FOR PUBLICATION
UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,	
Plaintiff,	No. CR 02-01289 AK
v.	
JUSTIN BARRETT HILL,	
Defendant.	**OPINION**

KOZINSKI, Circuit Judge.[*]

Defendant has been indicted on one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). He brings a series of pre-trial motions, raising the following issues: What must an affidavit allege to establish probable cause that images on a defendant's computer are child pornography? Is a warrant overbroad if it permits seizure of computer media without requiring that they be inspected at the scene? If it doesn't define the search methodology? Finally, are defense counsel and his expert entitled to copies

[*] Sitting by designation pursuant to 28 U.S.C. § 291(b).

of the computer media the government seized from defendant's home?

Facts

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, "[a]ll storage media belonging to either [the computer] or the individual identifying himself as [defendant] at the location," and "[a]ll sexually explicit images depicting minor[s] contained in [the storage media]." By the time the detective arrived at the store to execute the warrant, defendant had picked up his computer. Based on the computer technician's affidavit, the detective got 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] 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 that were eventually determined to contain images of child pornography; they 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. § 2252A(a)(5)(B).[3]

---

[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

(continued...)

At trial, the government will likely offer into evidence files from two zip diskettes recovered in the search. Defendant seeks to suppress this evidence on two grounds: (1) the affidavit on which the warrant was based did not establish probable cause to believe he was in possession of child pornography; and (2) the warrant was overbroad because it allowed seizure of all computer disks belonging to defendant regardless of whether they contained child pornography, and because

---

[2](...continued)
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).

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

knowingly possess[ing] 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.

it placed no limitations on the forensic examination of the disks that were seized. Defendant has also filed a motion for discovery, requesting "mirror image" copies of the computer media seized from him that are now in the government's possession.

Analysis

1. Not all nude pictures of children are child pornography: Only images containing "lascivious exhibition of the genitals or pubic area" qualify. 18 U.S.C. §§ 2256(8)(B), 2256(2)(B)(iii); see also Doe v. Chamberlin, 299 F.3d 192, 196 (3d Cir. 2002) ("Congress has chosen to criminalize only photos of the genitalia or pubic areas and of these parts only when they are the subject of 'lascivious exhibition.'"). To support issuance of the warrant, the affidavit had to establish probable cause that the images on defendant's computer were lascivious.

Lasciviousness[4] is an elusive concept, and courts have struggled to develop a test for identifying it.[5] The predominant test involves weighing six factors,

---

[4] Webster's defines "lascivious" as "[w]anton; lewd; lustful" or "[t]ending to produce voluptuous or lewd emotions." Webster's New International Dictionary 1395 (2d ed. 1939).

[5] "[The Ninth] circuit has held that 'lascivious' is a 'commonsensical term,' and that whether a given photo is lascivious is a question of fact. There is a consensus among the courts that whether the item to be judged is lewd, lascivious,

(continued...)

commonly known as the Dost factors: (1) whether the focal point of the visual depiction is the child's genitalia or pubic area; (2) whether the setting 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 for his age; (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; and (6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer. See United States v. Dost, 636 F. Supp. 828, 832 (S.D. Cal. 1986), aff'd sub nom. United States v. Wiegand, 812 F.2d 1239 (9th Cir. 1987).[6] While the Dost factors attempt to bring order and predictability to the lasciviousness inquiry, they are highly malleable and subjective in their application. Applying these factors to the two images described in the affidavit

---

[5](...continued)
or obscene is a determination that lay persons can and should make." United States v. Arvin, 900 F.2d 1385, 1390 (9th Cir. 1990) (citations omitted) (quoting United States v. Wiegand, 812 F.2d 1239, 1243–44 (9th Cir. 1987)).

[6] A number of other courts have relied on the Dost factors. See, e.g., Chamberlin, 299 F.3d at 196; United States v. Brunette, 256 F.3d 14, 17–18 & n.4 (1st Cir. 2001); United States v. Boudreau, 250 F.3d 279, 282–83 & n.2 (5th Cir. 2001); United States v. Moore, 215 F.3d 681, 686–87 (7th Cir. 2000); United States v. Horn, 187 F.3d 781, 789 (8th Cir. 1999); United States v. Amirault, 173 F.3d 28, 31–32 (1st Cir. 1999); United States v. Knox, 32 F.3d 733, 745–46 & n.10 (3d Cir. 1994); United States v. Wolf, 890 F.2d 241, 244–46 (10th Cir. 1989).

demonstrates their shortcomings.

The first Dost factor looks to whether the focal point of the image is the child's pubic area or genitalia. But it is not clear how this factor contributes to lasciviousness. A close-up image of female genitalia in a medical textbook will surely be less lascivious than a photograph showing the entire female body with the pubic area only partially visible. Nor is it easy to tell whether the genitalia are the focus of the picture. Do they need to be at or near the center? Does the subject or another person have to draw particular attention to them? In reality, exposed genitals tend to create their own focal point. Whether the genitals are the focus of the picture seems to involve as subjective an inquiry as lasciviousness itself.

The second Dost factor asks whether the setting is sexually suggestive, but what is a sexually suggestive setting? A bedroom might be the classic example, but that's also one of the most likely places where one might find a nude child. Defendant argues that the first image—the one of a girl about fifteen years old—is not lascivious in part because she is standing in a living room, not a bedroom. The government argues just the opposite: The fact that a fifteen-year-old girl is standing partially nude in the living room—a wholly inappropriate place for nudity—makes the pose sexually suggestive. Similarly, defendant contends that

the photograph of the young girls at the beach is not lascivious because the beach is not a sexually suggestive setting. But the beach—where even clothed people wear scanty bathing suits—can be a highly erotic location. Just ask Deborah Kerr and Burt Lancaster. See FROM HERE TO ETERNITY (Columbia Pictures Corp. 1953).

The third factor considers whether the pose or attire of the child is inappropriate. Courts applying this factor have mentioned garters, lingerie and high heels. See, e.g., United States v. Amirault, 173 F.3d 28, 33 (1st Cir. 1999) ("As the girl is naked, the issue of inappropriate attire is inapposite. But for what it is worth, she is wearing no sexually suggestive clothing such as garters, lingerie, or high heels."); United States v. Villard, 885 F.2d 117, 124 (3d Cir. 1989) ("[A] photograph of a naked girl might not be lascivious (depending on the balance of the remaining Dost factors), but a photograph of a girl in a highly sexual pose dressed in hose, garters, and a bra would certainly be found to be lascivious."). Defendant argues that bathrobes and shirts are not inappropriate, nor are the poses. The government counters that it is highly inappropriate for minor girls to pose wearing nothing but an open shirt and socks, or wearing open robes in a public area such as a beach. Nor, contends the government, are a shirt or robes less sexually provocative than garters and high heels; it's a matter of taste. This, too, is

a highly subjective and easily manipulated inquiry.

The fourth factor is whether the minor is fully or partially clothed. Again, there is no clear line between lascivious and non-lascivious. The girls described by the technician were all partially clothed, but their pubic areas and underdeveloped breasts were exposed. Once the genital area is exposed, covering other parts of the body may simply call attention to the parts that are uncovered. And, while an image of a fully-clothed minor engaged in sexual conduct could be lascivious, a family snapshot of a nude child bathing presumably would not.[7]

---

[7] In Knox, the Third Circuit held that nudity is not a prerequisite for child pornography:

> [A] "lascivious exhibition of the genitals or pubic area" of a minor necessarily requires only that the material depict some "sexually explicit conduct" by the minor subject which appeals to the lascivious interest of the intended audience. . . . [I]n the present case, it is readily apparent that the tapes . . . violate the statute. In several sequences, the minor subjects, clad only in very tight leotards, panties, or bathing suits, were shown specifically spreading or extending their legs to make their genital and pubic region entirely visible to the viewer. In some of these poses, the child subject was shown dancing or gyrating in a fashion indicative of adult sexual relations. Nearly all of these scenes were shot in an outdoor playground or park setting where children are normally found. Although none of these factors is alone dispositive, the totality of these factors leads us to conclude that the minor subjects were engaged in conduct—namely, the exhibition of their genitals or pubic area—which would appeal to the lascivious interest of an audience of pedophiles.

32 F.3d at 747.

The fifth Dost factor measures coyness or the minor's apparent willingness to engage in sexual activity. Almost any facial expression—or lack thereof—could fairly be described as one of these. A young girl looking straight at the camera, as in Image 1, could be perceived as willing to engage the viewer. But a naked child looking away from the camera, as in Image 2, or covering her face with her hands, could be coy. Not much help here.

Finally, the sixth Dost factor asks whether the conduct is intended to elicit a sexual response in the viewer. In other words, "[t]he final Dost factor simply puts again the underlying question: Is the exhibition lascivious?" Chamberlin, 299 F.3d at 196. This factor has no independent force.

A close look at the Dost factors persuades the court that the test is not particularly helpful. It is indeterminate even for a court that has pictures to analyze, and almost entirely useless to a magistrate asked to evaluate pictures he has never seen. The Ninth Circuit, too, has been skeptical of Dost, noting that "[t]he standard employed by the district court [in Dost] was over-generous to the defendant in implying as to the 17-year-old girl that the pictures would not be lascivious unless they showed sexual activity or willingness to engage in it." Wiegand, 812 F.2d at 1244. The court therefore adopts a different test, one that it believes better comports with the child pornography statute and provides more

meaningful guidance in evaluating lasciviousness: If an image of a minor displays the minor's naked genital area,[8] there is probable cause to believe that the image is lascivious unless there are strong indicators that it is not lascivious.[9]

---

[8] An image of a fully-clothed minor could still qualify as child pornography. For example, an image of a minor performing a simulated sex act might be lascivious, see note 7 supra, and images of actual sex acts certainly would be. However, the court need not consider what the test should be where the minor is fully clothed because the images at issue here involve genital nudity.

[9] The court is mindful that lasciviousness not only separates prohibited child pornography from legal images, it also divides protected from unprotected speech. See New York v. Ferber, 458 U.S. 747, 764 (1982) (requiring that a child pornography "offense be limited to works that visually depict sexual conduct by children below a specified age. The category of 'sexual conduct' proscribed must also be suitably limited and described." (footnote omitted)). Although this court's approach is preferable to the pliable Dost factors even at trial, the presumption could be misapplied to resolve close cases against a defendant, even where some indicators suggest an image is not lascivious. Later courts must therefore determine when the presumption can constitutionally be applied to prove lasciviousness at trial.

But, while the trier of fact reviews actual images to determine lasciviousness, judges evaluating probable cause—and courts reviewing those decisions—must work with probabilities, often without access to the images. See United States v. Wallace, 213 F.3d 1216, 1220 (9th Cir. 2000) ("The concept of probable cause is a 'fluid' one—it depends on an 'assessment of probabilities in particular factual contexts.'" (quoting Illinois v. Gates, 462 U.S. 213, 232 (1983))); see also Brinegar v. United States, 338 U.S. 160, 175 (1949) ("In dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act."). There is at least probable cause to conclude an image is lascivious when it exhibits a minor's bare genitalia, and weak or ambiguous indicators of an innocent purpose

(continued...)

In this case, there were no such indicators. The pictures are not part of a medical text. They do not appear to be bona fide artistic expression, nor do they depict a family setting where exposure of the genitals was incident to an innocuous activity such as swimming or horse-play. The girls in the two pictures posed for the apparent purpose of displaying their genitals to the viewer.

To determine whether probable cause existed, the judge had to "make 'a practical, commonsense decision whether, given all the circumstances set forth in the affidavit,' there [was] a fair probability that evidence of a crime [would] be found in a particular place." Id. at 1242 (citing Illinois v. Gates, 462 U.S. 213, 238 (1983)). The state court judge had before her an affidavit describing two images. Both descriptions involved minor girls with their bare breasts and pubic areas on display, which raised a presumption that the images were lascivious, and nothing indicated that the images were made for an innocent purpose. The judge had a substantial basis for concluding that there was probable cause for a warrant authorizing the search of defendant's home and seizure of evidence of child pornography. See Gates, 462 U.S. at 238–39.

2. Defendant argues that the warrant was overbroad because (a) it allowed

---

[9](...continued)
do not suggest otherwise.

seizure of all computer media without requiring inspection at the scene, even though the affidavit did not explain why such an inspection would not be feasible; and (b) it placed no limits or controls on the search methodology police used to analyze the seized media.

a. 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. The matter becomes more difficult if the police have cause to believe the records are not in English. Are the police required to bring with them at least one officer who can read the language of the documents and separate those that provide evidence of criminal activity from those that don't? The answer might turn on how readily the police can find an officer who is fluent in that language. In Los Angeles today, finding an officer who reads Spanish may be fairly easy, while finding one who can read Portuguese or Russian probably is not. Police are certainly not required to hire an expert translator to bring with them; they are entitled to limit the search team to officers already employed and reasonably available at the time the search is to be conducted.[10]

Returning to defendant's case, the court concludes that the police were not required to bring with them equipment capable of reading computer storage media

---

[10] Police are free to hire such experts to help them conduct a search, see, e.g., Forro Precision, Inc. v. IBM, 673 F.2d 1045, 1053–54 (9th Cir. 1982), and it may well be praiseworthy for them to do so. See, e.g., United States v. Tamura, 694 F.2d 591, 596 n.4 (9th Cir. 1982); see also United States v. Wuagneux, 683 F.2d 1343, 1353 (11th Cir. 1982) (lauding similar procedure as a way to "assure that [the search is] conducted in a manner that minimizes unwarranted intrusions into privacy." (internal quotation marks omitted)). But the Fourth Amendment does not require it.

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. See pages 23–24 infra. 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.

Because of these considerations, the court concludes that the police were not required to examine defendant's electronic storage media at the scene to determine which contained child pornography and which did not. They were entitled to seize all such media and take them to the police station for examination by an expert. Accord United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding, in a child pornography case, a warrant authorizing seizure of a defendant's entire computer system because the circumstances "justified taking the entire [computer] system off site because of the time, expertise, and controlled environment required for a proper analysis"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (holding, also in a case involving child pornography, that a warrant authorizing search and seizure of defendant's computer and all disks "was about the narrowest definable search and seizure reasonably likely to obtain the images" and that "a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs"); see also United States v. Lamb, 945 F. Supp. 441, 461–63 (N.D.N.Y. 1996) (holding that removal and off-site inspection is a reasonable approach for determining whether something is contraband when the determination cannot be

made on the spot).

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), is not to the contrary. Tamura involved a warrant authorizing seizure of three categories of business records. When FBI agents arrived to execute the warrant, they realized it would take a considerable time to separate the materials, so they seized all the company's accounting records for the period in question, whether covered by the warrant or not. They separated the seizable from the non-seizable materials later at the FBI offices. The Ninth Circuit held that the government's wholesale seizure of company documents was illegal because the agents intentionally seized materials they knew were not covered by the warrant. Here, by contrast, the officers were authorized by the warrant to seize all computer storage media—which is precisely what they did. Significantly, Tamura did not hold that a warrant would be too broad if it authorized wholesale seizure of materials that contain both evidence of crime and innocuous matter, if the two kinds of materials are too difficult or time-consuming to separate at the scene. To the contrary, the Tamura court suggested, albeit in dicta, that such a warrant would be appropriate:

> 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.

Id. at 596 (citing United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982)).

The warrant here authorized precisely such a seizure of intermingled materials that are difficult and time-consuming to separate on-site. That the officer seeking the warrant did not make a specific showing to this effect is of no consequence: The difficulties of examining and separating electronic media at the scene are well known. It is doubtless with these considerations in mind that the state court judge authorized seizure of all of defendant's storage media, not merely those containing contraband or evidence of crime.

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

3. The government intends to introduce into evidence "over 1,000 images of child pornography and/or child erotica," which it discovered on two 100 megabyte zip diskettes taken from defendant's home. The government's expert discovered the images through a comprehensive forensic computer analysis using "Encase" forensic software. Defendant wishes to obtain two "mirror image" copies of the computer media analyzed by the government's expert to allow his own expert to conduct a forensic analysis and his counsel to prepare his defense. The government opposes producing these items, offering instead to permit the

defense to view the media in an FBI office and to conduct its analysis in the government's lab.

Federal Rule of Criminal Procedure 16(a)(1)(E) provides:

> Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

Rule 16 clearly covers the items defendant has requested. They are "data, photographs, [and/or] tangible objects" within the government's possession. Moreover, they are material to the preparation of the defense, the government intends to use them in its case-in-chief and they were obtained from defendant. Rule 16(d)(1), however, allows the court to regulate discovery: "At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief."

The government argues that since child pornography is contraband, defense counsel and his expert should be required to examine the images in the controlled environment of the government facility. The cases cited by the government, though, all involve appeals from district court decisions denying a defendant's motion to compel production. They do not hold that a district court would abuse

its discretion if it were to order the government to produce copies of the materials. See, e.g., United States v. Kimbrough, 69 F.3d 723, 730–31 (5th Cir. 1995) (upholding the district court's denial of defendant's motion to compel production of a copy of a video containing child pornography); United States v. Horn, 187 F.3d 781, 792 (8th Cir. 1999) (upholding the district court's refusal to order the government to produce copies of videos alleged, and later found, to contain child pornography).

The government analogizes the zip disks to narcotics, arguing that their inspection and analysis by defendant's expert should take place in the government's lab under government supervision. This analogy is inapt. Analysis of a narcotics sample is a fairly straightforward, one-time event, while a thorough examination of the thousands of images on the zip disks will take hours, even days, of careful inspection and will require the ability to refer back to the images as the need arises.

The court concludes that defendant will be seriously prejudiced if his expert and counsel do not have copies of the materials. Defense counsel has represented that he will have to conduct an in-depth analysis of the storage media in order to explore whether and when the various images were viewed, how and when the images were downloaded and other issues relevant to both guilt and sentencing.

The court is persuaded that counsel cannot be expected to provide defendant with competent representation unless counsel and his expert have ready access to the materials that will be the heart of the government's case.

The government's proposed alternative—permitting the defense expert to analyze the media in the government's lab at scheduled times, in the presence of a government agent—is inadequate. The defense expert needs to use his own tools in his own lab. And, he cannot be expected to complete his entire forensic analysis in one visit to the FBI lab. It took defense counsel between two and three hours to quickly scroll through the 2,300 images in the Encase report, so it is likely to take the expert much longer than that to conduct a thorough analysis. Defendant's expert is located in another state, and requiring him to travel repeatedly between his office and the government's lab—and obtain permission each time he does so—is unreasonably burdensome. Moreover, not only does defendant's expert need to view the images, his lawyer also needs repeated access to the evidence in preparing for trial.

There is no indication that defendant's counsel or expert cannot be trusted with the material. The expert is a former government agent who has a safe in his office and has undertaken to abide by any conditions the court places on his possession of the materials. He has experience in dealing with child pornography

and takes precautions to ensure that contamination doesn't occur, including using the Encase software and fully "wiping" the forensic computers on which he examines the images. Defense counsel is a respected member of the bar of this court and that of the Ninth Circuit. The court has every confidence that he can be trusted with access to these materials.

After the court's oral ruling, the parties produced a stipulation setting forth procedures to be employed by defense counsel and his expert in the handling of these materials, and the court has adopted it as its order. Because the court believes that these safeguards provide a useful framework for how such materials can be handled, the relevant portion of the stipulation is reproduced as an appendix to this opinion.

* * *

The facts alleged in the affidavit were sufficient for the state court judge to conclude that there was probable cause; the warrant she issued was not overbroad. Defendant's motion to suppress is therefore DENIED. Defendant's motion for discovery is GRANTED.

_____

Alex Kozinski
United States Circuit Judge

DATED: June 17, 2004

Counsel

Teresa Mack, Assistant United States Attorney, Los Angeles, California, argued for the government.

Carlton F. Gunn, Deputy Federal Public Defender, Los Angeles, California, argued for defendant.

APPENDIX

GOOD CAUSE HAVING BEEN SHOWN, IT IS HEREBY ORDERED:

1. The government shall provide defendant's counsel (the Office of the Federal Public Defender) a copy of the 3 zip diskettes, 1 CD-ROM and 5 floppy diskettes (collectively referred to as "the retained computer evidence") currently in the custody of the FBI, necessarily including any and all actual or alleged child pornography and/or contraband contained thereon. Defense counsel shall maintain copies of the retained computer evidence as follows:

    a. Copies of the retained computer evidence shall be maintained by defense counsel in accordance with this Order, and shall be used by counsel and employees of the Federal Public Defenders' Office designated by defense counsel solely and exclusively in connection with this case (including trial preparation, trial and appeal).

    b. Copies of the retained computer evidence shall be maintained by defense counsel in a locked file or cabinet at all times, except while being actively utilized as provided for in this Order.

    c. A copy of this Order shall be kept with the copies of the retained computer evidence at all times.

    d. Copies of the retained computer evidence shall be accessed and viewed only by defense counsel and staff employed by defense counsel.

    e. Defendant himself shall not be permitted to access or view any graphic image file containing actual or alleged child pornography, on copies of the retained evidence or in the Encase evidence files, without petition and prior order of this Court. However, defendant may access and view non-image data contained on copies of the retained computer evidence for the purpose of assisting in the preparation of his defense in the presence of counsel and under the direct supervision and control of counsel.

f. Any computer into which copies of the retained evidence may be inserted for access and operation shall not be connected to a network while a copy of the retained evidence is inserted into any computer.

g. The computer into which copies of the retained evidence are inserted may be connected to a printer only under the following conditions: that any printer utilized is a local printer, that the printer may be connected only when and as necessary to print non-graphic image files, and that defense counsel or staff employed by defense counsel shall be personally present at all times a printer is connected.

h. In no event shall any graphic image containing actual or alleged child pornography be copied, duplicated, or replicated, in whole or in part, including duplication onto any external media.

2. The government shall provide defendant's expert, Marcus K. Lawson of Global Compusearch, LLC, a copy of all of the Encase evidence files relating to this case, which includes evidence files for all media seized from [address deleted] on April 6, 2000, necessarily including any and all actual or alleged child pornography and/or contraband contained thereon. Mr. Lawson shall maintain and secure the Encase evidence files in the following manner:

a. Copies of the Encase evidence files shall be maintained by Mr. Lawson in accordance with this Order, and shall be used by Mr. Lawson solely and exclusively in connection with this case.

b. Copies of the Encase evidence files shall be maintained by Mr. Lawson in a locked safe in the offices of Global Compusearch, LLC at all times, except while being actively utilized as provided for in this Order.

c. A copy of this Order shall be kept with the copies of the Encase evidence files at all times.

d. Copies of the Encase evidence files shall be accessed and viewed only by Mr. Lawson and staff employed by Global Compusearch,

LLC who Mr. Lawson has given this Order to and who agree to be bound by the requirements of this protective order.

e. Mr. Lawson shall maintain custody over the Encase evidence files and shall maintain a list of all Global Compusearch, LLC employees granted access to the Encase evidence files.

f. Any computer into which copies of the Encase evidence files may be inserted for access and operation shall not be connected to a network while a copy of the Encase evidence files is inserted into any computer.

g. The computer into which copies of the Encase evidence files are inserted may be connected to a printer only under the following conditions: that any printer utilized is a local printer, that the printer may be connected only when and as necessary to print non-graphic image files, and that Marcus Lawson or staff employed by Global Compusearch who are subject to this Order shall be personally present at all times a printer is connected.

h. In no event shall any graphic image containing actual or alleged child pornography be copied, duplicated, or replicated, in whole or in part, including duplication onto any external media.

3. Within 30 days of termination of this matter (including the termination of any appeal), defense counsel shall return (or cause the return of) copies of the retained computer evidence and the Encase evidence files to Special Agent Tim Alon or a representative of the Federal Bureau of Investigation. Upon the return of the copies of retained evidence and the Encase evidence files, defense counsel shall file a brief report to the Court specifying that the terms of this Order have been complied with and reporting the return of the copies of evidence.

IT IS SO ORDERED.