FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* v. JUSTIN BARRETT HILL, *Defendant-Appellant.*	No. 05-50219 D.C. No. CR-02-01289-AK-01 OPINION

Appeal from the United States District Court
for the Central District of California
Alex Kozinski, Circuit Judge, Presiding

Argued and Submitted
January 12, 2006—Pasadena, California

Filed August 11, 2006

Before: Mary M. Schroeder, Chief Judge, Alfred T. Goodwin and Raymond C. Fisher, Circuit Judges.

Opinion by Judge Fisher

COUNSEL

Carlton F. Gunn, Deputy Federal Public Defender, Los Angeles, California, for the defendant-appellant.

Michael R. Wilner (argued) and Thomas P. O'Brien, Assistant United States Attorneys, and Los Angeles, California, for the plaintiff-appellee.

OPINION

FISHER, Circuit Judge:

Justin Hill conditionally pled guilty to possession of child pornography subject to his challenge to the admission of evidence that he contends was seized in violation of the Fourth Amendment. His appeal involves the validity of a warrant to search his computer and storage media for evidence that he possessed pornographic (i.e., lascivious) images of children. We must also decide whether it was reasonable under the Fourth Amendment for the police to take all of Hill's computer storage media from his home (they did not find his computer) so they could conduct their search offsite in a police laboratory, rather than carrying out the search onsite and taking only whatever evidence of child pornography they might find. As we recently discussed in *United States v. Adjani*, ____ F.3d ____, 2006 WL 1889946 (9th Cir. July 11, 2006), because computers typically contain so much information beyond the scope of the criminal investigation, computer-related searches can raise difficult Fourth Amendment issues different from those encountered when searching paper files. Judge Kozinski, sitting as the district court in this case, thoughtfully addressed some of these issues in a published opinion upholding the validity of the search warrant and its execution. *United States v. Hill*, 322 F. Supp. 2d 1081, 1092 (C.D. Cal. 2004). We affirm the district court's ruling in most but not all respects for the reasons Judge Kozinski stated; to the extent we do agree with that reasoning, we adopt it verbatim in this opinion. In sum, we affirm the district court's denial of the defendant's motion to suppress evidence.

I. *Background*

As the district court explained:

> A computer technician was repairing defendant's computer when she discovered what she believed to

be child pornography. She called Long Beach police, and the detective who took the call obtained a search warrant from a judge of the Long Beach Superior Court. The warrant authorized a search of the computer repair store and seizure of the computer, any work orders relating to the computer, "all storage media belonging to either the computer or the individual identifying himself as defendant at the location," and "all sexually explicit images depicting minors contained in the storage media." By the time the detective arrived at the store to execute the warrant, defendant had picked up his computer. . . . [T]he detective [submitted an affidavit, which included the computer technician's sworn statement describing the images. On the basis of this affidavit, the officer obtained] a second warrant, this one directed at defendant's home, authorizing seizure of the same items.

The affidavit on which the warrants were based described "two images of child pornography":

Image 1

Is a color picture of a female, white, approximately 15 years old, with long dark brown hair. The female is in a room standing between a couch and a coffee table. There is a framed picture on the wall above the couch. She is wearing only a long blouse and pair of socks. The blouse is open and she is exposing her breast and pubic area to the camera, which she is facing while leaning to her left.

Image 2

Is a color picture of a [sic in affidavit] two females, white, approximately 7-9 years of age, both with dirty blond hair. These females are standing on a

beach during the daytime. The shorter of the two females is standing to the right of the picture while the other female is standing behind her. Both females are facing the camera askew and wearing only a robe, which is open exposing the undeveloped breast and pubic area of both girls. They both are turning their faces away from the camera preventing the viewer from seeing their faces.

Officers executed the search warrant but did not find the computer in defendant's apartment.[1] In what appeared to be defendant's bedroom, they found and seized computer storage media[, specifically: 22 5.25-inch floppy disks, two CD-ROMs, 124 3.5-inch floppy disks and six zip disks.] [Two of the zip disks] were eventually determined to contain images of child pornography; [officers] also seized other evidence consistent with the warrant. Defendant was subsequently charged with one count of possession of child pornography,[2] in violation of 18 U.S.C.

[1]Or anywhere else: The computer was never found.

[2]18 U.S.C. § 2256(8) defines "child pornography" as

> any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where —
>
> (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
>
> (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
>
> (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Section 2256(2)(B)(iii) defines "sexually explicit conduct" as "graphic or simulated lascivious exhibition of the genitals or pubic area of any person." Thus, the lascivious exhibition of the genitals or pubic area of a minor constitutes child pornography. A portion of section 2256(8) that is irrelevant to the issues raised in these motions was held unconstitutional in *Ashcroft v. Free Speech Coalition*. *See* 535 U.S. 234 (2002).

§ 2252A(a)(5)(B).[3]

Hill, 322 F. Supp. 2d at 1083-84 (alterations in original).

In the district court, the defendant moved to suppress the evidence recovered from the two zip disks on the grounds that, (1) contrary to the magistrate's finding, the warrant affidavit did not establish probable cause to believe the defendant was guilty of criminal activity; and (2) the warrant was overbroad in allowing seizure of all discovered computer storage media with no regard to whether such media contained child pornography, and in placing no limitation on the police officers' search of the seized disks. *Id.* at 1084.[4] The district court denied the motion to suppress and the defendant conditionally pled guilty to the charge, reserving the right to appeal the district court's evidentiary ruling.[5] This timely appeal followed.

[3]Section 2252A(a)(5)(B) prohibits:

> knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

[4]The defendant did not challenge the warrant affidavit on the ground that it included only a written description of the images and not the images themselves. *Cf. United States v. Battershell*, ___ F.3d ___, ___, slip op. at 9271 (9th Cir. Aug. 10, 2006) ("It would have been preferable if the affiant in this case had included copies of the photographs [to which the affiant had access] in the warrant application. But failing to include a photograph in a warrant application is not fatal to establishing probable cause. (citing *United States v. Smith*, 795 F.2d 841, 847 (9th Cir. 1986))).

[5]In the district court, the defendant also argued that in order to prepare a defense his counsel and his expert were entitled to "mirror image" copies of the computer media the government seized. The district court agreed and ordered the government to provide defendant with copies. *Hill*, 322 F. Supp. 2d at 1091-92. That ruling is not contested here.

II. *Standard of Review*

We review de novo the district court's denial of a motion to suppress evidence. *United States v. Meek*, 366 F.3d 705, 711 (9th Cir. 2004). We review for clear error a magistrate's finding of probable cause to issue a search warrant and give "great deference" to such a finding. *United States v. Hay*, 231 F.3d 630, 634 n.4 (9th Cir. 2000).

III. *Discussion*

A. *Probable Cause*

The defendant argues first that the affidavit submitted in support of the search warrant was insufficient to establish probable cause to believe the defendant was guilty of criminal activity. We do not agree.

[1] "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Constitution is clear; a magistrate may authorize a search of a location only if officers establish probable cause to believe evidence of a crime may be found there. Probable cause means only a "fair probability," not certainty, and requires consideration of the totality of the circumstances. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Accordingly, we must determine whether the officer's affidavit, which described the two images from the defendant's computer as showing three different, minor girls with their breasts and pubic areas exposed, established a fair probability that there was child pornography or evidence thereof to be found in computer hardware or software at the defendant's home. We agree with the district court that the affidavit did establish probable cause, but reach that conclusion somewhat differently.

[2] Child pornography is a particularly repulsive crime, but not all images of nude children are pornographic. For example, "a family snapshot of a nude child bathing presumably would not" be criminal. *Hill*, 322 F. Supp. 2d at 1086. Moreover, the law recognizes that some images of nudity may merit First Amendment protection because they serve artistic or other purposes, and possessing those images cannot be criminal. *See Osborne v. Ohio*, 495 U.S. 103, 112-13 (1990) (upholding Ohio's child pornography law because it had been interpreted to criminalize possession of images depicting not just nudity, but "nudity constitut[ing] a lewd exhibition"); *New York v. Ferber*, 458 U.S. 747, 765 n.18 (1982) ("[N]udity, without more[,] is protected expression."). Images depicting "minor[s] engag[ed] in sexually explicit conduct" are, however, prohibited. 18 U.S.C. § 2256(8)(A). "[S]exually explicit conduct," in turn, is defined to include "graphic or simulated *lascivious* exhibition of the genitals or pubic area of any person." 18 U.S.C. § 2256(2)(A)(v) (emphasis added). Thus the more precise question we must answer is whether the officer's affidavit established probable cause that the images on the defendant's computer were — as described — lascivious.[6] *See Hill*, 322 F. Supp. 2d at 1084. In answering that question, it is important to remember that in issuing the search warrant, the magistrate had to make a practical, commonsense decision, based on the totality of the circumstances

[6]We stress that in this case the state court judge who issued the warrant made his determination based upon a *written description* of the images. The officer presenting that description of the images had a duty, of course, to do so in good faith, providing all relevant information to the magistrate. *See United States v. Mendonsa*, 989 F.2d 366, 369 (9th Cir. 1993) ("Suppression remains an appropriate remedy, however, when a magistrate is misled by information in the affidavit, which the affiant knows, or should know, is false."); *see also Baldwin v. Placer County*, 405 F.3d 778, 782 (9th Cir.), *amended by* 418 F.3d 966 (9th Cir. 2005) (refusing to grant an officer qualified immunity because "[t]he plaintiffs' established civil rights were violated by presentation of [a] false affidavit"). If the magistrate had been able to view the two images for himself, his analysis and our subsequent review might be different.

presented to him in the affidavit, that there was a "fair probability" that the images were lascivious. *See United States v.* Gourde, 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc).[7]

[3] Various courts have attempted to articulate a test for determining lasciviousness. Many have relied upon a six-factor test originated in *United States v. Dost*:

> (1) whether the focal point of the visual depiction is on the child's genitalia or pubic area;
>
> (2) whether the setting of the visual depiction is sexually suggestive, i.e., in a place or pose generally associated with sexual activity;
>
> (3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child;
>
> (4) whether the child is fully or partially clothed, or nude;
>
> (5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity;
>
> (6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer.

[7]The defendant challenges only whether there was probable cause to believe the images described were lascivious, i.e., whether there was a fair probability that the defendant possessed evidence of a crime (child pornography). Assuming he loses the lasciviousness argument, he does not argue there was no probable cause to believe that such evidence could be found on his computer (or storage media). *Cf. Gourde*, 440 F.3d at 1069 ("We conclude that the affidavit contained sufficient facts to support the magistrate judge's finding that there was a 'fair probability' that Gourde's *computer* contained evidence that he violated 18 U.S.C. §§ 2252 or 2252A." (emphasis added)).

636 F.Supp. 828, 832 (S.D. Cal. 1986), *aff'd sub nom. United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987); *see also United States v. Brunette*, 256 F.3d 14, 18 (1st Cir. 2001) (adopting and applying *Dost* factors); *United States v. Villard*, 885 F.2d 117, 122 (3d Cir. 1989) (same).

The district court, analyzing each of these six factors, found *Dost* to be "not particularly helpful" in determining whether a given image is lascivious — generally or as applied to the images here. *See Hill*, 322 F.Supp.2d at 1086. Instead, the court fashioned a new test that would create a presumption of lasciviousness, and therefore probable cause, "[i]f an image of a minor displays the minor's naked genital area . . . [,] unless there are strong indicators that [the image] is *not* lascivious."[8] *Id.* at 1086-87. Although we appreciate the district court's careful analysis and critique of *Dost*, we do not think it necessary to adopt a new test or to deny the utility of *Dost* in the context of this case.

[4] The *Dost* factors can be a starting point for judges to use in determining whether a particular image is likely "so presented by the photographer as to arouse or satisfy the sexual cravings of a voyeur." *Wiegand*, 812 F.2d at 1244. But the factors are neither exclusive nor conclusive. *Dost* itself acknowledged that it did not seek to offer "a comprehensive definition of . . . lasciviousness," because a determination of

[8]The district court's test might be an improvement over the *Dost* six-factor inquiry, at least when the magistrate can see and evaluate the images first hand. However, when (as here) the magistrate does not have the images, the judge would have to determine whether "there are strong indicators that [the image] is not lascivious" based on the information the attesting officer (or, as in this case, a third-party witness) includes in the description. It is not clear that officers would be as able to decide and articulate what is relevant *mitigating* information (from the unrepresented target's viewpoint) as in making their affirmative showing of lasciviousness under existing doctrine. *Cf. Hill*, 322 F. Supp. 2d at 1085-86 (discussing the government's and the defendant's starkly differing views of the images during the suppression hearing).

lasciviousness "ha[s] to be made based on the overall content of the visual depiction." 636 F. Supp. at 832. The factors are merely "general principles as guides for analysis." *Id.* For instance, we have already recognized that, in some instances, the factors may be "over generous" to defendants. *Wiegand*, 812 F.2d at 1244; *see also United States v. Amirault*, 173 F.3d 28, 32 (1st Cir. 1999) ("We believe that the *Dost* factors are generally relevant and provide some guidance in evaluating whether the display in question is lascivious. We emphasize, however, that these factors are neither comprehensive nor necessarily applicable in every situation. Although *Dost* provides some specific, workable criteria, there may be other factors that are equally if not more important in determining whether a photograph contains a lascivious exhibition. The inquiry will always be case-specific.").

[5] Ultimately, probable cause is a fluid and nontechnical conception not readily susceptible to multifactor tests or rebuttable presumptions. *See Maryland v. Pringle*, 540 U.S. 366, 370-71 (2003) ("[T]he probable-cause standard is a . . . nontechnical conception . . . . [and] a fluid concept — turning on the assessment of probabilities in particular factual contexts — not readily, or even usefully, reduced to a neat set of legal rules . . . . [It] is incapable of precise definition or quantification . . . ." (internal quotation marks and citation omitted).) The magistrate, relying on *Dost* as a guidepost or on some other test for lasciviousness, need only make a "practical, common-sense decision" that the description presented in the affidavit demonstrates a "fair probability" that the images are lascivious. *Gates*, 462 U.S. at 238; *see also Gourde*, 440 F.3d at 1071; *Wiegand*, 812 F.2d at 1244 ("The definition of 'lasciviousness' is a matter of law . . . .").

[6] Based on our independent review of the affidavit describing the two images, we are satisfied that the state judge's finding of probable cause was well within his discretion. There was a fair probability that the images were "so presented by the photographer as to arouse or satisfy the sex-

ual cravings of a voyeur." *Wiegand*, 812 F.3d at 1244; *see also id.* ("Necessarily in deciding whether the district court erred as to the facts [in determining that the images were lascivious], we must view the pictures ourselves and must interpret the statutory term."). The affidavit described in some detail the images of three partially nude children, who were provocatively and unnaturally dressed in light of the photographs' settings. The girls' clothing was opened so as to reveal their breasts and pubic areas, with the girls appearing in sexually suggestive poses.[9] Moreover the descriptions themselves did not raise doubts that the images served some purpose other than that proscribed in *Wiegand*.[10] *Cf. Battershell*, ___ F.3d at ___, slip op. at 9267 (holding that an affidavit describing "a young female (8-10 YOA) naked in a bathtub" is insufficient to establish probable cause to believe the image is lascivious). The affidavit was sufficient to create "a substantial basis for concluding that probable cause existed" to believe that evidence of a violation of 18 U.S.C. § 2252A(a)(5)(B) could be found on the defendant's computer. *See Gates*, 462 U.S. at 238-39 (internal quotation marks and alterations omitted).

B. *Overbreadth*

1. *Seizure of All Computer Media*

The defendant argues that the search warrant was overbroad because it authorized the officers to seize and remove from his home his computer and storage media without first

[9]Although the defendant at trial might have been able to present evidence supporting innocent explanations for the content of the pictures, that does not negate the images' *prima facie* appearance of lasciviousness — which is the issue relevant to probable cause.

[10]In contrast to the concerns we raised in footnote 8, *supra*, the defendant does not argue that the affidavit's description of the images was incomplete in any way; nor does he claim that the attesting officer was aware of but failed to disclose mitigating facts that would tend to show the images were not lascivious.

determining whether they actually contained child pornography. Given the nature of computers and storage media, this argument sweeps too broadly, as the district court explained in addressing the defendant's suggested limitations on the nature and scope of the search:

> Search warrants must be specific. "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993) (internal quotation marks and citations omitted). A warrant describing a category of items is not invalid if a more specific description is impossible. *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). The level of specificity required "varies depending on the circumstances of the case and the type of items involved." *Id.*
>
> The warrant here commanded the officers to search for and seize: "1) An IBM 'clone' medium tower personal computer . . . 3) All storage media belonging to either item # 1 or the individual identifying himself as defendant at the location. 4) All sexually explicit images depicting minors contained in item # 3." Defendant argues the warrant was overbroad because it authorized seizure of storage media whether or not they contained child pornography. He suggests it should have authorized seizure only of media containing child pornography. But it is impossible to tell what a computer storage medium contains just by looking at it. Rather, one has to examine it electronically, using a computer that is running the appropriate operating system, hardware and software. The police had no assurance they would find such a computer at the scene — nor did they, for that

matter — or that, if they found one, they could bypass any security measures and operate it.

Defendant suggests that the police could have brought their own laptop computer: Having probable cause to seize only computer storage media that contained certain types of files, the police should have been required to bring with them the equipment necessary to separate the sheep from the goats. Defendant's argument raises an important question about how police must execute seizures pursuant to a warrant. Because seizable materials are seldom found neatly separated from their non-seizable counterparts, how much separating must police do at the scene to avoid taking items that are neither contraband nor evidence of criminal activity?

As always under the Fourth Amendment, the standard is reasonableness. To take an extreme example, if police have probable cause to seize business records, the warrant could not authorize seizure of every piece of paper on the premises on the theory that the police conducting the search might not know how to read. . . .

[T]he court concludes that the police were not required to bring with them equipment capable of reading computer storage media and an officer competent to operate it. Doing so would have posed significant technical problems and made the search more intrusive. To ensure that they could access any electronic storage medium they might find at the scene, police would have needed far more than an ordinary laptop computer. Because computers in common use run a variety of operating systems — various versions or flavors of Windows, Mac OS and Linux, to name only the most common — police would have had to bring with them a computer (or

computers) equipped to read not only all of the major media types, but also files encoded by all major operating systems. Because operating systems, media types, file systems and file types are continually evolving, police departments would frequently have to modify their computers to keep them up-to-date. This would not be an insuperable obstacle for larger police departments and federal law enforcement agencies, but it would pose a significant burden on smaller agencies.

Even if the police were to bring with them a properly equipped computer, and someone competent to operate it, using it would pose two significant problems. First, there is a serious risk that the police might damage the storage medium or compromise the integrity of the evidence by attempting to access the data at the scene. As everyone who has accidentally erased a computer file knows, it is fairly easy to make mistakes when operating computer equipment, especially equipment one is not intimately familiar with. The risk that the officer trying to read the suspect's storage medium on the police laptop will make a wrong move and erase what is on the disk is not trivial. Even if the officer executes his task flawlessly, there might be a power failure or equipment malfunction that could affect the contents of the medium being searched. For that reason, experts will make a back-up copy of the medium before they start manipulating its contents. Various other technical problems might arise; without the necessary tools and expertise to deal with them, any effort to read computer files at the scene is fraught with difficulty and risk.

Second, the process of searching the files at the scene can take a long time. To be certain that the medium in question does *not* contain any seizable

> material, the officers would have to examine every one of what may be thousands of files on a disk — a process that could take many hours and perhaps days. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress, and this would necessarily interfere with the suspect's access to his home or business. If the search took hours or days, the intrusion would continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible.

Hill, 322 F. Supp. 2d at 1087-89 (alteration in original and internal citation omitted).

[7] We agree with the district court that under the circumstances here, the warrant was not fatally defective in failing to require an onsite search and isolation of child pornography before removing storage media wholesale. That does not mean, however, that the government has an automatic blank check when seeking or executing warrants in computer-related searches. Although computer technology may in theory justify blanket seizures for the reasons discussed above, the government must still demonstrate to the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand. There may well be situations where the government has no basis for believing that a computer search would involve the kind of technological problems that would make an immediate onsite search and selective removal of relevant evidence impracticable. Thus, there must be some threshold showing before the government may "seize the haystack to look for the needle."

Our cases illustrate this principle. In *United States v. Hay*, for example, we held permissible a "generic classification"

authorizing seizure of an "entire computer system and virtually every document in [the defendant's] possession without referencing child pornography or any particular offense conduct" because, although officers "knew that [a party] had sent 19 images [of child pornography] directly to [the defendant's] computer, [they] had no way of knowing where the images were stored." 231 F.3d 630, 637 (9th Cir. 2000). Similarly *United States v. Lacy* allowed "blanket seizure" of the defendant's "entire computer system." 119 F.3d 742, 746 (9th Cir. 1997). We reasoned that "no more specific description of the computer equipment sought was possible," because the agents "did not know whether the images were stored on the hard drive or on one or more of [the defendant's] many computer disks." *Id.*; *accord United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (holding, in a child pornography case, that "the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images"). Significantly, in both *Hay* and *Lacy* we carefully noted the critical role played by the officers' affidavits supporting the warrants. *See Hay*, 231 F.3d at 637 ("[T]he affidavit explained why it was necessary to seize the entire computer system in order to examine the electronic data for contraband. It also justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis."); *Lacy*, 119 F.3d at 746-47 ("In the affidavit supporting the search warrant application, a Customs agent explained there was no way to specify what hardware and software had to be seized to retrieve the images accurately.").

[8] By contrast, although the warrant in this case authorized a wholesale seizure, the supporting affidavit did not explain why such a seizure was necessary. *See United States v. Adjani*, ___ F.3d at ___ , 2006 WL 1889946 at *7 n.7 (noting favorably an affidavit's computer search and seizure protocol explaining when a computer had to be searched offsite, because "[s]uch specificity increases our confidence that the magistrate judge was well aware of what he was authorizing

and that the agents knew the bounds of their authority in executing the search"); U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 43, 69 (July 2002) (recommending that "if agents expect that they may need to seize a personal computer and search it off-site to recover the relevant evidence, the affidavit should explain this expectation and its basis to the magistrate judge. The affidavit should inform the court of the practical limitations of conducting an on-site search, and should articulate the plan to remove the entire computer from the site if it becomes necessary."); *cf. United States v. Tamura*, 694 F.2d 591, 596 (9th Cir. 1982) ("If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted by the magistrate issuing the warrant only where on site sorting is infeasible and no other practical alternative exists.").[11]

[9] We do not approve of issuing warrants authorizing blanket removal of all computer storage media for later examination when there is no affidavit giving a reasonable explanation, such as that provided in *Hay* and *Lacy*, as to why a wholesale seizure is necessary.[12] *See Tamura*, 694 F.2d at 595 ("[T]he wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intru-

[11]In retrospect, it is clear that not all the storage media needed to be seized as evidence of criminal activity; of the 154 disks seized, only two zip disks contained lascivious images of children. There is no evidence or allegation that the officers knew of this result before they searched and seized.

[12]As the defendant pointed out during oral argument, the magistrate must be made aware of what officers are contemplating and why they are doing so. For some people, computer files are the exclusive means of managing one's life — such as maintaining a calendar of appointments or paying bills. Thus, there may be significant collateral consequences resulting from a lengthy, indiscriminate seizure of all such files. As noted earlier, however, in this case the district court granted the defendant the right to "mirror copies" of the seized storage media. *See supra* n. 5.

sive, and has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent" (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980))). Without such individualized justification being presented to the magistrate, we cannot be sure that the judge was aware of the officers' intent and the technological limitations meriting the indiscriminate seizure — and thus was intelligently able to exercise the court's oversight function. An explanatory statement in the affidavit also assures us that the officers could not reasonably describe the objects of their search with more specificity. *See United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 2005) ("Generic classifications in a warrant are acceptable only when a more precise description is not possible." (internal quotation marks and citation omitted)); *see also Upham*, 168 F.3d at 535 ("Of course, if the [seized] images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of *all* computer equipment, a category potentially including equipment that contained no images and had no connection to the crime."). Accordingly, we hold that the warrant here was overbroad in authorizing a blanket seizure in the absence of an explanatory supporting affidavit, which would have documented the informed endorsement of the neutral magistrate. *See Tamura*, 694 F.2d at 596 ("The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate.").[13]

[10] Nonetheless, as in *Tamura*, we conclude that suppression of the evidence of child pornography found on the defendant's seized zip disks is not an appropriate remedy. *Tamura* involved an indiscriminate seizure of all files found in an

[13]The district court found no violation because it assumed the state judge must have known it was not technologically feasible to search onsite, and therefore the affidavit did not need to so provide. *See Hill*, 322 F. Supp. 2d at 1090. We do not think the record is so clear, and our case law requires more.

office even though the warrant authorized the officers to search for only three categories of records for evidence of various alleged crimes. *See id*. at 594-95. Although we refused to sanction the "wholesale *seizure* for later detailed examination of records not described in a warrant," *id.* at 595, we held that "the exclusionary rule does not require the suppression of evidence within the scope of a warrant simply because other items outside the scope of the warrant were unlawfully taken as well," *id*. at 597. *See also id*. ("Regardless of the illegality of the Government's seizure and retention of documents not covered by the warrant, however, reversal is not compelled in this case.").

[11] Similarly, the pornographic images from the defendant's zip disks that he sought to exclude as evidence at trial was "seized and retained lawfully because described in and therefore taken pursuant to the valid search warrant." *Id.* As we have discussed above, the officers' wholesale seizure was flawed here because they failed to justify it to the magistrate, not because they acted unreasonably or improperly in executing the warrant. Because the officers were "motivated by considerations of practicality rather than by a desire to engage in indiscriminate 'fishing,' we cannot say . . . that the officers so abused the warrant's authority that the otherwise valid warrant was transformed into a general one, thereby requiring all fruits to be suppressed." *Id. See also Hudson v. Michigan*, 547 U.S. ____, 126 S.Ct. 2159, 2163 (2006) ("Suppression of evidence . . . has always been our last resort, not our first impulse,"and is appropriate "only 'where its remedial objectives are thought most efficaciously served.' " (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)).

[12] Therefore, we hold that the district court properly admitted the evidence of child pornography found on the defendant's computer storage media notwithstanding the lack of a sufficiently detailed supporting affidavit describing the need for wholesale seizure of such media.

2. *Absence of Search Protocol*

[13] The defendant also argues that the search warrant was overbroad because it did not include a search protocol to limit the officers' discretion as to what they could examine when searching the defendant's computer media, nor did the affidavit explain why such a protocol was unnecessary. We, like the district court, find no error in the search warrant on this ground and adopt the district court's analysis:

> Defendant also argues that the warrant was overbroad because it did not define a "search methodology." He claims that the search should have been limited to certain files that are more likely to be associated with child pornography, such as those with a ".jpg" suffix (which usually identifies files containing images) or those containing the word "sex" or other key words.
>
> Defendant's proposed search methodology is unreasonable. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." *United States v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998). Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.
>
> Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating tal-

> cum from cocaine except by testing it. The ease with which child pornography images can be disguised — whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated — forecloses defendant's proposed search methodology.

Hill, 322 F. Supp. 2d at 1090-1091; *see also Adjani*, ___ F.3d at ___, 2006 WL 1889946 at *7 (rejecting defendants' argument that officers should have looked at only specified areas of certain email programs for enumerated keywords because "[t]o require such a pinpointed computer search, restricting the search to an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought").

[14] Moreover, in contrast to our discussion of the overbroad seizure claim above, there is no case law holding that an officer *must* justify the lack of a search protocol in order to support issuance of the warrant. As we have noted, we look favorably upon the inclusion of a search protocol; but its absence is not fatal. We have also held that even though a warrant authorizing a computer search might not contain a search protocol restricting the search to certain programs or file names, the officer is always "limited by the longstanding principle that a duly issued warrant, even one with a thorough affidavit, may not be used to engage in a general, exploratory search." *Id.* The 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. *See United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978) ("Where evidence is uncovered during a search pursuant to a warrant, the threshold question must be whether the search was confined to the warrant's terms. . . . [T]he search must be one directed in good faith toward the objects specified in the warrant or for other means and instrumentalities by which the

crime charged had been committed. It must not be a general exploratory search . . . ." (internal quotation marks omitted)).[14]

IV. *Conclusion*

We realize that judicial decisions regarding the application of the Fourth Amendment to computer-related searches may be of limited longevity. Technology is rapidly evolving and the concept of what is reasonable for Fourth Amendment purposes will likewise have to evolve. *See Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."); *cf. id.* at 41, 51 (Stevens, J., dissenting) (expressing concern with "the supposedly 'bright-line rule' the Court has created in response to its concerns about future technological developments" as it "is unnecessary, unwise, and inconsistent with the Fourth Amendment" and commenting that "[i]t would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues [of technology] rather than to shackle them with prematurely devised constitutional constraints"). New technology may become readily accessible, for example, to enable more efficient or pinpointed searches of computer data, or to facilitate onsite searches. If so, we may be called upon to reexamine the

[14]As we noted in *Adjani*, ____ F.3d at ____, 2006 WL 1889946 at *9, like the Tenth Circuit in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), we recognize that computer files are often intermingled and officers who have a warrant to seize evidence of a specific crime may come across evidence that implicates the defendant in another crime. *See also United States v. Walser*, 275 F.3d 981 (10th Cir. 2001). The proper steps for the officer to take in such a situation — when dealing with computer files — have not been clearly defined, and this case does not provide occasion to do so. *Cf. Tamura*, 694 F.2d at 595-96 ("In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search . . . .").

technological rationales that underpin our Fourth Amendment jurisprudence in this technology-sensitive area of the law.

That said, for the reasons set forth in this opinion, the search here was supported by probable cause and, notwithstanding the shortcomings of the search warrant affidavit, the manner of its execution does not mandate suppression of the fruits of that search. The district court's denial of the defendant's motion to suppress is therefore **AFFIRMED**.