in which the initial warrant establishes the criteria for off-site review is sufficient. *See United States v. Hay,* 231 F.3d 630, 637 (9th Cir. 2000) (affidavit that establishes "why it was necessary to seize the entire computer system" and "justified taking the entire system off site," with magistrate approval, "makes inapposite *United States v. Tamura*"); *United States v. Brooks,* 427 F.3d 1246, 1251 (10th Cir. 2005) ("we have not required a specific prior authorization along the lines suggested in *Carey* in every computer search").

3. Analysis Using Forensic Software

☞ Provided the forensic examiner is attempting to find data that is responsive to the warrant, the Fourth Amendment does not limit the techniques an examiner may use to examine a hard drive.

"[A] computer search may be as extensive as reasonably required to locate the items described in the warrant." *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006). So long as the forensic examiner is attempting to find data that is responsive to the warrant, the Fourth Amendment does not restrain the techniques an examiner uses. The use of forensic software, no matter how "sophisticated," also does not affect Fourth Amendment analysis. *Cf. United States v. Long*, 425 F.3d 482, 487 (7th Cir. 2005) (noting in consent search case that "it is impossible to search computer hardware or software without using some type of software," and "[t]he fact that the Encase search engine [is] sophisticated is of no importance.").

Even if a defendant has taken steps to conceal evidence on a hard drive, a forensic review that nonetheless uncovers it does not invade a reasonable expectation of privacy so long as the warrant permitted a search of the hard drive for that evidence. For example, reading the contents of deleted files by examining unallocated space on the disk has been upheld. *See United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) ("recovery [by law enforcement of

unlawful images] after attempted destruction, is no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note").

4. Changes of Focus and the Need for New Warrants

A single computer can be involved in several types of crimes, so a computer hard drive might contain evidence of several different crimes. When an agent searches a computer under the authority of a warrant, however, the warrant will often authorize a search of the computer only for evidence of certain specified crimes. If the agent comes across evidence of a crime that is not identified by the warrant, it may be a safe practice to obtain a second warrant. In *United States v. Carey,* 172 F.3d 1268 (10th Cir. 1999), detectives obtained a warrant to search the defendant's computer for records of narcotics sales. Searching the computer back at the police station, a detective discovered images of child pornography. At that point, the detective "abandoned the search for drug-related evidence" and instead searched the entire hard drive for evidence of child pornography. *Id.* at 1277-78. The Tenth Circuit suppressed the child pornography, holding that the subsequent search for child pornography exceeded the scope of the original warrant. *See id.* at 1276. *Compare Carey with United States v. Walser*, 275 F.3d 981, 986-87 (10th Cir. 2001) (upholding search where officer with warrant to search for electronic records of drug transactions discovered child pornography on computer, suspended search, and then returned to magistrate for second warrant to search for child pornography), *and Gray*, 78 F. Supp. 2d at 530-31 (upholding search where agent discovered child pornography in the course of looking for evidence of computer hacking pursuant to a warrant, and then obtained a second warrant before searching the computer for child pornography).

The Tenth Circuit has subsequently characterized *Carey* as "simply stand[ing] for the proposition that law enforcement may not expand the scope of a search beyond its original justification." *United States v. Grimmett*, 439 F.3d 1263, 1268 (10th Cir. 2006). *Grimmett*, then, shifts the analysis away from the agent's subjective intent and toward what the warrant justified. Notably, *Carey*'s focus on the agent's subjective intent reflects a somewhat outdated view of the Fourth Amendment. The Supreme Court has declined to examine an agent's subjective intent and instead has focused on whether the circumstances, viewed objectively, justified the agent's conduct. *See, e.g.*, *Brigham City v. Stuart*, 547 U.S. 398, 404 (2006) ("An action is 'reasonable' under the Fourth Amendment, regardless of the individual officer's state of mind, as long as the

circumstances, viewed objectively, justify the action.") (internal quotation marks removed); *Whren v. United States*, 517 U.S. 806, 813 (1996); *Horton v. California*, 496 U.S. 128, 138 (1990). Relying on these precedents, several courts have indicated that an agent's subjective intent during the execution of a warrant no longer determines whether the search exceeded the scope of the warrant and violated the Fourth Amendment. *See United States v. Van Dreel*, 155 F.3d 902, 905 (7th Cir. 1998) ("[U]nder *Whren*, . . . once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search is irrelevant."); *United States v. Ewain*, 88 F.3d 689, 694 (9th Cir. 1996) ("Using a subjective criterion would be inconsistent with *Horton*, and would make suppression depend too much on how the police tell their story, rather than on what they did."). According to these cases, the proper inquiry is whether, from an objective perspective, the search that the agents actually conducted was consistent with the warrant obtained. *See Ewain*, 88 F.3d at 694. The agent's subjective intent is either "irrelevant," *Van Dreel*, 155 F.3d at 905, or else merely one factor in the overall determination of "whether the police confined their search to what was permitted by the search warrant." *Ewain*, 88 F.3d at 694.

Under an objective standard for agents' conduct, there is inherent tension between *Carey* and cases such as *Hill*, 322 F. Supp. 2d at 1090, which recognized that "[t]here is no way to know what is in a file without examining its contents." This fact, combined with the principle that "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately," *United States v. Ross*, 456 U.S. 798, 823 (1982), suggests that it should not be necessary to seek a second warrant after discovering evidence of a separate crime. As the court explained in *Gray*, 78 F. Supp. 2d at 531 n.11, "[a]rguably, [the agent] could have continued his systematic search of defendant's computer files pursuant to the first search warrant, and, as long as he was searching for the items listed in the warrant, any child pornography discovered in the course of that search could have been seized under the 'plain view' doctrine." Nevertheless, *Carey* has not been overruled, so it remains prudent to seek a second warrant upon discovering evidence of an additional crime not identified in the initial warrant.

5. Permissible Time Period for Examining Seized Media

Neither the Fourth Amendment nor Rule 41 imposes any specific limitation on the time period of the government's forensic examination. The government ordinarily may retain the seized computer and examine its contents in a careful

and deliberate manner, subject only to the reasonableness requirement of the Fourth Amendment, and the reasonableness of the government's search is determined primarily by whether probable cause for the search has dissipated. The absence of a specific time frame for forensic examination is confirmed by a new amendment to Rule 41(e), which is scheduled to take effect (assuming no contrary congressional action) on December 1, 2009:

> A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Courts have agreed that neither the Fourth Amendment nor Rule 41 places explicit limits on the duration of any of forensic analysis, and courts have upheld forensic analyses begun months after investigators acquire a computer or data. *See United States v. Burns*, 2008 WL 4542990, at *8-9 (N.D. Ill. Apr. 29, 2008) (ten month delay); *United States v. Gorrell*, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (ten month delay); *United States v. Hernandez*, 183 F. 3d 468, 480 (D.P.R. 2002) (six week delay); *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 66 (D. Conn. 2002); *cf. United States v. New York Tel. Co.*, 434 U.S. 159, 169 n.16 (1977) (applying Fourth Amendment standards to pen registers before the enactment of the pen register act, holding that "the requirement … that the search be conducted within 10 days of its issuance does not mean that the duration of a pen register surveillance may not exceed 10 days").

The Fourth Amendment does require that forensic analysis of a computer be conducted within a reasonable time. *See United States v. Mutschelknaus*, 564 F. Supp. 2d 1072, 1077 (D.N.D. 2008) ("[T]he Federal Rules of Criminal Procedure do not require that the forensic analysis of computers and other electronic equipment take place within a specific time limit. Any subsequent search only needs to be conducted within a reasonable time."); *Burns*, 2008 WL 4542990, at *8 ("A delay must be reasonable, but there is no constitutional upper limit on reasonableness."); *United States v. Grimmett*, 2004 WL 3171788, at *5 (D. Kan. Aug. 10, 2004), *aff'd* 439 F.3d 1263 (10th Cir. 2006). In judging the reasonableness of time for forensic analysis, courts may recognize that

analysis of computers is a difficult and time-consuming process. *See Triumph Capital Group, Inc.*, 211 F.R.D. at 66 (finding that time to complete search reasonable because "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution").

Importantly, courts usually treat the dissipation of probable cause as the chief measure of the "reasonableness" of a search's length under the Fourth Amendment. For example, in *United States v. Syphers*, 426 F.3d 461 (1st Cir. 2005), the First Circuit stated that the Fourth Amendment "contains no requirements about *when* the search or seizure is to occur or the *duration*," but cautioned that "unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant." *Id.* at 469 (quotations omitted). *See Burns*, 2008 WL 4542990 at *9 (upholding search despite "lengthy" delay because "Burns does not assert that the time lapse affected the probable cause to search the computer (nor could he, given that suspected child pornography had already been found on the hard drive), that the government has acted in bad faith, or that he has been prejudiced in any way by the delay"). Significantly, dissipation of probable cause is unlikely in computer search cases because evidence is "frozen in time" when storage media is imaged or seized. *Triumph Capital Group, Inc.*, 211 F.R.D. at 66.

A few magistrate judges have taken a different view, however, and have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, such as thirty days. Some magistrate judges have imposed time limits as short as seven days, and several have imposed specific time limits when agents apply for a warrant to seize computers from operating businesses. In support of these limitations, a few magistrate judges have expressed their concern that it might be constitutionally "unreasonable" under the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time.[1]

Prosecutors should oppose such limitations. The law does not expressly authorize magistrate judges to issue warrants that impose time limits on law enforcement's examination of seized evidence, and the authority of magistrates

[1] When the computer does not contain contraband (such as child pornography), this specific concern can usually be addressed by imaging the computer, returning it promptly, and later taking as much time as necessary to conduct the forensic exam on the image copy.

to impose such limits is open to question, especially in light of the forthcoming amendment to Rule 41 stating that the time for executing a warrant "refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." As the Supreme Court suggested in one early case, the proper course is for the magistrate to issue the warrant so long as probable cause exists, and then to permit the parties to litigate the constitutional issues afterwards. *See Ex Parte United States*, 287 U.S. 241, 250 (1932) ("The refusal of the trial court to issue a warrant . . . is, in reality and effect, a refusal to permit the case to come to a hearing upon either questions of law or fact, and falls little short of a refusal to permit the enforcement of the law."). Prosecutors encountering this issue may contact CCIPS at (202) 514-1026 for further assistance.

At least one court has adopted the severe position that suppression is appropriate when the government fails to comply with court-imposed limits on the time period for reviewing seized computers. In *United States v. Brunette,* 76 F. Supp. 2d 30 (D. Me. 1999), a magistrate judge permitted agents to seize the computers of a child pornography suspect on the condition that the agents searched through the computers for evidence "within 30 days." The agents executed the search five days later and seized several computers. A few days before the thirty-day period elapsed, the government applied for and obtained a thirty-day extension of the time for review. The agents then reviewed all but one of the seized computers within the thirty-day extension period, and found hundreds of images of child pornography. However, the agents did not begin reviewing the last of the computers until two days after the extension period had elapsed. The defendant moved for suppression of the child pornography images found in the last computer, on the ground that the search outside of the sixty-day period violated the terms of the warrant and subsequent extension order. The court agreed, stating that "because the Government failed to adhere to the requirements of the search warrant and subsequent order, any evidence gathered from the . . . computer is suppressed." *Id.* at 42.

The result in *Brunette* makes little sense either under Rule 41 or the Fourth Amendment. Even assuming that a magistrate judge has the authority to impose time constraints on forensic testing in the first place, it seems incongruous to impose suppression for violations of such conditions when analogous violations of Rule 41 itself would not result in suppression. *Compare Brunette* with *United States v. Twenty-Two Thousand, Two Hundred Eighty Seven Dollars ($22,287.00), U.S. Currency*, 709 F.2d 442, 448 (6th Cir. 1983) (rejecting suppression when

agents began search "shortly after" 10 p.m., even though Rule 41 states that all searches must be conducted between 6:00 a.m. and 10 p.m.). Similarly, the Fourth Amendment requires only reasonableness, and courts have rejected challenges based on claims of delay, as discussed above. This incongruity is especially true when the hardware to be searched is a container of contraband child pornography, and it is therefore subject to forfeiture and will not be returned.

The use of the exclusionary rule to police delays by forensic examiners is even more questionable after *Hudson v. Michigan,* 547 U.S. 586 (2006). In *Hudson*, in which the Supreme Court rejected a suppression remedy for violation of the knock-and-announce rule, the Court held that "but-for causality is only a necessary, not a sufficient, condition for suppression." *Id.* at 592. In rejecting suppression, the Court also relied on the conclusion that suppression would not "vindicate the interests protected by the [constitutional] requirement [at issue]," *id.* at 593, and that "the exclusionary rule has never been applied" when its "substantial social costs" outweigh its deterrent benefits. *Id.* (citation omitted).

6. Contents of Rule 41(f) Inventory Filed With the Court

☞ Officers should file inventories with returns that simply indicate the hardware devices that were seized.

Rule 41(f) requires an officer executing a warrant to "prepare and verify an inventory of any property seized," and to "return [the warrant]—together with a copy of the inventory—to the magistrate judge designated on the warrant," Fed. R. Crim. P. 41(f)(1)(B), (D). Currently, "[t]he Rules do not dictate a requisite level of specificity for inventories of seized items," and whether an inventory is sufficiently specific is a question of fact. *In re Searches of Semtex Indus. Corp.*, 876 F. Supp. 426, 429 (E.D.N.Y. 1995). When documents are seized, an inventory listing each of them is not required; such "specificity and particularization would not seem to be called for even under an extreme construction of Rule 41" in light of its requirement that an inventory be "promptly" filed with the magistrate. *United States v. Birrell*, 269 F. Supp. 716, 722 (S.D.N.Y. 1967).

Thus, in computer cases, officers have typically filed inventories with returns that simply indicate the information or hardware devices that were seized, such as "image of one Maxtor 500 gigabyte hard drive." This approach has been

adopted in a new amendment to Rule 41(f), which is scheduled to take effect (assuming no contrary congressional action) on December 1, 2009. The new rule specifies that "[i]n a case involving the seizure of electronic storage media or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied."

Courts have also held that when the government seizes documents or data, providing defendants with "a copy of everything seized" has been held to "obviate[] the need for a detailed inventory." *United States v. Triumph Capital Group, Inc.,* 211 F.R.D. 31, 66 (D. Conn. 2002); *United States v. Ogden,* 2008 WL 2247074, at *13 (W.D. Tenn. May 28, 2008) (rejecting suppression motion based on failure to provide a timely inventory of a computer search "[b]ecause the Defendant has had access to the seized files, has personal knowledge of the files, and was recently given a list of the files"). Providing defendants with "access" to paper records seized from an office also "obviates the need for a more detailed inventory" beyond one that simply identifies which file cabinets were seized. *Semtex,* 876 F. Supp. at 429-30.

E. Challenges to the Search Process

1. Challenges Based on "Flagrant Disregard"

Defense counsel will sometimes attempt to use the seizure of storage media or commingled information as the basis for a motion to suppress all of the evidence obtained in a search. To be entitled to the extreme remedy of blanket suppression, the defendant must establish that the seizure of additional materials proves that the agents executed the warrant in "flagrant disregard" of its terms. *See, e.g.*, *United States v. Khanani*, 502 F.3d 1281, 1289 (11th Cir. 2007); *United States v. Le*, 173 F.3d 1258, 1269 (10th Cir. 1999); *United States v. Matias*, 836 F.2d 744, 747-48 (2d Cir. 1988) (citing cases). A search is executed in "flagrant disregard" of its terms when the officers so grossly exceed the scope of the warrant during execution that the authorized search appears to be merely a pretext for a "fishing expedition" through the target's private property. *See, e.g.*, *United States v. Liu*, 239 F.3d 138 (2d Cir. 2000); *United States v. Foster*, 100 F.3d 846, 851 (10th Cir. 1996); *United States v. Young*, 877 F.2d 1099, 1105-06 (1st Cir. 1989).

As discussed above in Section C.3, for practical and technical reasons, agents executing computer searches frequently must seize hardware or files beyond those described in the warrant. Defense lawyers sometimes argue that by

seizing more than the specific computer files named in the warrant, the agents "flagrantly disregarded" the seizure authority granted by the warrant. *See, e.g.*, *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988); *United States v. Hunter*, 13 F. Supp. 2d 574, 585 (D. Vt. 1998); *United States v. Gawrysiak*, 972 F. Supp. 853, 865 (D.N.J. 1997), *aff'd*, 178 F.3d 1281 (3d Cir. 1999); *United States v. Schwimmer*, 692 F. Supp. 119, 127 (E.D.N.Y. 1988).

Prosecutors can best respond to "flagrant disregard" motions by showing that any seizure of property not named in the warrant resulted from a good faith response to inherent practical difficulties, rather than an attempt to conduct a general search of the defendant's property under the guise of a narrow warrant. The courts have recognized the practical difficulties that agents face in conducting computer searches for specific files, and they routinely approve off-site searches despite the incidental seizure of additional property. *See, e.g.*, *United States v. Hill*, 459 F.3d 966, 974-75 (9th Cir. 2006) ("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"); *Davis v. Gracey*, 111 F.3d 1472, 1280 (10th Cir. 1997) (noting "the obvious difficulties attendant in separating the contents of electronic storage [sought as evidence] from the computer hardware [seized] during the course of a search"); *United States v. Schandl*, 947 F.2d 462, 465-466 (11th Cir. 1991) (noting that an on-site search "might have been far more disruptive" than the off-site search conducted); *Henson*, 848 F.2d at 1383-84 ("We do not think it is reasonable to have required the officers to sift through the large mass of documents and computer files found in the [defendant's] office, in an effort to segregate those few papers that were outside the warrant."); *United States v. Scott-Emuakpor*, 2000 WL 288443, at *7 (W.D. Mich. Jan. 25, 2000) (noting "the specific problems associated with conducting a search for computerized records" that justify an off-site search); *Gawrysiak*, 972 F. Supp. at 866 ("The Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant."); *United States v. Sissler*, 1991 WL 239000, at *4 (W.D. Mich. Jan. 25, 1991) ("The police . . . were not obligated to inspect the computer and disks at the . . . residence because passwords and other security devices are often used to protect the information stored in them. Obviously, the police were permitted to remove them from the . . . residence so that a computer expert could attempt to 'crack' these security measures, a process that takes some time and effort. Like the seizure of documents, the seizure of the computer hardware and software was

motivated by considerations of practicality. Therefore, the alleged carte blanche seizure of them was not a 'flagrant disregard' for the limitations of a search warrant."). *See also United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) ("It is no easy task to search a well-laden hard drive by going through all of the information it contains . . . . The record shows that the mechanics of the search for images later performed [off-site] could not readily have been done on the spot."); *United States v. Lamb*, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) ("[I]f some of the image files are stored on the internal hard drive of the computer, removing the computer to an FBI office or lab is likely to be the only practical way of examining its contents.").

2. Motions for Return of Property

Rule 41(g) allows an "aggrieved" person to move for the property's return. Fed. R. Crim. P. 41(g). This rule has particular importance in computer search cases because it permits owners of seized computer equipment to move for the return of the equipment before an indictment is filed. In some cases, defendants will file such motions because they believe that the seizure of their equipment violated the Fourth Amendment. If they are correct, the equipment must be returned. *See, e.g.*, *In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853, 855-56 (9th Cir. 1997). Rule 41(g) also permits owners to move for a return of their property when the seizure was lawful, but the movant is "aggrieved by the government's continued possession of the seized property." *Id.* at 856. The multi-functionality of computer equipment occasionally leads to Rule 41(g) motions on this basis. For example, a suspect under investigation for computer hacking may file a motion claiming that he must have his computer back to calculate his taxes or check his email. Similarly, a business suspected of fraud may file a motion for the return of its equipment claiming that it needs the equipment returned or else the business will suffer.

Owners of properly seized computer equipment must overcome several formidable barriers before a court will order the government to return the equipment. First, the owner must convince the court that it should exercise equitable jurisdiction over the owner's claim. *See Floyd v. United States*, 860 F.2d 999, 1003 (10th Cir. 1988) ("Rule 41(e) jurisdiction should be exercised with caution and restraint."). Although the jurisdictional standards vary widely among different courts, most courts will assert jurisdiction over a Rule 41(g) motion only if the movant establishes: (1) that being deprived of possession of the property causes "irreparable injury," and (2) that the movant is otherwise without a remedy at law. *See In re Search of Kitty's East*, 905 F.2d 1367, 1370-

71 (10th Cir. 1990). *Cf. Ramsden v. United States*, 2 F.3d 322, 325 (9th Cir. 1993) (articulating four-factor jurisdictional test from pre-1989 version of Rule 41(g)). If the movant established these elements, the court will move to the merits of the claim. On the merits, seized property will be returned only if the government's continued possession is unreasonable. *See Ramsden*, 2 F.3d at 326. This test requires the court to weigh the government's interest in continued possession of the property with the owner's interest in the property's return. *See United States v. Premises Known as 608 Taylor Ave.*, 584 F.2d 1297, 1304 (3d Cir. 1978). In particular,

> If the United States has a need for the property in an investigation or prosecution, its retention of the property generally is reasonable. But, if the United States' legitimate interests can be satisfied even if the property is returned, continued retention of the property would be unreasonable.

Advisory Committee Notes to the 1989 Amendment of Rule 41(g) (quoted in *Ramsden*, 2 F.3d at 326); *see also In re Search of Law Office*, 341 F.3d 404, 413-14 (5th Cir. 2003) ("Rule 41(e) does not permit a district court to order complete suppression of seized evidence absent, at the very least, a substantial showing of irreparable harm").

Motions requesting the return of properly seized computer equipment succeed only rarely. First, courts will usually decline to exercise jurisdiction over the motion if the government has offered the property owner an electronic copy of the seized computer files. *See, e.g.*, *In re Search of 5444 Westheimer Road*, 2006 WL 1881370, at *2 (S.D. Tex. Jul. 6, 2006) (declining to exercise jurisdiction over a claim for pre-indictment return of property when government had provided copies of seized computer data); *In re Search Warrant Executed February 1, 1995*, 1995 WL 406276, at *2 (S.D.N.Y. Jul. 7, 1995) (concluding that owner of seized laptop computer did not show irreparable harm where government offered to allow owner to copy files it contained); *United States v. East Side Ophthalmology,* 1996 WL 384891, at *4 (S.D.N.Y. Jul. 9, 1996). *See also Standard Drywall, Inc. v. United States*, 668 F.2d 156, 157 n.2. (2d Cir. 1982) ("We seriously question whether, in the absence of seizure of some unique property or privileged documents, a party could ever demonstrate irreparable harm [justifying jurisdiction] when the Government either provides the party with copies of the items seized or returns the originals to the party and presents the copies to the jury.").

Second, courts that reach the merits generally find that the government's interest in the computer equipment outweighs the defendant's so long as a criminal prosecution or forfeiture proceeding is in the works. *See United States v. Stowe*, 1996 WL 467238, at *1-3 (N.D. Ill. Aug. 15, 1996) (continued retention of computer equipment is reasonable after 18 months where government claimed that investigation was ongoing and defendant failed to articulate convincing reason for the equipment's return); *In the Matter of Search Warrant for K-Sports Imports, Inc.*, 163 F.R.D. 594, 597 (C.D. Cal. 1995) (denying motion for return of computer records relating to pending forfeiture proceedings); *see also Johnson v. United States*, 971 F. Supp. 862, 868 (D.N.J. 1997) (denying Rule 41(e) motion to return bank's computer tapes because bank was no longer an operating business). If the government does not plan to use the computers in further proceedings, however, the computer equipment must be returned. *See United States v. Moore*, 188 F.3d 516, 1999 WL 650568, at *6 (9th Cir. Aug. 25, 1999) (ordering return of computer where "the government's need for retention of the computer for use in another proceeding now appears . . . remote"); *K-Sports Imports, Inc.*, 163 F.R.D. at 597. Further, a court may grant a Rule 41(g) motion if the defendant cannot operate his business without the seized computer equipment and the government can work equally well from a copy of the seized files. *See United States v. Bryant*, 1995 WL 555700, at *3 (S.D.N.Y. Sept. 18, 1995) (referring to magistrate judge's prior unpublished ruling ordering the return of computer equipment, and stating that "the Magistrate Judge found that defendant needed this machinery to operate his business").

F. Legal Limitations on the Use of Search Warrants to Search Computers

In general, so long as the proper procedures are followed, the government may execute a search warrant against any individual—including individuals not themselves suspected of crimes—if there is probable cause to believe that the search will reveal contraband or evidence of a crime. *See Zurcher v. Stanford Daily*, 436 U.S. 547 (1978); *Warden v. Hayden*, 387 U.S. 294, 309 (1967). Yet in a few circumstances, Congress and the Attorney General have limited the situations in which criminal investigators can use search warrants to obtain evidence. Three of these limitations apply with special force to the field of computer searches.

1. Journalists and Authors: the Privacy Protection Act

☞ When agents have reason to believe that a search may result in a seizure of materials relating to First Amendment activities such as publishing or posting materials on the Internet, they must consider the effect of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa. Every federal computer search that implicates the PPA must be approved by the Justice Department, coordinated through CCIPS at (202) 514-1026.

Under the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, law enforcement must take special steps when planning a search that agents have reason to believe may result in the seizure of certain materials that relate to the freedom of expression. Federal law enforcement searches that implicate the PPA must be pre-approved by a Deputy Assistant Attorney General of the Criminal Division. The Computer Crime and Intellectual Property Section serves as the contact point for all such searches involving computers and should be contacted directly at (202) 514-1026.

a. A Brief History of the Privacy Protection Act

When deciphering the inscrutable text of the PPA, it can be helpful to understand the context in which it was enacted. Before the Supreme Court decided *Warden v. Hayden*, 387 U.S. 294, 309 (1967), law enforcement officers could not obtain search warrants to search for and seize "mere evidence" of crime. Warrants were permitted only to seize contraband, instrumentalities, or fruits of crime. *See Boyd v. United States*, 116 U.S. 616 (1886). In *Hayden*, the Court reversed course and held that the Fourth Amendment permitted the government to obtain search warrants to seize mere evidence. This ruling set the stage for a collision between law enforcement and the press. Because journalists and reporters often collect evidence of criminal activity in the course of developing news stories, they frequently possess "mere evidence" of crime that may prove useful to law enforcement investigations. By freeing the Fourth Amendment from *Boyd*'s restrictive regime, *Hayden* created the possibility that law enforcement could use search warrants to target the press for evidence of crime it had collected in the course of investigating and reporting news stories.

It did not take long for such a search to occur. On April 12, 1971, the District Attorney's Office in Santa Clara County, California obtained a search warrant to search the offices of The Stanford Daily, a Stanford University

student newspaper. The DA's office was investigating a violent clash between the police and demonstrators that had occurred at the Stanford University Hospital three days earlier. The Stanford Daily had covered the incident, and published a special edition featuring photographs of the clash. Believing that the newspaper probably had more photographs of the clash that could help the police identify the demonstrators, the police obtained a warrant and sent four police officers to search the newspaper's office for further evidence that could assist the investigation. The officers found nothing. A month later, however, the Stanford Daily and its editors brought a civil suit against the police claiming that the search had violated their First and Fourth Amendment rights. The case ultimately reached the Supreme Court, and in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), the Court rejected the newspaper's claims. Although the Court noted that "the Fourth Amendment does not prevent or advise against legislative or executive efforts to establish nonconstitutional protections" for searches of the press, it held that neither the Fourth nor First Amendment prohibited such searches. *Id.* at 567.

Congress passed the PPA in 1980 in response to *Stanford Daily*. According to the Senate Report, the PPA protected "the press and certain other persons not suspected of committing a crime with protections not provided currently by the Fourth Amendment." S. Rep. No. 96-874, at 4 (1980), *reprinted in* 1980 U.S.C.C.A.N. 3950. The statute was intended to grant publishers certain statutory rights to discourage law enforcement officers from targeting publishers simply because they often gathered "mere evidence" of crime. As the legislative history indicates:

> The purpose of this statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.

Id. at 11.

b. The Terms of the Privacy Protection Act

Subject to certain exceptions, the PPA makes it unlawful for a government officer "to search for or seize" materials when:

(a) the materials are "work product materials" prepared, produced, authored, or created "in anticipation of communicating such materials to the public," 42 U.S.C. § 2000aa-7(b)(1);

(b) the materials include the "mental impressions, conclusions, or theories" of their creator, 42 U.S.C. § 2000aa-7(b)(3); and

(c) the materials are possessed for the purpose of communicating the material to the public by a person "reasonably believed to have a purpose to disseminate to the public" some form of "public communication," 42 U.S.C. §§ 2000aa-7(b)(3), 2000aa(a);

or

(a) the materials are "documentary materials" that contain "information," 42 U.S.C. § 2000aa-7(a); and

(b) the materials are possessed by a person "in connection with a purpose to disseminate to the public" some form of "public communication." 42 U.S.C. §§ 2000aa(b), 2000aa-7(a).

In these situations, the government is required to use a subpoena or other compulsory process rather than use a search warrant, unless a PPA exception applies.

The PPA protects a broad set of actors. It is not limited to journalists: it has been used by a publisher of role-playing games, *see Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993), and a publisher of an "internet-based journal," although the latter's claim was dismissed on other grounds. *See Mink v. Suthers*, 482 F.3d 1244, 1257-58 (10th Cir. 2007).

The PPA contains several important exceptions:

Contraband. The PPA does not apply to "contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used as, the means of committing a criminal offense." 42 U.S.C. § 2000aa-7(a), (b).

Criminal suspect. The PPA does not apply if "there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate," although the statute sets forth a further exception to this exception in certain circumstances where the offense "consists of the receipt, possession, communication, or withholding" of the

targeted materials. *See* 42 U.S.C. §§ 2000aa(a)(1), 2000aa(b)(1); *Guest v. Leis*, 255 F.3d 325, 342 (6th Cir. 2001); *DePugh v. Sutton,* 917 F. Supp. 690, 696 (W.D. Mo. 1996) ("The P.P.A. clearly allows the government to depart from the requirements of the Act in those instances in which the person suspected of a crime is in possession of documents related to the crime."). Materials may "relate" to an offense even when the relations are somewhat remote. For example, in *S.H.A.R.K. v. Metro Parks Serving Summit County*, 499 F.3d 553 (6th Cir. 2007), animal rights activists placed hidden cameras on trees to document planned extermination of deer. The removal (and seizure) of those cameras did not violate the PPA, because the cameras were "related" to the crime of trespass necessary to place them there in the first place. *Id.* at 567.

Emergency. The PPA does not apply if there is reason to believe that the immediate seizure of such materials is necessary to prevent death or serious bodily injury. *See* 42 U.S.C. §§ 2000aa(a)(2), 2000aa(b)(2).

Subpoena would be inadequate. The PPA does not apply in a search for or seizure of "documentary materials" as defined by § 2000aa-7(a), if a subpoena has proven inadequate or there is reason to believe that a subpoena would not result in the production of the materials, *see* 42 U.S.C. § 2000aa(b)(3)-(4). One court held this exception was met when an incriminating videotape was in the possession of a person who was friends with the person whom the tape would incriminate. *See Berglund v. City of Maplewood*, 173 F. Supp. 2d 935, 949-50 (D. Minn. 2001).

Importantly, these exceptions are exceptions to the PPA only, not to Fourth Amendment protections in general. When a PPA exception applies, it means only that the government may apply for a warrant – it does not mean that the government may proceed to search without a warrant. *See DePugh v. Sutton*, 917 F. Supp. 690, 696 (W.D. Mo. 1996).

Violations of the PPA do not result in suppression of the evidence, *see* 42 U.S.C. § 2000aa-6(d), but can result in civil damages against the sovereign whose officers or employees execute the search. *See* § 2000aa-6(a), (e); *Davis v. Gracey*, 111 F.3d 1472, 1482 (10th Cir. 1997) (dismissing PPA suit against municipal officers in their personal capacities because such suits must be filed only against the "government entity" unless the government entity has not waived sovereign immunity). If State officers or employees violate the PPA and the state does not waive its sovereign immunity and is thus immune from suit, *see Barnes v. State of Missouri*, 960 F.2d 63, 65 (8th Cir. 1992), individual

State officers or employees may be held liable for acts within the scope or under the color of their employment, subject to a reasonable good faith defense. *See* § 2000aa-6(a)(2),(b).

c. Application of the PPA to Computer Searches and Seizures

PPA issues frequently arise in computer cases for two reasons that would have been difficult to foresee when Congress enacted it in 1980. First, the use of personal computers for publishing and the Internet has dramatically expanded the scope of who is "involved in First Amendment activities." Today, anyone with a computer and access to the Internet may be a publisher who possesses PPA-protected materials on his or her computer.

The second reason that PPA issues arise frequently in computer cases is that the language of the statute does not explicitly rule out liability following *incidental* seizures of PPA-protected materials, and such seizures may result when agents search for and seize computer-stored contraband or evidence of crime that is commingled with PPA-protected materials. For example, investigations into illegal businesses that publish images of child pornography over the Internet have revealed that such businesses frequently support other publishing materials (such as drafts of adult pornography) that may be PPA-protected. Seizing the computer for the contraband necessarily results in the seizure of the PPA-protected materials, because the contraband is commingled with PPA-protected materials on the business's computers. If the PPA were interpreted to forbid such seizures, the statute would not merely deter law enforcement from targeting innocent publishers for their evidence, but also would bar the search and seizure of a criminal suspect's computer if the computer included PPA-protected materials, even incidentally.

The legislative history and text of the PPA indicate that Congress probably intended the PPA to apply only when law enforcement intentionally targeted First Amendment material that related to a crime, as in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). For example, the "suspect exception" eliminates PPA liability when "there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense *to which the materials relate*," 42 U.S.C. § 2000aa(a)(1), § 2000aa(b)(1) (emphasis added). This text indicates that Congress believed that PPA-protected materials would necessarily relate to a criminal offense, as when investigators target the materials as evidence. When agents collaterally seize PPA-protected materials because they are commingled on a computer with other materials properly

targeted by law enforcement, however, the PPA-protected materials might not necessarily relate to any crime at all. For example, the PPA-protected materials might be drafts of a horticulture newsletter that just happen to sit on the same hard drive as images of child pornography or records of a fraud scheme.

The Sixth Circuit has explicitly ruled that the incidental seizure of PPA-protected material commingled on a suspect's computer with evidence of a crime does *not* give rise to PPA liability. *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001), involved two lawsuits brought against the Sheriff's Department in Hamilton County, Ohio. The suits arose from the seizures of two servers that had been used to host bulletin board systems suspected of housing evidence and contraband relating to obscenity, phone tapping, child pornography, credit card theft, and software piracy. The Sixth Circuit noted that "when police execute a search warrant for documents on a computer, it will often be difficult or impossible (particularly without the cooperation of the owner) to separate the offending materials from other 'innocent' material on the computer" at the site of the search. *Id.* at 341-42. Given these pragmatic concerns, the court refused to find PPA-liability for incidental seizures; to construe the PPA otherwise would "prevent police in many cases from seizing evidence located on a computer." *Id.* at 342. Instead, the court held that "when protected materials are commingled on a criminal suspect's computer with criminal evidence that is unprotected by the act, we will not find liability under the PPA for seizure of the PPA-protected materials." *Id.* The Guest court cautioned, however, that although the incidental seizure of PPA-related work-product and documentary materials did not violate the Act, the subsequent search of such material was probably forbidden. *Id.*

The Sixth Circuit's decision in *Guest* verifies that the suspect exception works as the legislature intended: limiting the scope of PPA protection to "the press and certain other persons not suspected of committing a crime." S. Rep. No. 96-874, at 4 (1980), *reprinted in* 1980 U.S.C.C.A.N. 3950. At least one other court has also reached this result by broadly interpreting the suspect exception's phrase "to which materials relate" when an inadvertent seizure of commingled matter occurs. *See United States v. Hunter*, 13 F. Supp. 2d 574, 582 (D. Vt. 1998) (concluding that materials for weekly legal newsletter published by the defendant from his law office "relate" to the defendant's alleged involvement in his client's drug crimes when the former was inadvertently seized in a search for evidence of the latter). *See also S.H.A.R.K. v. Metro Parks Serving Summit County*, 499 F.3d 553, 567 (6th Cir. 2007) (seizure of video cameras placed

by trespassers did not violate PPA because cameras were related to the crime of trespass); *Carpa v. Smith*, 2000 WL 189678, at *1 (9th Cir. Feb. 15, 2000) ("[T]he Privacy Protection Act . . . does not apply to criminal suspects.").

The Sixth Circuit's decision in *Guest* does not address the commingling issue when the owner of the seized computer is not a suspect. In the only published decision to date directly addressing this issue, a district court held the United States Secret Service liable for the inadvertent seizure of PPA-protected materials. *See Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd on other grounds*, 36 F.3d 457 (5th Cir. 1994).[2] Steve Jackson Games, Inc. ("SJG") was primarily a publisher of role-playing games, but it also operated a network of thirteen computers that provided its customers with email, published information about SJG products, and stored drafts of upcoming publications. Believing that the system administrator of SJG's computers had stored evidence of crimes, the Secret Service obtained a warrant and seized two of the thirteen computers connected to SJG's network, in addition to other materials. The Secret Service did not know that SJG's computers contained publishing materials until the day after the search. However, the Secret Service did not return the computers it seized until months later. At no time did the Secret Service believe that SJG itself was involved in the crime under investigation.

The district court in *Steve Jackson Games* ruled that the Secret Service violated the PPA; unfortunately, the exact contours of the court's reasoning are difficult to discern. For example, the court did not explain exactly which of the materials the Secret Service seized were covered by the PPA; instead, the court merely recited the property that had been seized, and concluded that some PPA-protected materials "were obtained" during the search. *Id.* at 440. Similarly, the court indicated that the search of SJG and the initial seizure of its property did not violate the PPA, but that the Secret Service's continued retention of SJG's property after it learned of SJG's publisher status, and despite a request by SJG for return of the property, was the true source of the PPA violation – something that the statute itself does not appear to contemplate. *See id.* at 441. The court also suggested that it might have ruled differently if the Secret Service had

[2] The *Steve Jackson Games* litigation raised many important issues involving the PPA and the SCA before the district court. On appeal, however, the only issue raised was "a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an 'intercept' proscribed by 18 U.S.C. § 2511(1)(a)." *Steve Jackson Games*, 36 F.3d at 460. This issue is discussed in the electronic surveillance chapter. *See* Chapter 4, *infra*.

made "copies of all information seized" and returned the hardware as soon as possible, but did not answer whether in fact it would have reached a different result in such case. *Id.*

Incidental seizure of PPA-protected materials on a non-suspect's computer continues to be an uncertain area of the law, in part because PPA issues are infrequently litigated. As a practical matter, agents can often avoid the seizure of PPA-protected materials on a non-suspect's computer by using a subpoena or process under the SCA to require the non-suspect to produce the desired information, as described in Chapter 3. To date, no other court has followed the PPA approach of *Steve Jackson Games*. *See, e.g.*, *State v. One (1) Pioneer CD-ROM Changer*, 891 P.2d 600, 607 (Okla. App. 1994) (questioning the apparent premise of *Steve Jackson Games* that the seizure of computer equipment could violate the PPA merely because the equipment "also contained or was used to disseminate potential 'documentary materials'"). Moreover, even if courts eventually refuse to restrict the PPA to cases in which law enforcement intentionally seizes from a non-suspect First Amendment material that is merely evidence of a crime, courts may conclude that other PPA exceptions, such as the "contraband or fruits of a crime" exception, should be read as broadly as the *Guest* court read the suspect exception.

The additional handful of federal courts that have resolved civil suits filed under the PPA have ruled against the plaintiffs with little substantive analysis. *See, e.g.*, *Davis v. Gracey*, 111 F.3d 1472, 1482 (10th Cir. 1997) (dismissing for lack of jurisdiction PPA suit improperly filed against municipal employees in their personal capacities); *Berglund v. City of Maplewood*, 173 F. Supp. 2d 935, 949-50 (D. Minn. 2001) (holding that the police seizure of a defendant's videotape fell under the "criminal suspect" and "destruction of evidence" exceptions to the PPA because the tape might have contained documentary evidence of the defendant's disorderly conduct); *DePugh v. Sutton*, 917 F. Supp. 690, 696-97 (W.D. Mo. 1996) (rejecting *pro se* PPA challenge to seizure of materials relating to child pornography because there was probable cause to believe that the person possessing the materials committed the criminal offense to which the materials related), *aff'd*, 104 F.3d 363 (8th Cir. 1996); *Powell v. Tordoff*, 911 F. Supp. 1184, 1189-90 (N.D. Iowa 1995) (dismissing PPA claim because plaintiff did not have standing to challenge search and seizure under the Fourth Amendment). *See also Lambert v. Polk County*, 723 F. Supp. 128, 132 (S.D. Iowa 1989) (rejecting PPA claim after police seized videotape

because officers could not reasonably believe that the owner of the tape had a purpose to disseminate the material to the public).

Agents and prosecutors who have reason to believe that a computer search may implicate the PPA should contact the Computer Crime and Intellectual Property Section at (202) 514-1026 or the CHIP in their district (*see* Introduction, p. xii) for more specific guidance.

2. Privileged Documents

Agents must exercise special care when planning a computer search that may result in the seizure of legally privileged documents such as medical records or attorney-client communications. Two issues must be considered. First, agents should make sure that the search will not violate the Attorney General's regulations relating to obtaining confidential information from disinterested third parties. Second, agents should devise a strategy for reviewing the seized computer files following the search so that no breach of a privilege occurs.

a. The Attorney General's Regulations Relating to Searches of Disinterested Third Party Lawyers, Physicians, and Clergymen

Agents should be very careful if they plan to search the office of a doctor, lawyer, or member of the clergy who is not implicated in the crime under investigation. At Congress's direction, the Attorney General has issued guidelines for federal officers who want to obtain documentary materials from such disinterested third parties. *See* 42 U.S.C. § 2000aa-11(a); 28 C.F.R. § 59.4(b). Under these rules, federal law enforcement officers should not use a search warrant to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman where the material sought or likely to be reviewed during the execution of the warrant contains confidential information on patients, clients, or parishioners. 28 C.F.R. § 59.4(b). The regulation does contain a narrow exception. A search warrant can be used if using less intrusive means would substantially jeopardize the availability or usefulness of the materials sought; access to the documentary materials appears to be of substantial importance to the investigation; and the application for the warrant has been recommended by the U.S. Attorney and approved by the appropriate Deputy Assistant Attorney General. *See* 28 C.F.R. § 59.4(b)(1) and (2).

When planning to search the offices of a lawyer under investigation, agents should follow the guidelines offered in the United States Attorneys' Manual,

and should consult OEO at (202) 514-6809. *See generally* United States Attorneys' Manual, § 9-13.420 (1997).

b. Strategies for Reviewing Privileged Computer Files

☞ Agents contemplating a search that may result in the seizure of legally privileged computer files should devise a post-seizure strategy for screening out the privileged files and should describe that strategy in the affidavit.

When agents seize a computer that contains legally privileged files, a trustworthy third party must examine the computer to determine which files contain privileged material. After reviewing the files, the third party will offer those files that are not privileged to the prosecution team. Preferred practices for determining who will comb through the files vary widely among different courts. In general, however, there are three options. First, the court itself may review the files *in camera*. Second, the presiding judge may appoint a neutral third party known as a "special master" to the task of reviewing the files. Third, a team of prosecutors or agents who are not working on the case may form a "filter team" or "taint team" to help execute the search and review the files afterwards. The filter team sets up a so-called "ethical wall" between the evidence and the prosecution team, permitting only unprivileged files to pass over the wall.

Because a single computer can store millions of files, judges will undertake *in camera* review of computer files only rarely. *See Black v. United States*, 172 F.R.D. 511, 516-17 (S.D. Fla. 1997) (accepting *in camera* review given unusual circumstances); *United States v. Skeddle*, 989 F. Supp. 890, 893 (N.D. Ohio 1997) (declining *in camera* review). Instead, the typical choice is between using a filter team and a special master. Most prosecutors will prefer to use a filter team if the court consents. A filter team can usually review the seized computer files fairly quickly, whereas special masters often take several years to complete their review. *See Black*, 172 F.R.D. at 514 n.4. On the other hand, some courts have expressed discomfort with filter teams. *See In re Grand Jury Subpoenas*, 454 F.3d 511, 522-23 (6th Cir. 2006) (approving of use of filter teams in connection with search warrants while disapproving of their use in connection with grand jury subpoenas); *United States v. Neill*, 952 F. Supp. 834, 841 (D.D.C. 1997); *United States v. Hunter*, 13 F. Supp. 2d 574, 583 n.2 (D. Vt. 1998) (stating that review by a magistrate judge or special master "may

be preferable" to reliance on a filter team) (citing *In re Search Warrant*, 153 F.R.D. 55, 59 (S.D.N.Y. 1994)).

Although no single standard has emerged, courts have generally indicated that evidence screened by a filter team will be admissible only if the government shows that its procedures adequately protected the defendants' rights and no prejudice occurred. *See, e.g.*, *Neill*, 952 F. Supp. at 840-42; *Hunter*, 13 F. Supp. 2d at 583. One approach to limit the amount of potentially privileged material in dispute is to have defense counsel review the output of the filter team to identify those documents for which counsel intends to raise a claim of privilege. Files thus identified that do not seem relevant to the investigation need not be litigated. Although this approach may not be appropriate in every case, magistrates may appreciate the fact that defense counsel has been given the chance to identify potential claims before the material is provided to the prosecution team.

In unusual circumstances, the court may conclude that a filter team would be inadequate and may appoint a special master to review the files. *See, e.g.*, *United States v. Abbell*, 914 F. Supp. 519 (S.D. Fla. 1995); *DeMassa v. Nunez*, 747 F.2d 1283 (9th Cir. 1984). In any event, the reviewing authority will almost certainly need a neutral technical expert to assist in sorting, identifying, and analyzing digital evidence for the reviewing process.

3. Other Disinterested Third Parties

In addition to the more specific restrictions on using a search warrant to obtain information from disinterested publishers, lawyers, physicians, and clergymen, Department of Justice policy favors the use of a subpoena or other less intrusive means to obtain evidence from disinterested third parties, unless use of those less intrusive means would substantially jeopardize the availability or usefulness of the materials sought. *See* 28 C.F.R. § 59.4(a)(1); United States Attorneys' Manual, § 9-19.210. Except in emergencies, the application for such a warrant must be authorized by an attorney for the government. *See* 28 C.F.R. § 59.4(a)(2); United States Attorneys' Manual, § 9-19.210. Importantly, however, failure to comply with this policy "may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion of evidence." 28 C.F.R. § 59.5(b).

4. Communications Service Providers: the SCA

☞ When a search may result in the incidental seizure of network accounts belonging to innocent third parties, agents should take every step to protect the integrity of the third party accounts.

One category of disinterested third party often encountered in the computer context is Internet service providers. The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, governs law enforcement access to the contents of electronic communications stored by third-party service providers. *See* Chapter 3, *infra* (discussing the SCA). In most cases, law enforcement officials should use the compulsory process provisions of § 2703 to compel a service provider to disclose information; when possible, law enforcement officials should avoid physical execution of a Rule 41 search warrant on service providers. When law enforcement officers execute a Rule 41 search warrant on an Internet service provider and seize the accounts of customers and subscribers, those customers and subscribers may bring civil actions claiming that the search violated the SCA. In addition, the SCA has a criminal provision that prohibits unauthorized access to electronic or wire communications in "electronic storage." *See* 18 U.S.C. § 2701; Chapter 3, *infra* (discussing the definition of "electronic storage").

The text of the SCA does not appear to contemplate civil liability for searches and seizures authorized by valid Rule 41 search warrants: the SCA expressly authorizes government access to stored communications pursuant to a warrant issued under the Federal Rules of Criminal Procedure, *see* 18 U.S.C. § 2703(a), (b), (c)(1)(A); *Davis v. Gracey*, 111 F.3d 1472, 1483 (10th Cir. 1997), and the criminal prohibition of § 2701 does not apply when access is authorized under § 2703. *See* 18 U.S.C. § 2701(c)(3). Nonetheless, *Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993), raised the concern that a search executed pursuant to a valid warrant might violate the SCA. In *Steve Jackson Games*, the district court held the Secret Service liable under the SCA after it seized, reviewed, and (in some cases) deleted stored electronic communications seized pursuant to a valid search warrant. *See id.* at 442-43. The court's holding appears to be rooted in the mistaken belief that the SCA requires that search warrants also comply with 18 U.S.C. § 2703(d) and the various notice requirements of § 2703. *See id.* In fact, the SCA makes quite clear that § 2703(d) and the notice requirements of § 2703

are implicated only when law enforcement does not obtain a search warrant.[3] *Compare* 18 U.S.C. § 2703(b)(1)(A), *with* 18 U.S.C. § 2703(b)(1)(B). Further, objectively reasonable good faith reliance on a warrant, court order, or statutory authorization is a complete defense to an SCA violation. *See* 18 U.S.C. § 2707(e). *Compare Gracey*, 111 F.3d at 1484 (applying good faith defense because seizure of stored communications incidental to a valid search was objectively reasonable), *with Steve Jackson Games*, 816 F. Supp. at 443 (stating without explanation that the court "declines to find this defense").

The best way to square the result in *Steve Jackson Games* with the plain language of the SCA is to exercise great caution when agents need to execute searches of Internet service providers and other third-parties holding stored wire or electronic communications. In every computer search, agents should strive to avoid unwarranted intrusions into private areas, and searches of service providers are no different. *See Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) ("responsible officials, including judicial officials, must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy."). In most cases, investigators will want to avoid a wholesale search and seizure of the provider's computers by relying instead on compulsory process served on the provider consistent with the SCA. When investigators have no choice but to execute the search, such as where the service provider lacks the ability or will to comply with compulsory process or is suspected of involvement in the criminal conduct, agents must search the provider's computers themselves. Because each of the provider's computers might contain records relating to users who are wholly unrelated to the criminal investigation, special procedures designed to uphold those users' privacy interests may be appropriate. For example, agents might inform the magistrate judge in the search warrant affidavit that they will take steps to ensure the confidentiality of the accounts and not expose their contents to human inspection. Safeguarding the accounts of innocent persons absent specific reasons to believe that evidence may be stored in the persons' accounts

[3] This raises a fundamental distinction overlooked in *Steve Jackson Games:* the difference between a search warrant issued under Rule 41 that law enforcement executes with a physical search, and a search warrant issued under the SCA that law enforcement executes by compelling a provider of electronic communication service or remote computing service to disclose the contents of a subscriber's network account. Although both are search warrants, they are different in practice. This distinction is especially important when a court concludes that the SCA was violated and then must determine the remedy because there is no statutory suppression for nonconstitutional violations of the SCA. *See* 18 U.S.C. § 2708; Chapter 3.I, *infra* (discussing remedies for violations of the SCA).

should satisfy the concerns expressed in *Steve Jackson Games*. *Compare Steve Jackson Games*, 816 F. Supp. at 441 (finding SCA liability where agents read the private communications of customers not involved in the crime "and thereafter deleted or destroyed some communications either intentionally or accidentally"), *with Gracey*, 111 F.3d at 1483 (declining to find SCA liability in seizure where "[p]laintiffs have not alleged that the officers attempted to access or read the seized e-mail, and the officers disclaimed any interest in doing so").