RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit Rule 206

File Name: 11a0282p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee/Cross-Appellant,

v.

TIMOTHY RYAN RICHARDS,
Defendant-Appellant/Cross-Appellee.

Nos. 08-6465/6503

Appeal from the United States District Court
for the Middle District of Tennessee at Nashville.
No. 05-00185-001—Aleta Arthur Trauger, District Judge.

Argued: January 21, 2011

Decided and Filed: October 24, 2011

Before: SILER, MOORE, and GRIFFIN, Circuit Judges.

COUNSEL

ARGUED: Kimberly S. Hodde, HODDE & ASSOCIATES, Nashville, Tennessee, for Appellant. John-Alex Romano, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee. **ON BRIEF:** Kimberly S. Hodde, HODDE & ASSOCIATES, Nashville, Tennessee, for Appellant. John-Alex Romano, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., S. Carran Daughtrey, ASSISTANT UNITED STATES ATTORNEY, Nashville, Tennessee, for Appellee.

GRIFFIN, J., delivered the opinion of the court, in which SILER, J., joined. MOORE, J. (pp. 35–46), delivered a separate opinion concurring in the judgment only.

OPINION

GRIFFIN, Circuit Judge. Defendant Timothy Ryan Richards appeals his convictions by a jury on eleven child-pornography related offenses, in violation of 18 U.S.C. §§ 2251(a) and (d)(1)(A); 18 U.S.C. §§ 2252A(a)(1), (a)(5)(B), and (b)(1);

and 18 U.S.C. § 2257(f)(4). The government cross-appeals as substantively unreasonable Richards' below-Guidelines sentence of sixteen years of imprisonment, to be followed by eight years of supervised release. For the reasons that follow, we affirm Richards' convictions and sentence.

I.

The government's investigation of defendant Richards began in July 2005, when a nineteen-year-old "adult performer" named Justin Berry contacted the Federal Bureau of Investigation ("FBI"), offering to provide information about the commercial production, advertising, sale, and distribution of child pornography videos. Berry gave this information under a limited grant of use immunity for his statements, which led to the arrest and prosecution of Richards and two other individuals, Gregory Mitchel and Aaron Brown.

The ensuing FBI investigation revealed that Richards was engaged in the production and distribution of child pornography. Despite his youth,[1] Richards was a sophisticated pornography entrepreneur, operating at least a dozen websites that contained sexually explicit conduct involving adults and minors, pornographic images of boys under eighteen, and advertisements for or links to other child pornography sites.[2] Some of these websites, such as CaseyandDew.tv, did not show visual pornography but did contain video discussions about sexual activity. In addition, Richards managed and operated other pornography-related websites, including billing sites.[3] He profited handsomely from these websites, using advertising techniques such as sending out e-mail solicitations, setting up discounts for customers who visited multiple websites, offering standard and premium membership plans, using an on-line credit card

[1]Richards was twenty-four years of age when he was indicted and charged in October 2005.

[2]The websites that displayed sexual images of boys under the age of eighteen included www.CaseyandKylesCondo.com, www.CaseyandDew.tv, www.CaseysApartment.com, www.CaseysCondo.com, www.Condodollars.com, www.JustinsFriends.com, and www.JustinsFriends.net.

[3]These websites included www.CollegeBoysLive.com, www.KylesRoom.com, www.PenisClub.com, www.TorysLife.com, www.WebCamFam.com, www.Nimenet.com, and www.NimeBill.com.

processing company for membership payments, and, to dissuade customers from unsubscribing, requiring the customers to watch a fifteen-minute video before being permitted to terminate their memberships.[4]

To manage the large amount of computer data, Richards kept several computers in his home in Nashville, Tennessee, and utilized multiple servers in California that contained approximately one terabyte (a thousand gigabytes) of information. Server log records indicated that shortly after assuming control of the JustinsFriends.com website in July 2005, Richards logged into the server that controlled the website from the internet protocol address tied to his home in Nashville, Tennessee, and uploaded child pornography to the JustinsFriends.net site.

Richards, who used the online alias "Casey Masterson," appeared in many videos in which he engaged in sexually explicit conduct with a then-minor child named Patrick Lombardi, a/k/a "Kyle." Richards befriended and began dating Lombardi in May of 2000, when Richards was almost nineteen and Lombardi was fourteen years old. Their relationship continued for four years. During this time period, Richards produced and made available on the internet recorded images of Lombardi engaged in sexually explicit conduct when Lombardi was fifteen years old. Richards produced a digital file and a videotape – "Casey@16" – of himself and Lombardi engaging in sexual acts. Richards also took sexually explicit photos of Lombardi and engaged in repeated sexual contact with him when they traveled to Australia in 2002 and Iceland in 2003.

Shortly before Lombardi's eighteenth birthday, Richards and Lombardi planned a new website – CaseyandKylesCondo.com – on which they intended to show homosexual pornography with links to photos, journals, and videos. Richards registered the internet domain for this website in his own name, created the content, advertised for it, and made it part of his affiliate marketing program. According to Lombardi, Richards purposefully waited until Lombardi turned eighteen to launch the website, which

[4]The FBI's investigation revealed that Richards received over $64,000 in credit card payments, although the government was unable to distinguish which portion of this revenue was attributable specifically to child pornography, as opposed to adult pornography, which was also available on the websites.

included pornography of Lombardi when he was a minor. The CaseyandKylesCondo.com website was hosted on a server in Los Angeles operated by BlackSun Technologies (the "BlackSun server"). After their relationship ended, Lombardi signed a release that allowed Richards to keep the depictions of him, and thereafter Richards alone controlled the website and its contents. In January 2005, Richards registered the CaseysCondo.com domain name, and that site eventually replaced CaseyandKylesCondo.com. The CaseysCondo.com site included the explicit photographs of Lombardi in Australia.

Another website, JustinsFriends.com, was a homosexual pornographic website featuring Justin Berry and other male models. The website was originally run by Berry and Gregory Mitchel, but Berry sought out Richards' assistance in running the website. Richards agreed to help in exchange for a percentage of the profits, and he eventually took over JustinsFriends.com in July 2005 in the wake of a falling out between Berry and Mitchel. Richards transferred the website to the BlackSun server and changed the site's internet domain to JustinsFriends.net, which was registered in his name. Like his other websites, Richards offered access to the sexually explicit content for a fee. The contents of JustinsFriends.net included a version of the Iceland video of Lombardi and Richards and depicted the sexual activity of another minor, "Taylor." Federal agents saw the latter video playing in the free section of JustinsFriends.net in July 2005, during their investigation.

On September 12, 2005, agents executed a search warrant for the BlackSun server in Los Angeles, which had been identified as the host for JustinsFriends.com and JustinsFriends.net. On the same date, agents also executed a search warrant for a server in the San Francisco area (the "Hurricane Electric server"), which had hosted JustinsFriends.com and was associated with Aaron Brown. Ten days later, on the basis of information provided by Berry and Mitchel, Richards was arrested at his Nashville home. Agents then executed search warrants for the Nashville residence and a second residence to which Richards was moving. The seized items included eight computers, cameras, videotapes (including the "Casey@16" video), and documents. The subsequent

search of the BlackSun server revealed that the JustinsFriends websites were stored in one of two hard drives on the server, along with several of Richards' websites containing pornography and child pornography.

In October 2005, the government returned a single count indictment charging Richards with the distribution of child pornography. Other charges were added and, ultimately, in September 2006, a twenty-seven count third superseding indictment was issued, charging Richards with various child-pornography offenses: four counts of distribution (via the internet), in violation of 18 U.S.C. § 2252A(a)(1); seven counts of advertising, in violation of 18 U.S.C. § 2251(d)(1)(A); four counts of production, in violation of 18 U.S.C. § 2251(a)(1); four counts of possession, in violation of 18 U.S.C. § 2252A(a)(5)(B); two counts of conspiring to advertise, contrary to 18 U.S.C. § 2251(e); one count of conspiring to distribute, contrary to 18 U.S.C. § 2252(A)(b)(1); four counts of record-keeping violations under 18 U.S.C. § 2257(f)(4); and one count of transferring obscene material to a minor, in violation of 18 U.S.C. § 1470.

Pertinent to the present appeal, the district court denied Richards' pretrial motions to suppress the fruits of the searches and seizures of the computer servers; to compel compliance with the court's order requiring the government to identify images to be used in its case-in-chief; and to dismiss counts in the indictment as multiplicitous.

The trial commenced on October 10, 2006. At trial, the defense did not dispute the fact that Richards operated the various websites. The defense challenged the government's assertion that the pornography on the websites actually depicted minors and that Richards knew of their status as minors. Lombardi testified as a prosecution witness that he was a minor when the videos were made; Richards testified on his own behalf that Lombardi and the other alleged minors, Taylor and Tory, were eighteen years of age when the images and videos were recorded.

Six of the twenty-seven counts were dismissed and not submitted to the jury. On October 26, the jury convicted Richards on eleven counts – three transportation counts, three advertising counts, two record-keeping counts, one conspiracy to transport count,

one production count, and one possession count. The jury acquitted Richards on the remaining ten counts.

With a total offense level of 48 and a Category I criminal history, the recommended Guidelines sentence was life imprisonment. On November 7, 2008, the district court sentenced Richards to 16 years of imprisonment, 8 years of supervised release, and a special assessment of $1,100. Richards now timely appeals his convictions, and the government cross-appeals the sentence, which it asserts is too lenient and substantively unreasonable.

II.

A.

Richards first contends that the district court erred in denying his motion to suppress evidence obtained from the search of the BlackSun computer server because the search warrant was overbroad under the Fourth Amendment and the search exceeded the scope of probable cause set forth in the warrant.

On September 12, 2005, FBI Special Agent Monique Winkis applied in the Western District of Virginia for a warrant to seize and search the BlackSun server.[5] Specifically, her 27-page affidavit that was cross-referenced in the application for the search warrant requested permission to search the BlackSun server "for the contents of the websites known as justinfriends.com and/or justinfriends.net and stored wire and electronic communications and transactional records that may be evidence of violations of [18 U.S.C. §§] 2251, 2252, and 2252A, including the advertising, possession, transportation, and distribution of child pornography. . . ." Agent Winkis recounted in detail the course of the investigation, starting with Justin Berry's initial voluntary contact with law enforcement regarding the commercial production and distribution of on-line child pornography and the website that he started at age 13, justinsfriends.com. The affidavit explained Justin Berry's developing interest in the internet and his relationship

[5]Richards does not challenge the search warrant for the Hurricane Electric server.

with Gregory Mitchel, who had a sexual relationship with Berry when Berry was a minor; Mitchel later produced child pornography videos featuring Berry and the minor, Taylor, that were uploaded onto the JustinsFriends.com website and could be previewed from the site.

Agent Winkis stated that federal agents made an undercover purchase of a membership to JustinsFriends.net after being redirected there by the JustinsFriends.com website, where they saw, inter alia, sexually-explicit videos of Berry and Taylor, both minors at the time. The company that processed memberships for the JustinsFriends websites advertised its name as "Neova.net." Further investigation identified BlackSun as the web hosting company for the websites; this information was confirmed by BlackSun representatives. The BlackSun facility in Los Angeles, California, has 2,000 servers; investigators discovered that the particular server in question, which hosted both JustinsFriends.com and JustinsFriends.net was located "in cabinet 200.02, server number 4 and has a sticker on it that states collegeboyslive."

In her affidavit, Winkis stated that James Fottrell, the Manager of the High Technology Investigative Unit in the Child Exploitation Section of the U.S. Department of Justice, informed her that upon approval and execution of the search warrant, the contents of the server and/or hard drives hosting the JustinsFriends.com and JustinsFriends.net websites would be "imaged" (exact copies made) so that their contents could be examined at an FBI field office and other locations following completion of the on-site search. Fottrell further advised Winkis that "the entirety of the unallocated space of the servers on which materials relating to IP address 66.54.91.171 are found should be searched because the unallocated space of those servers is likely to contain relevant evidence of materials that have been deleted or otherwise moved from the servers." Agent Winkis represented that "[i]t is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which expert possesses sufficient specialized skills to best obtain the evidence and subsequently analyze it," but "[n]o matter which method is used, . . . data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even hidden,

erased, compressed, password-protected, or encrypted files." Any content or materials unrelated to the investigation would be erased or deleted from the government storage devices within a reasonable time. On the basis of the foregoing information, Agent Winkis submitted that

> probable cause exists to conclude that servers found in cabinet 200.02, server 4, located at BlackSun, . . . contains content associated with the websites www.justinsfriends.com and www.justinsfriends.net and have been used to facilitate the production, possession, receipt and distribution (sale) of child pornography in violation of [18 U.S.C. §§ 2251, 2252, and 2252A]. Further, that there is probable cause to believe that evidence of such criminal offenses is currently located on the server used by www.justinsfriends.com and www.justinsfriends.net and located in cabinet 200.02, server 4 . . . as specifically set forth in Attachment A to the Search Warrant.

Attachment A described the BlackSun premises and the specific server to be searched, "cabinet number 200.02, server number 4." Attachment B listed the items to be seized:

> 1. All content of the justinsfriends.com and/or justinsfriends.net servers at BlackSun 1200 West 7th Street, Los Angeles, California 90017, including any computer files that were or may have been used as a means to advertise, transport, distribute, or possess child pornography, . . . as well as any child pornography images.
>
> 2. All business records, in any form, which pertain to the justinsfriends.com and/or justinsfriends.net account and its use of IP address 66.54.91.171, to include all e-mail, ICQ communications, log files of any and all activity, or other communications sent by or received by the account holders, directly, or indirectly, whether saved or deleted, and any and all credit card numbers or other methods or identifiers used to pay for the account, including, but not limited to:
>
> a. e-mail and other correspondence between BlackSun and the individual or entity that created and/or controls the website known as justinsfriends.com and/or justinsfriends.net;
>
> b. any and all transactional records including File Transfer Protocol (FTP) if available, HTTP logs, port 80 logs, and logs including the dates and times the customer uploaded content to the website known as justinsfriends.com and/or justinsfriends.net; and

> c. any records of customer service complaints made to BlackSun concerning the website known as justinsfriends.com and/or justinsfriends.net.
>
> d. any records of subscribers to the justinsfriends.com and/or justinsfriends.net website(s).

(Emphasis removed.)[6]

On September 12, 2005, a magistrate judge issued the warrant, which on its face authorized a search of "BlackSun, 66.54.91.171, Server # 4, Cabinet # 200.02, 1200 West 7th Street, Los Angeles, CA 90017." It was executed that same day, with the eventual search yielding some of Richards' child-pornography websites on Server # 4.

Richards moved to suppress the fruits of the seizure and search of the BlackSun server on the grounds that the warrant authorized seizing only those sections of the server hosting JustinsFriends.com and JustinsFriends.net; alternatively, if the warrant did in fact authorize seizure of the entire server, then the warrant was unconstitutionally overbroad.

At the suppression hearing convened by the district court, James Fottrell, the government's expert, testified that the BlackSun server was a commercial web server, which provided configuration for websites and "serve[d] up" those webpages for computers requesting access through the internet. Each website's files were stored in the server's directory, either in a folder structure that distinguishes between websites or in an "intermeshed" structure that contains elements common to the websites. Each server had an operating system and an account for an administrator, who had access to and complete control over the files stored on the server. Each website operator had control over the website and the file directories associated with it, but could not alter content on other sites or in other directories unless that operator was also the administrator of the server. A server may also provide individual users with storage space and a directory structure; such content would be accessible by the administrator.

---

[6]Both Attachments and the affidavit are cross-referenced and incorporated in Agent Winkis's application and affidavit for the search warrant.

Fottrell's examination of the entire server after its seizure revealed that JustinsFriends.net was stored in one of two hard drives on the server, along with six other websites, including Richards' CandKcondo.com, PenisClub.com, CaseysCondo.com, Premium.ckcondo.com, and CollegeBoysLive.com. Fottrell found an administrator account and user accounts for "Casey" and "Aaron" on the server. At the time of the suppression hearing, he had not yet detected any "locks or barriers" at the web site level on the server that would have precluded users from accessing the entire server, and he confirmed that the BlackSun administrator had unfettered access to the server.

Fottrell explained that he would not restrict his search for child pornography offenses to the folders associated with the JustinsFriends websites, but would search the entire server because, in his experience, individuals intentionally mislabel directory structures to hide the presence of child pornography and thus store it in other locations on the server. Moreover, servers have unallocated space, which might contain deleted files, log records, relevant e-mails, and there may be commonalities with the credit card transaction processors, advertising, or shared links. Thus, without looking at individual server files, Fottrell would not know whether any of the websites were related.

At the conclusion of the hearing, the district court denied Richards' motion to suppress. Noting that Richards conceded that unallocated server space could be searched, the court found probable cause to search the entire server because: (1) the agents did not know how many websites were on the server before seizing it; and (2) the server administrator had access to all of the sites and, therefore, "could have secreted in any other websites [or in the unallocated space] information relevant to the investigation concerning the child pornography contained on the [JustinsFriends websites]." The court concluded that the search warrant was not impermissibly overbroad.

B.

When reviewing the denial of a motion to suppress, we review the district court's findings of fact for clear error and its conclusions of law de novo, considering the evidence in the light most favorable to the government. *United States v. Lucas*, 640 F.3d 168, 173 (6th Cir. 2011). We review de novo a district court's determination of particularity. *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001). "The proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure." *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978).

The Fourth Amendment guarantees the right of liberty against unreasonable searches and seizures by providing:

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

U.S. Const. amend. IV.

"It is well-settled that items to be seized pursuant to a search warrant must be described with particularity to prevent the seizure of one thing under a warrant describing another in violation of the Fourth Amendment." *United States v. Wright*, 343 F.3d 849, 863 (6th Cir. 2003) (citation and internal quotation marks omitted). "The chief purpose of the particularity requirement [is] to prevent general searches by requiring a neutral judicial officer to cabin the scope of the search to those areas and items for which there exists probable cause that a crime has been committed." *Baranski v. Fifteen Unknown Agents of the Bureau of Alcohol, Tobacco and Firearms*, 452 F.3d 433, 441 (6th Cir. 2006). As we stated in *Ellison v. Balinski*, 625 F.3d 953 (6th Cir. 2010), "the history of the Fourth Amendment [demonstrates that it] was enacted in part to curb the abuses of general warrants, devices which provided British officers with broad discretion to search the homes of citizens of the Colonies for evidence of vaguely specified

crimes." *Id*. at 958; *see also Steagald v. United States*, 451 U.S. 204, 220 (1981) (discussing the history of the Fourth Amendment).

The particularity requirement may be satisfied through the express incorporation or cross-referencing of a supporting affidavit that describes the items to be seized, even though the search warrant contains no such description. *Id.* at 439-40. "[T]he degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought." *Greene*, 250 F.3d at 477; *see also Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("A search warrant must particularly describe the things to be seized, but the description, whose specificity will vary with the circumstances of the case, will be valid if it is as specific as the circumstances and the nature of the activity under investigation permit.") (internal quotation marks omitted).

"The cases on particularity are actually concerned with at least two rather different problems: one is whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take; and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized." *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (citations and internal quotation marks omitted). It is the latter problem – overbreadth – that is alleged by Richards in this case. "[I]nfirmity due to overbreadth does not doom the entire warrant; rather, it requires the suppression of evidence seized pursuant to that part of the warrant . . . , but does not require the suppression of anything described in the valid portions of the warrant . . . ." *Greene*, 250 F.3d at 477 (internal quotation marks omitted).

We recently observed, in the context of determining that the search of a defendant's laptop computer did not exceed the scope of his consent to search his home, that

> analogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life. . . . . [T]here is a far greater potential "for the 'intermingling' of documents and a consequent invasion of privacy when police execute a

> search for evidence on a computer." *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001).

United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011); *see also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) ("The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.").[7]

Courts that have addressed the permissible breadth of computer-related searches have grappled with how to balance two interests that are in tension with each other:

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

United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011) (citation and internal quotation marks omitted).

Our court has not yet had occasion to confront this issue in depth. Ultimately, however, given the unique problem encountered in computer searches,[8] and the practical difficulties inherent in implementing universal search methodologies, the majority of

---

[7] *Cf. United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (recognizing that "email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve").

[8] *See United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010) ("Undoubtedly the warrant's description serves as a limitation on what files may reasonably be searched. The problem with applying this principle to computer searches lies in the fact that such images could be nearly anywhere on the computers. Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents.").

federal courts have eschewed the use of a specific search protocol[9] and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis: "While officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant, . . . a computer search may be as extensive as reasonably required to locate the items described in the warrant based on probable cause." *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir.), *cert. denied*, 130 S. Ct. 1028 (2009) (citations and internal quotation marks omitted). We agree with the Tenth Circuit's succinct assessment in *Burgess* that

> it is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives. One would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to "file cabinets in the basement" or to file folders labeled "Meth Lab" or "Customers." And there is no reason to so limit computer searches. But that is not to say methodology is irrelevant.
>
> A warrant may permit only the search of particularly described places and only particularly described things may be seized. As the description of such places and things becomes more general, the method by which the search is executed become[s] more important – the search method must be tailored to meet allowed ends. And those limits must be functional. For instance, unless specifically authorized by the warrant there would be little reason for officers searching for evidence of drug trafficking to look at tax returns (beyond verifying the folder labeled "2002 Tax Return" actually contains tax returns and not drug files or trophy pictures).
>
> Respect for legitimate rights to privacy in papers and effects requires an officer executing a search warrant to first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure. That is the purpose of a search protocol which structures the search by requiring an analysis of the file structure, next looking for suspicious file folders, then looking for files and types of files most likely to contain the objects of the search by doing keyword searches.

---

[9] *See Stabile*, 633 F.3d at 238-39; *Mann*, 592 F.3d at 785-86; *United States v. Burgess*, 576 F.3d 1078, 1092, 1094 (10th Cir. 2009); *United States v. Cartier*, 543 F.3d 442, 447-48 (8th Cir. 2008); *United States v. Khanani*, 502 F.3d 1281, 1290 (11th Cir. 2007); *United States v. Hill*, 459 F.3d 966, 977 (9th Cir. 2006); *United States v. Adjani*, 452 F.3d 1140, 1149-50 (9th Cir. 2006); *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005); *Guest*, 255 F.3d at 335; and *Upham*, 168 F.3d at 535.

> But in the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files. It is particularly true with image files.

Id. at 1094 (footnote omitted).

As is the case with paper documents, on occasion in the course of a reasonable search, investigating officers may examine, "at least cursorily," some "innocuous documents . . . 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); *see also Stabile*, 633 F.3d at 234 (applying *Andresen* to a computer search); *United States v. Banks*, 556 F.3d 967, 973 (9th Cir. 2009) (holding that search warrant for a computer and other items, for evidence of child pornography, was not overbroad, noting, "[a] generalized seizure of business documents may be justified if it is demonstrated that the government could not reasonably segregate . . . documents on the basis of whether or not they were likely to evidence criminal activity") (citation and internal quotation marks omitted).[10]

Applying a reasonableness analysis on a case-by-case basis, the federal courts have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers. *See, e.g.*, *Stabile*, 633 F.3d at 239 (determining that the search of a computer folder was objectively reasonable because "criminals can easily alter file names . . . to conceal contraband" and the officer "took steps to ensure that his investigation complied with the state search warrant"); *Banks*, 556 F.3d at 973 (holding that warrant to search personal computer for items connected to "child pornography" or "minors engaged in sexually explicit conduct" was not overbroad because the warrant sought only evidence of child pornography and no more limited search would have been feasible); *United States v. Summage*, 481 F.3d 1075, 1079-80

[10]Consistent with this rule, the federal courts have not required a second warrant to search a properly seized computer where the evidence obtained in the search did not exceed the probable cause articulated in the original warrant. *See United States v. Gregoire*, 638 F.3d 962, 967-68 (8th Cir. 2011); *Grimmett*, 439 F.3d 1263, 1268-69 (10th Cir. 2006); *Upham*, 168 F.3d at 535; *United States v. Simpson*, 152 F.3d 1241, 1248 (10th Cir. 1998).

(8th Cir. 2007) (finding that a warrant authorizing broad search of personal computer for child pornography was sufficiently particular where, at the time the warrant was sought, "the officers knew only that a video and photographs of the alleged incident supposedly existed, not the particular format in which these items were being kept"); *Grimmett*, 439 F.3d at 1269-70 (rejecting the defendant's particularity challenge to a warrant authorizing the search of "any computer equipment" in a child pornography investigation); *Upham*, 168 F.3d at 535 ("A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs."); *cf*. *Guest*, 255 F.3d at 336 (rejecting particularity challenge to the seizure and off-site search of entire computers and their contents in an obscenity investigation because "the warrants required that the communications and computer records pertain to the listed offenses" and "[d]efendants could not have obtained more specific identification of e-mails and subscriber data, which were not accessible to them").[11]

In other words, in general, "[s]o long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence." *United States v. Roberts*, No. 3:08-CR-175, 2010 WL 234719, at *15 (E.D. Tenn. Jan. 14, 2010) (quoting *United States v. Jack*, No. S-07-0266, 2009 WL 453051, at *4 (E.D. Cal. Feb. 29, 2009)). Under the

[11]In addition, *see United States v. Meeks*, 290 F. App'x 896, 903 (6th Cir. 2008) (warrant for computer-related equipment, discs, records and notes, and diaries related to child pornography was "as specific as the circumstances allowed, given the information investigators had" and therefore was not overbroad); *United States v. Clark*, 257 F. App'x 991, 992 (6th Cir. 2007) (holding that warrant to search and seize the defendant's whole computer met the particularity requirement because the affidavit created probable cause to believe that he used the computer to obtain and store images of child pornography); *United States v. Simpson*, 152 F.3d 1241, 1248 (10th Cir. 1998) ("We are aware of no authority finding that computer disks and hard drives are closed containers somehow separate from the computers themselves, and similar warrants authorizing the search of computer systems and components have been upheld."); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (warrant authorizing seizure of entire personal computer system was sufficiently specific where it contained "objective limits to help officers determine which items they could seize – allowing seizure only of documents linked to [a specific child pornography computer bulletin board system]"). *Cf. United States v. Sherman*, 372 F. App'x 668, 676 (8th Cir. 2010) ("The search warrant necessarily needed to include all computer equipment and systems to effectively allow law enforcement to recognize and seize the materials described [in the warrant alleging fraudulent billing practices].") (citation and internal quotation marks omitted).

facts of the present case, this principle should be applied to Richards' computer *server* as well.

C.

Like the district court, we find no ambiguity in the search warrant's authorization to seize and search the entire server. The warrant identified "BlackSun 66.54.91.171, Server # 4, Cabinet #200.02" at the BlackSun facility address. Attachment B to the warrant listed, as one of the items to be seized, "[a]ll content of the justinsfriends.com and/or justinsfriends.net servers at BlackSun . . . including any computer files that were or may have been used as a means to advertise, transport, distribute, or possess child pornography[.]" In her cross-referenced affidavit, Agent Winkis stated that there was "probable cause to believe that evidence of [the child pornography] offenses is currently located on the server used by www.justinsfriends.com and www.justinsfriends.net and located in cabinet 200.02, server 4[.]" She requested permission to search for "the contents of the websites known as justin[s]friends.com and/or justin[s]friends.net and stored wire and electronic communications and transactional records that may be evidence of [child pornography offenses]." Clearly, the warrant and supporting documents did not restrict the seizure and search only to those portions of the server containing the JustinsFriends websites. *See Greene*, 250 F.3d at 477-78 ("the language of a warrant is to be construed in light of an illustrative list of seizable items") (citation and internal quotation marks omitted).

Nor was the warrant overbroad. Richards argues that the BlackSun server was set up in a neatly compartmentalized and segregated fashion, rendering it entirely unnecessary to search beyond the content maintained in the JustinsFriends file directory. However, hindsight is 20/20. At the time of the seizure, agents did not know how and where the JustinsFriends-related content would be stored on the server. Richards does not dispute that the government had probable cause to believe that the JustinsFriends websites involved child pornography. Agent Winkis's affidavit explained that "[i]t is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which expert possesses sufficient specialized skills to best

obtain the evidence and subsequently analyze it." It also indicated that a forensic procedure could uncover "even hidden, erased, compressed, password-protected, or encrypted files." Therefore, as explained by James Fottrell, searching the entire server was necessary to look for child pornography related to the JustinsFriends websites because individuals often mislabel directory files, the server might contain related websites, and the unallocated server space might contain materials pertaining to those websites.

Although Richards contends that the warrant failed to distinguish between "shared" and "dedicated" servers, Agent Winkis explained that distinction in her affidavit. In any event, before the search, investigators did not know whether the server was shared or dedicated, and, if shared, whether any websites were related, whether users had access to the entire server, or how the directory was organized. The trial evidence confirmed that the websites on the server were related through cross-promotion and use of the same images and videos, and that the user "Casey" (Richards) had administrative rights over the BlackSun server to control all the contents associated with that server. However, it was only *after* the search that Fottrell discovered that the JustinsFriends content was separated from the other sites and divided into distinct file directories. "The prohibition of general searches is not to be confused with a demand for precise ex ante knowledge of the location and content of evidence . . . . The proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation." *United States v. Meek*, 366 F.3d 705, 716 (9th Cir. 2004).

In light of the information known at the time the search warrant was issued, we hold that it was not unconstitutionally overbroad. The scope of the warrant was restricted to a search for evidence of child pornography crimes and did not permit a free-ranging search. *See Banks*, 556 F.3d at 973 ("[T]he affidavit explained why it was necessary to seize the entire computer system in order to examine the electronic data for contraband . . . and the warrant did not authorize [] seizure of every document, but of child pornography which is a sufficiently specific definition to focus the search.")

(citation and internal quotation marks omitted). Significantly, Richards does not claim that the search process was abused by the federal agents. The search was carried out in a controlled manner, not in "flagrant disregard for the limitations of [the] warrant." *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988); *see also Grimmett*, 439 F.3d at 1270 ("There is no evidence of exploratory rummaging through files, or inadvertent discoveries."). Certainly, the suggestive name of at least one of Richards' pornographic websites on the server – PenisClub.com – was a red flag that the additional contents of the server might be tied to child pornography offenses. Thus, the search of the entire contents of the server was objectively reasonable under the circumstances.

Out of over 2,000 servers at the BlackSun facility, investigators pinpointed the specific IP address and server that hosted the JustinsFriends websites – "BlackSun 66.54.91.171, Server #4, Cabinet # 200.02" – and in conducting their search and seizure, did not exceed the bounds of reasonableness required by the Fourth Amendment.

D.

Moreover, for the sake of argument, were the warrant overbroad, we hold in the alternative that suppression of the evidence is not required under the *Leon* good-faith exception, "which allows admission of evidence 'seized in reasonable, good-faith reliance on a search warrant that is subsequently held to be defective.'" *United States v. Paull*, 551 F.3d 516, 523 (6th Cir. 2009) (quoting *United States v. Leon*, 468 U.S. 897, 905 (1984)). "The *Leon* Court based its refusal to suppress evidence in such situations on its conclusion that 'the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion.'" *United States v. Hodson*, 543 F.3d 286, 292 (6th Cir. 2008) (quoting *Leon*, 468 U.S. at 922). *Leon* made clear that only in exceptional circumstances is law enforcement to disregard a magistrate judge's authorization – for instance, when a warrant is "so lacking in indicia of probable cause as to render official belief in its existence unreasonable[,]" or when a warrant is "so facially deficient that it could not reasonably be presumed valid." *Hodson*, 543 F.3d at 292 (citations and internal quotation marks omitted).

Neither of these exceptions applies here. Agent Winkis's affidavit explained in detail the facts establishing probable cause to believe that child pornography was distributed through JustinsFriends.net. Further, the warrant was not "so facially deficient" in describing the items to be seized that the agents could not reasonably presume it to be valid. *See United States v. Potts*, 586 F.3d 823, 834 (10th Cir. 2009) (applying *Leon* good-faith exception where reasonable officers could have read the warrant's multiple references to child pornography in attachment to apply to the entire warrant). The affidavit set forth why it was necessary to image the server. Hence, this is not a situation where "even a cursory reading of the warrant . . . would have revealed a glaring deficiency that any reasonable police officer would have known was constitutionally fatal." *Groh v. Ramirez*, 540 U.S. 551, 564 (2004).

III.

Next, Richards contends that the government's initial refusal to identify the pornographic images embraced by the charges, and its subsequent identification of over 20,000 images, constitutes an obfuscation of the letter and intent of Federal Rule of Criminal Procedure 16(a)(1)(E), which requires the government, upon a defendant's request, to permit the defendant to inspect, inter alia, documents and photographs that the government intends to use in its case-in-chief at trial or that are material to preparation of the defense. Fed. R. Crim. P. 16(a)(1)(E)(i) and (ii).

Rule 16 "is intended to prescribe the minimum amount of discovery to which the parties are entitled, and leaves intact a court's discretion to grant or deny the broader discovery requests of a criminal defendant." *United States v. Jordan*, 316 F.3d 1215, 1249 n.69 (11th Cir. 2003) (citation and internal quotation marks omitted). If a party fails to comply with Rule 16, the district court has discretion to impose a number of sanctions – it may order discovery, grant a continuance, exclude the undisclosed evidence, or enter any other order that is just under the circumstances. *United States v. Jordan*, 544 F.3d 656, 667 (6th Cir. 2008) (citing Fed. R. Crim. P. 16(d)(2)). We review an alleged violation of Rule 16 for abuse of discretion. *Warshak*, 631 F.3d at 296; *United States v. Clark*, 385 F.3d 609, 619 (6th Cir. 2004).

On April 5, 2006, pursuant to the district court's order granting defendant's motion to compel production of discovery, the government provided Richards with copies of the hard drives seized from his computers and from the BlackSun and Hurricane Electric servers. On May 19, 2006, Richards moved for an order requiring the government to identify the images it would use in its case-in-chief. The district court granted the motion, ordering the government to identify the images by August 25, 2006. The government complied, identifying 20,429 computer files.

This information was provided in a flexible digital format, Microsoft Excel, and included the corresponding file path and file source for each identified file. The government also provided Richards with a "hash" value for each file and a database of the hash values of all the images on the servers in Microsoft Access database format, which could be used to identify duplicate images. Counsel for the government consulted with Richards' attorney on August 25, August 28, and again on August 30, 2006, and provided detailed explanations and guidance about the images and the evidence anticipated for trial. The government identified the child victims, previewed the nature of the charges in the impending superseding indictment, and responded to defense counsel's queries about specific files.

On August 30, 2006, the defense filed a motion to compel the government to comply with the identification order, complaining that the government had provided a list of over 20,000 files, rather than what the defense believed was required – "a list of a dozen or so files/images with a corresponding representation of which files/images relate[d] to each count in the Indictment." In response, the government offered to answer defense counsel's future questions about specific files and stated that it did not intend to show 20,000 images at trial, but planned to introduce "restored websites, each of which require[d] the use of thousands of the files listed," and to display some images and identify the multiple places where the images were found. The district court denied defendant's motion to compel, noting that the government had complied with its order.

The issue arose again on the second day of the October 2006 trial, when a federal agent testified about the images and videos found on the BlackSun server. Defense counsel objected that it was impossible to know, in advance, whether the images had been previously identified by the government. The district court ordered the government to preview with defense counsel the images it would show to the jury. Consequently, during a recess, the parties reviewed the exhibits and the government provided an exhibit list. When the trial resumed, defense counsel successfully objected to the introduction of several exhibits that were not included on the August list, but again expressed frustration about the sheer volume of images and being "swamped with trying to pick the needle out of the haystack . . . ."

Recently, in *Warshak*, we rejected the defendants' contention that the district court abused its discretion under Rule 16 by allowing the government to turn over millions of pages of electronic discovery evidence in an allegedly "disorganized and unsearchable format":

> [D]efendants cite scant authority suggesting that a district court must order the government to produce electronic discovery in a particular fashion. Furthermore, it bears noting that Federal Rule of Criminal Procedure 16, which governs discovery in criminal cases, is entirely silent on the issue of the form that discovery must take; it contains no indication that documents must be organized or indexed. Thus, if we are to find that the district court abused its discretion, we must do so despite a pronounced dearth of precedent suggesting that the district court was wrong.
>
> There are a number of factors that counsel against such a finding. First, the overwhelming majority of the discovery at issue was taken directly from [the defendants' company's] computers, which means the defendants had ready access to that information. . . .
>
> Furthermore, . . . an expert witness who testified for the defense indicated that, with the use of certain software, he could perform "very quick and thorough" searches of the electronic discovery. Consequently, it does not appear that the discovery materials were nearly as unsearchable as the defense purports.
>
> Lastly, it should be observed that the government did provide the defense with something of a guide to the electronic discovery. In response to the defense's discovery request, the government furnished the defendants

> with a detailed room-by-room inventory of all items seized from the company, including a listing of the various computers that were imaged. That listing surely offered the defendants some aid in identifying and marshaling the documents relevant to the litigation. Accordingly, we decline to hold that the district court abused its discretion in failing to order the government to produce discovery in a different form.

Warshak, 631 F.3d at 296-97 (footnotes, citation, and internal quotation marks omitted); *see also United States v. Prince*, 618 F.3d 551, 561-62 (6th Cir. 2010) (rejecting the defendant's claim under Rule 16(a)(1)(E)(ii) that the district court abused its discretion by not requiring the government to specifically identify the exhibits it intended to introduce at trial from among the estimated 70,000 pages of discovery materials that were provided to the defendant); *Jordan*, 316 F.3d at 1253 (rejecting the defendant's Rule 16 challenge that the government's discovery was so massive that it hindered their pretrial preparation, and observing: "The discovery was indeed voluminous – because the Government gave the defense access to far more information and materials than the law required. The defendants could hardly complain about that. If they had insufficient time to sort things out, they should have asked for a continuance.").

Similarly, we find no abuse of discretion in the district court's denial of Richards' motion to compel identification of evidence under Rule 16. Richards conceded in his pretrial motion for identification of images that Rule 16(a)(1)(E)(ii) does not require separate identification of the government's case-in-chief evidence. Moreover, there is no evidence that the government acted in bad faith and "attempted to obfuscate the relevant documents by burying them without direction under an avalanche of irrelevant materials." *United States v. Perraud*, No. 09-60129-CR, 2010 WL 228013, at *11 (S.D. Fla. Jan. 14, 2010) (unpublished) (holding that further identification of the government's proffered 5,000 documents was not required under Rule 16(a)(1)(E) where the government separately directed the defendants to materials it deemed most relevant, provided an indexed searchable database, and offered to

provide its exhibit list and hard copies of the exhibits prior to the start of trial).[12] Quite to the contrary, six weeks before trial, the government, as ordered by the district court, timely provided a comprehensive, indexed list of the images and files to Richards' attorney. The majority of the identified files were contained in a handful of computer subdirectories, and the government worked to facilitate the defense's review of the files both before and during the trial. Thus, the government fulfilled – indeed exceeded – its obligations under Rule 16, and reasonably accommodated Richards, who could have, but did not, ask for a continuance.

IV.

Richards also appeals, on hearsay grounds, the district court's ruling admitting into evidence certain age-labeled discs containing pornographic images of Lombardi when he was allegedly a minor. The images and videos of Lombardi, produced by Richards during their relationship, were placed on separate discs by the government. In preparation for trial, a federal agent interviewed Lombardi as to his age and the location where each image or video was filmed. The discs were then labeled accordingly with Lombardi's age at production ("16-17" and "17") and the location, and each disc was initialed by Lombardi and the agent. The images and videos were shown to the jury during the agent's testimony.

Defense counsel objected to both the premature admission and display of the images and the labeling on the discs. The government responded that the labels would be authenticated by Lombardi's subsequent testimony and explained that it showed the videos when the agent testified so that Lombardi would not have to view the pornography of himself in front of the jury. The district court provisionally admitted the images, but ordered that the labels must be excised before the discs went to the jury.

---

[12] *Cf. Warshak*, 631 F.3d at 297-98 (noting that "evidence that the government 'padded' an open file with pointless or superfluous information to frustrate a defendant's review of the file might raise serious . . . issues [under *Brady v. Maryland*, 373 U.S. 83 (1963)]," but there was "no proof that the government larded its production with entirely irrelevant documents," "made access to the documents *unduly* onerous," or "deliberately concealed any exculpatory evidence in the information it turned over to the defense") (citation, internal quotation marks, and footnotes omitted).

On direct examination, Lombardi identified his handwriting on ten discs, the content of and his age in each image, and confirmed that he had reviewed each image with the agent. Defense counsel then cross-examined Lombardi about his age in particular images and videos. At the conclusion of Lombardi's testimony, the district court opined that the labels had been adequately authenticated and allowed the labeled discs to be admitted and submitted to the jury during deliberations. In doing so, the court overruled defense counsel's objection to the purported "imprimatur . . . of seeing those ages written on there" and his fear that the jury "may attach too much significance" to the labels, noting that defense counsel had cross-examined and impeached Lombardi.

Richards now argues that the labeling on the discs was inadmissible hearsay, emphasizing that he was convicted on several child-pornography counts directly related to Lombardi's testimony that he was underage at the time the videos were made. Richards concedes, however, that a hearsay objection to the contents of the labels was never raised below and, therefore, our review of this issue is limited to plain-error analysis. *See United States v. Knowles*, 623 F.3d 381, 385 (6th Cir. 2010) ("A district court's decision to admit evidence in a jury trial that is objected to for the first time on appeal is subject to plain error review."). The plain error exception to the contemporaneous-objection rule is to be used solely in those circumstances in which a miscarriage of justice would otherwise result. *Id.* "For us to correct an error not raised at trial: (1) there must be error; (2) the error must be plain; and (3) the error must affect substantial rights." *Id.* (citations omitted). If these conditions are met, we "may then exercise [our] discretion to notice a forfeited error, but only if (4) the error seriously affect[s] the fairness, integrity, or public reputation of judicial proceedings." *Id*. at 385-86 (citation and internal quotation marks omitted). Here, we find no such plain error in the district court's determination that redaction of the labels was unnecessary.

In *United States v. Bentley*, 489 F.3d 360 (D.C. Cir. 2007), the jury, in a prosecution for firearm and drug possession offenses, asked to see the drug evidence during its deliberations. *Id*. at 362. A deputy marshal inadvertently delivered not only the drugs, which had been admitted into evidence, but also the labels attached to the bags

of drug evidence, which had not been admitted. *Id.* The labels – pre-printed forms filled out by the police after the search of the defendant's residence – listed the defendant's name and address, his physical description, details about the charged offense, and a description of the materials inside each bag. *Id.* at 365. The *Bentley* court held that "because the labels were merely cumulative of properly admitted evidence, even if they constituted hearsay, their inadvertent delivery to the jury was harmless." *Id.* The court also rejected the defendant's argument that the labels were nonetheless prejudicial because they provided a "'neat condensation' of the government's theories[,]" stating: "[T]he testimony of the officer who filled in the labels made clear that he did so merely to preserve the chain of custody of their contents. The jury was therefore aware that the labels served only an administrative function, rather than as an expression of the government's theory of the defendant['s] liability." *Id.*

Bentley's rationale is equally applicable here. Lombardi's age at the time of production of the images was, without question, a pivotal issue in this case. However, the agent and Lombardi both verified the accuracy of the information on the labels, and Lombardi provided direct testimony concerning his age at the time the videos were made. Defense counsel countered by cross-examining Lombardi about his age in the specific videos; in addition, Richards testified at trial that Lombardi was eighteen when the images were made. The age-labeling on the discs thus became cumulative evidence which, as made clear to the jury, served a limited record-keeping purpose. In submitting the discs to the jury, the district court rightly ruled that the jury was capable of deciding for itself whether the images depicted Lombardi as a minor. In fact, the jury acquitted defendant on three counts which were based on videos from age-labeled discs, but convicted defendant on six other counts related to Lombardi's claim that he was underage. Under these circumstances, Richards has failed to demonstrate plain error affecting his substantial rights as a result of submission of the age-labeled discs to the jury.

V.

Next, Richards argues that the district court erred in denying his motion to dismiss Counts 1 and 16 as multiplicitous, in violation of the Double Jeopardy Clause of the Fifth Amendment. Counts 1 and 16 charged him with transporting child pornography via CaseyandKylesCondo.com and CaseysCondo.com, respectively, in violation of 18 U.S.C. § 2252A(a)(1). According to Richards, because CaseysCondo.com and CaseyandKylesCondo.com were simply renamed versions of the same website, and purportedly never co-existed or overlapped in operation, his separate prosecution on these counts "is tantamount to charging 2 counts of mortgage fraud involving the same house which is distinguished only by a change of paint color" and constitutes impermissible multiple punishments for the same offense. We disagree.

"Whether an indictment suffers from a problem of duplicity or multiplicity is a legal question that this Court reviews *de novo*." *United States v. Swafford*, 512 F.3d 833, 844 (6th Cir. 2008). "Generally, an indictment may not charge a single criminal offense in several counts without offending the rule against 'multiplicity' and implicating the double jeopardy clause." *United States v. Davis*, 306 F.3d 398, 417 (6th Cir. 2002) (citation and internal quotation marks omitted). Where an indictment includes more than one count charging the same statutory violation, the question is whether Congress intended the facts underlying each count to constitute a separate unit of prosecution. *Swafford*, 512 F.3d at 844. "The inquiry as to what constitutes the correct unit of prosecution focuses in part on the identification of the key element of the federal offense." *United States v. Esch*, 832 F.2d 531, 541 (10th Cir. 1987).

Section 2252A(a)(1) provides that it is unlawful for any person to "knowingly mail[], or transport[] or ship[] using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, *any* child pornography[.]" 18 U.S.C. § 2252A(a)(1) (emphasis added). A reasonable interpretation of this broadly worded statute is that the transportation of child pornography through two different websites constitutes distinct violations punishable as separate offenses. *Cf. United States v. Hinkeldey*, 626 F.3d 1010, 1012-14 (8th Cir.

2010) (holding that the defendant's rights under the Double Jeopardy Clause were not violated by the district court's refusal to treat the six counts of possession of child pornography under 18 U.S.C. § 2252A(a)(5)(B) as one for sentencing purposes, where the indictment charged one possession count each for images stored on his computer, zip drive, and four computer disks); *United States v. Schales*, 546 F.3d 965, 979 (9th Cir. 2008) ("[W]here a defendant has stored sexually explicit images in separate mediums, the government may constitutionally charge that defendant with separate counts for each type of material or media possessed."); *United States v. Planck*, 493 F.3d 501, 504 (5th Cir. 2007) ("[W]here a defendant has images stored in separate materials (as defined in 18 U.S.C. § 2252A), such as a computer, a book, and a magazine, the Government may charge multiple counts, each for the type of material or media possessed, as long as the prohibited images were obtained through the result of different transactions."); *United States v. Gallardo*, 915 F.2d 149, 151 (5th Cir. 1990) ("With respect to the child pornography statute [18 U.S.C. § 2252(a)(1)], each separate use of the mail to transport or ship child pornography should constitute a separate crime because it is the act of either *transporting or shipping* that is the central focus of this statute. [The defendant] mailed four separate envelopes containing child pornography, thus committing four separate acts of transporting or shipping.").[13]

Consistent with the logic that the possession, receipt, or distribution of child pornography on different mediums or computer devices constitutes separate offenses, the use of distinct websites to transport child pornography likewise is not redundant for double jeopardy purposes.

---

[13]*See also United States v. Martin*, 278 F. App'x 696, 697 (8th Cir. 2008) (unpublished) (holding that the defendants' two convictions under 18 U.S.C. § 2252A(a)(5)(B) were not multiplicitous where the defendant "stipulated to possessing multiple disks containing pornographic images of children"); *United States v. Reedy*, 304 F.3d 358, 367-68 (5th Cir. 2002) (where the defendants charged with transporting pornography under § 2252(a)(1) were intermediaries operating a website security screening device, counts should have been grouped by website rather than by individual images); *United States v. Esch*, 832 F.2d 531, 541-42 (10th Cir. 1987) (holding that each sexually explicit photograph of children amounted to a separate and distinct sexual exploitation under 18 U.S.C. § 2251(a) and, therefore, an indictment charging separate counts for each photograph was not multiplicitous, even though the photos depicted the same children and were produced in the same photo session).

Here, despite Richards' claim to the contrary, CaseyandKylesCondo.com and CaseysCondo.com were not the same website. Although CaseysCondo.com eventually replaced CaseyandKylesCondo.com, the government's expert, James Fottrell, emphatically disagreed that the two websites were one and the same. The domain names were different and therefore required separate acts of registration, which occurred when Richards discontinued use of the CaseyandKylesCondo.com site, first registered in January 2003, and replaced it with the CaseysCondo.com website in early 2005. Fottrell opined that, although these two websites drew content from the same folder on the BlackSun server, it did not necessarily mean they were the same website – the sites could have operated at the same time and drawn different images from the same folder because they were on different domains. Fottrell testified that e-mails recovered from customers of these websites were consistent with the sites' simultaneous operation at some point in time prior to the government's seizure.

Moreover, in his effort to attract new customers, Richards marketed CaseysCondo.com as a new and different entity. On the site, he recounted his history of operating pornographic sites, including CaseyandKylesCondo.com, and stated that his "current website was born" when, in September of 2004, he returned from Amsterdam and "decided to do things differently."

Based upon this evidence, the district court did not err in denying Richards' motion to dismiss Counts 1 and 16 as multiplicitous. We agree fully with the government that punishing, through multiple offenses, a defendant who funnels child pornography through different websites is consistent with Congress's intent to halt the dissemination of such images and to stop the sexual abuse of children. *See New York v. Ferber*, 458 U.S. 747, 759-60 (1982) ("The distribution of photographs and films depicting sexual activity by juveniles is intrinsically related to the sexual abuse of children. . . . The most expeditious if not the only practical method of law enforcement may be to dry up the market for this material by imposing severe criminal penalties on persons selling, advertising, or otherwise promoting this product."); *cf. United States v. McNerney*, 636 F.3d 772, 777, 780 (6th Cir. 2011) (taking note of "Congress' significant

purpose in prohibiting the dissemination of child pornography" in holding that "duplicate digital images, like duplicate hard copy images, should be counted separately for purposes of calculating a sentence enhancement pursuant to [U.S.S.G.] § 2G2.2(b)(7)]").

VI.

Richards' remaining arguments are also without merit. He contends that the district court violated the Confrontation Clause by precluding him from cross-examining and impeaching a prosecution witness – an adult performer and former friend – about his previous sexual acts involving minors. The district court did not abuse its discretion in determining that the witness's sexual encounters with minors were of peripheral relevance to the case. *See United States v. Reid*, 625 F.3d 977, 986 (6th Cir. 2010) ("The district court retains wide latitude insofar as the Confrontation Clause is concerned to impose reasonable limits on such cross-examination based on concerns about, among other things, harassment, prejudice, confusion of the issues, the witness' safety, or interrogation that is repetitive or only marginally relevant.") (citation and internal quotation marks omitted).

Lastly, Richards' cursory argument alluding to cumulative error has no merit because "cumulative-error analysis is not relevant where no individual ruling was erroneous." *United States v. Deitz*, 577 F.3d 672, 697 (6th Cir. 2009).

VII.

The government cross-appeals Richards' sentence of sixteen years' imprisonment and eight years of supervised release on the ground that it is substantively unreasonable. With a total offense level of 48 and a Category I criminal history, the advisory Guidelines range was life imprisonment.

We review the district court's sentencing decision for substantive reasonableness under a deferential abuse-of-discretion standard. *United States v. Jones*, 641 F.3d 706, 711 (6th Cir. 2011) (citing *Gall v. United States*, 552 U.S. 38, 51 (2007)). "'A sentence is substantively unreasonable if the district court selects a sentence arbitrarily, bases the

sentence on impermissible factors, fails to consider relevant sentencing factors, or gives an unreasonable amount of weight to any pertinent factor.'" *United States v. Camiscione*, 591 F.3d 823, 832 (6th Cir. 2010) (quoting *United States v. Lapsins*, 570 F.3d 758, 772 (6th Cir. 2009)). The Supreme Court in *Gall v. United States*, 552 U.S. 38 (2007), "reject[ed]. . . an appellate rule that requires 'extraordinary' circumstances to justify a sentence outside the Guidelines range" and "also reject[ed] the use of a rigid mathematical formula that uses the percentage of a departure as the standard for determining the strength of the justifications required for a specific sentence." *Gall*, 552 U.S. at 47. However, the Court "permit[ted] district and appellate courts to require some correlation between the extent of a variance and the justification for it," *United States v. Grossman*, 513 F.3d 592, 596 (6th Cir. 2008), explaining that if a sentencing judge "decides . . . an outside-Guidelines sentence is warranted, he must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance," *Gall*, 552 U.S. at 50. Naturally, "a major departure should be supported by a more significant justification than a minor one." *Id.*

We "must give due deference to the district court's decision that the § 3553(a) factors, on a whole, justify the extent of the variance. The fact that the appellate court might reasonably have concluded that a different sentence was appropriate is insufficient to justify reversal of the district court." *Gall*, 552 U.S. at 51.

Pointing out that Richards' sixteen-year term of imprisonment is only one year more than the mandatory minimum sentence that he faced on the child-pornography production count alone, *see* 18 U.S.C. § 2251(a) and (e), the government argues that: (1) the district court's downward variance was excessive and fails to reflect the seriousness of Richards' overall offense conduct, which included not only the production of child pornography, but also its advertisement and the distribution for profit of more than 600 images through multiple websites; (2) the court unduly minimized the gravity of Richards' crimes when it noted that they involved adolescent boys, rather than younger victims or girls; (3) the court did not give appropriate consideration to uncharged conduct which entailed Richards' sexual relationship with a thirteen-year-old

boy, "Doe," with whom Richards was living at the time of his arrest; (4) the court gave undue weight to certain factors in Richards' history and circumstances to the exclusion of others – for instance, finding regret in Richards when his post-arrest conduct in jail showed neither remorse nor acceptance of responsibility, and viewing Richards as a victim himself based upon Richards' claim that he had been "tricked" into pornography; and (5) the sentence does not adequately protect minors from further sexual predation by Richards.[14]

Certainly there are troubling aspects in the district court's sentencing rationale, particularly its mitigation of the seriousness of Richards' actions, by noting that his relationship with minors was to a certain extent consensual behavior. That said, we disagree with the government that the district court abused its sentencing discretion. The sentencing record shows that in its oral and written statement of reasons, the court thoroughly addressed and weighed the parties' arguments for and against a variance, including Richards' post-arrest and uncharged conduct, considered the relevant sentencing factors, and clearly understood its sentencing options. In summarizing all of these considerations, the court provided justification – albeit reflecting a different perspective on Richards than the government – for the downward variance:

> In the court's view, this defendant has serious mental health issues related to his addictions and his different, identifiable internet persona, "Casey." With addiction treatment, mental health treatment, and sex offender treatment, the court has hope that this young man, "stopped in his tracks at 24" (the government's words) from engaging in illegal child pornography activity, can reform and lead a productive life after 16 years of incarceration. The defendant is a gay man who will remain a gay man, but his taste for sex with adolescents must be changed. If 16 years of sex offender, mental health and addiction treatment cannot change that pattern, certainly 30 or 40 years has no better chance of doing so. And following his period of incarceration, he will be on an extensive period

[14]The PSR reported that in 2005, Richards was living with a thirteen-year-old boy ("Doe"), whom he met through Doe's mother. In January 2004, Richards married Doe's mother in Las Vegas, Nevada, and indicated on his 2006 prison medical questionnaire that he was married. At the sentencing hearing, a federal agent testified that Richards blogged from jail (apparently through an outsider) on a website he created about his sexual relationships with Lombardi, Doe, and another inmate. The government also presented evidence in the form of sexually explicit e-mail communications and photos indicating that Richards was sexually involved with the minor Doe. In addition, the government produced Richards' jail record, which showed disciplinary infractions.

> of supervised release, with sex offender special conditions that put substantial limitations on his freedom and provide more opportunity for treatment and close supervision of his activities.
>
> This sentence is sufficient but not greater than necessary to accomplish the goals of sentencing. It reflects the seriousness of the offense, will promote respect for the law and be just punishment for the offenses of this defendant. It will provide the defendant with needed treatment for a substantial period of time, which should provide an adequate deterrence to further criminal conduct on the part of this defendant, who has no criminal record, and hopefully will protect the public from further crimes of this defendant during his 16 years in prison and 8 years of close supervision after he is released.

"It is the essence of discretion that it may properly be exercised in different ways and likewise appear differently to different eyes." *United States v. Andrews*, 633 F.2d 449, 465 (6th Cir. 1980) (en banc) (Engel, J., dissenting). As in other cases, "[w]hile we cannot say that this is the sentence we would have given, neither can we say that this variance exceeded the discretion *Gall* gives district court judges." *United States v. Beach*, 275 F. App'x 529, 535 (6th Cir. 2008) (holding in transportation and receipt of child pornography case that downward variance to 96 months' imprisonment from a Guidelines range of 210 to 240 months was not substantively unreasonable under the circumstances).

Here, as in *Grossman*, "[t]he district court never lost sight of the sentence recommended by the guidelines and gave ample reasons for reducing the sentence as far as he did." *Id*. at 597. Our reminder in *United States v. Vonner*, 516 F.3d 382 (6th Cir. 2008), is apt here:

> *Booker* empowered district courts, not appellate courts and not the Sentencing Commission. Talk of presumptions, plain error and procedural and substantive rules of review means nothing if it does not account for the central reality that *Booker* breathes life into the authority of district court judges to engage in individualized sentencing within reason in applying the § 3553(a) factors to the criminal defendants that come before them. . . . [T]he central lesson . . . [is] that district courts have considerable discretion in this area and thus deserve the benefit of the doubt when we review their sentences and the reasons given for them.

Vonner, 516 F.3d at 392; *see also United States v. Guthrie*, 557 F.3d 243, 256 (6th Cir. 2009) ("District courts enjoy discretion in sentencing based on their ring-side perspective on the sentencing hearing and [their] experience over time in sentencing other individuals. Accordingly, we do not presume to read the mind of a sentencing judge, on a search for impropriety.") (citation and internal quotation marks omitted); *Paull*, 551 F.3d at 529 ("Far from being impermissible or inadequate, [the] analysis of the considerations the court found most important – the defendant's circumstances and the seriousness of the crime – is just the sort of balancing a sentencing court should be doing.").

Following our deferential review, we hold that Richards' sixteen-year sentence was not an abuse of discretion and therefore affirm it.

VIII.

For the foregoing reasons, we affirm Richards' convictions and sentence.

CONCURRING IN THE JUDGMENT ONLY

KAREN NELSON MOORE, Circuit Judge, concurring in the judgment only. I write separately because I would affirm the district court solely on the basis of the good-faith exception to a subsequently invalidated warrant. I agree with the majority's conclusion that the search warrant explicitly authorized the search of the entire server. I disagree, however, that the Federal Bureau of Investigation ("FBI") had probable cause to search the entire server. The majority's analysis applies our case law on searches of personal computers to searches of shared space without a moment's pause to consider the differences between the two. The rule announced by the majority would authorize the government to invade the privacy of any number of unidentified individuals or companies without any probable cause, just because they may, without their knowledge, share server space with suspected criminals.

I. WARRANT LACKED PROBABLE CAUSE TO SEARCH ENTIRE SERVER

A company like BlackSun provides web hosting services to other parties by allowing them to make use of its servers. A server is a computer that provides services to other computers; web servers, for example, send web pages to a computer when a user enters a specific URL[1] into his or her browser. R. 87-1 (BlackSun Aff. at ¶ 8(a)). Web servers at a place like BlackSun can be "shared," meaning one server may host "multiple websites of unrelated companies," *id.* at ¶ 8(h), or one company or individual can lease an entire server. In such instances, the leasing company may use the server solely for its own websites, or it may in turn sublease the space to other unaffiliated websites just as BlackSun does.

[1]"URL" stands for uniform resource locator. A URL identifies a specific page within a website, such as http://www.justinsfriends.net/members. *See Interactive Prods. Corp. v. a2z Mobile Office Solutions, Inc.*, 326 F.3d 687, 691 (6th Cir. 2003).

On any given server, there can be any number of user accounts with varying levels of access. Each server has an administrative account to access the whole server; each website has an individual operator account to access just the website's directory. The government wants to analogize a server to a house with many open rooms. The appellant wants to analogize a server to an apartment with many locked units. Depending on how the server is set up, either of these analogies may hold true.

Two hypothetical servers may be useful to illustrate this point.[2] Hypothetical Server A is owned by BlackSun, which then leases the space to 30 unaffiliated websites. Each website has its own user account on the server for its operator to log on remotely and make changes to his or her website directory. The operator of one website cannot put content in the directory of another website because his user account does not have access. The server has an administrator account that an employee at BlackSun uses to maintain the server. This administrator has access to every directory but is not affiliated with any of the websites. The administrator of this hypothetical server is like the landlord of the server, and each room or unit is separated from the other by a lock and key.

Hypothetical Server B is also owned by BlackSun, but instead BlackSun leases the entire space to Company B. Company B now maintains the administrator account itself and can set up as many websites on the server as it wants. It could use the server solely to host its own websites. It could set up six websites of its own and sublease the remaining space to a seventh, unaffiliated website. It could set up no websites of its own and sublease all the space to unaffiliated websites, just as BlackSun did with Server A. Company B as administrator maintains rights over the whole space and can access all the directories, whether the websites are operated by Company B or subleased and operated by unaffiliated companies. Server B is now more like a 30-bedroom house leased to one person, who may then choose to occupy all the rooms himself, fill them

[2]At the suppression hearing, the government's expert, James Fottrell, was asked about the many different ways a server could be set up. The basis for these hypothetical servers comes from his testimony.

with his relatives, or sublet one or all of them to complete strangers and give them each locks on their rooms.

It should be obvious that, depending on whether a building is structured like Server A or Server B, the government may or may not have probable cause to search all the rooms when criminal activity is reasonably linked to one. The majority, however, would draw no distinction.

Neither party disputes that at the time of the seizure[3] and search, the investigating officers had probable cause to suspect that the site justinsfriends.net contained child pornography. The affidavit in support of the search warrant states that BlackSun confirmed that it was the current web hosting company for justinsfriends.net and justinsfriends.com (together, "JustinsFriends").[4] R. 87-1 (BlackSun Aff. at ¶ 46). The only additional communication from BlackSun provided in the supporting affidavit is the following:

> BlackSun is located at 1200 West 7th Street, Los Angeles, California 90017. BlackSun is an 18,000 square foot facility and has 2000 servers. The websites www.justinsfriends.com and www.justinsfriends.net websites [sic] resolving to IP address [xyz] resolve to one server that is a server owned and leased by BlackSun. The server is in cabinet 200.02, server number 4 and has a sticker on it that states collegeboyslive.

Id. at ¶ 47. The affidavit does not state to whom (or to how many parties) BlackSun leased computer server #4 in cabinet #200.02 ("Server #4"). It does not state who the administrator of Server #4 was. It does not state whether there were any other web sites hosted on Server #4, or whether those web sites were in any way related to JustinsFriends or had a common operator. In short, the affidavit does not state whether Server #4 is more like Server A in the above hypothetical or Server B.

---

[3]The search warrant authorized only on-site imaging of the servers, not taking the hardware off-site. However, one hard drive was removed and "imaged off-site due to technical issues." Appellee Br. at 25 n.10. Richards has not challenged whether the removal was an unlawful seizure; therefore, we need not address that issue.

[4]Users visiting justinsfriends.com were redirected to justinsfriends.net.

Based on the information that the FBI knew at the time the warrant was issued, probable cause existed to search any part of the server that someone affiliated with JustinsFriends could access. But the affidavit does not indicate that the FBI had any reason to suspect that someone affiliated with JustinsFriends was the administrator of the server as opposed to someone at BlackSun. The fact that *some person* had universal access to the server, without more, is insufficient grounds to justify a search of the entire server. Limiting the search to only a portion of the server under these circumstances is more consistent with our prior cases on electronic searches.

"A search warrant must particularly describe the things to be seized, but the description, whose specificity will vary with the circumstances of the case, will be 'valid if it is as specific as the circumstances and the nature of the activity under investigation permit.'" *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (quoting *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988), *cert. denied*, 488 U.S. 1005 (1989)). General warrants that merely authorize "wide-ranging rummaging searches" violate the Fourth Amendment. *United States v. Logan*, 250 F.3d 350, 364-65 (6th Cir.), *cert. denied*, 534 U.S. 895 (2001). Although cases addressing particularity are often concerned with supplying enough information to the agents executing the warrant, of equal concern "is whether the category as specified is too broad in the sense that it includes items that should not be seized." *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.), *cert. denied*, 527 U.S. 1011 (1999); *see also United States v. Greene*, 250 F.3d 471, 476-78 (6th Cir. 2001). Given that the individual server was clearly identified by location and name, the issue in this case stems from the breadth of the warrant—whether the warrant should have covered the entire server.

I agree with the majority that, in the course of a reasonable search, investigating officers may have to examine cursorily innocuous documents "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). The same is true in an electronic search. When a warrant authorizes the search of a personal computer for child pornography, the agents are not required to open only the files or folders labeled "child pornography" even

though this may result in brief access of private, innocuous material. *United States v. Burgess*, 576 F.3d 1078, 1093-94 (10th Cir.), *cert. denied*, 130 S. Ct. 1028 (2009). This flexibility recognizes that the owner of the computer has access to the full hard drive and may hide criminal activity under non-criminal names. That, however, is not the situation here.

As discussed above, a server like the one at BlackSun is inherently different from a personal computer in that it may belong entirely to one person, and thus be like a house with many accessible rooms, or it may host material provided by any number of potentially unaffiliated users who cannot access each others' content, resembling more an apartment complex with locked doors. The government wants to consider a server always like a home and therefore always to have probable cause to search the whole thing. The defense wants to consider a server always like an apartment building and to require a separate search warrant for every locked door. The reality is that servers can be structured to function like either, and our rules regarding searching shared server space should be flexible to accommodate both situations.

Almost all of the cases offered by the majority to justify the search of the entire server involve searches of computers or hard drives within the complete control of the individual suspected of criminal activity.[5] Only two cases address somewhat

[5]In most of the cases, the search warrant was issued because a specific individual was suspected of criminal activity. *See United States v. Clark*, 257 F. App'x 991, 992 (6th Cir. 2007) (unpublished opinion) (upholding broad search of computer or related storage media found in suspect's home), *cert. denied*, 555 U.S. 829 (2008); *United States v. Stabile*, 633 F.3d 219, 234 (3d Cir.) (same), *cert. denied*, --- S. Ct. ---, No. 10-10825, 2011 WL 2182609 (Oct. 11, 2011); *United States v. Mann*, 592 F.3d 779, 784 (7th Cir.) (same), *cert. denied*, 130 S. Ct. 3525 (2010); *Burgess*, 576 F.3d at 1093-94 (same); *United States v. Banks*, 556 F.3d 967, 973 (9th Cir. 2009) (same); *United States v. Hill*, 459 F.3d 966, 976-77 (9th Cir. 2006) (same), *cert. denied*, 549 U.S. 1299 (2007); *United States v. Grimmett*, 439 F.3d 1263, 1268-69 (10th Cir. 2006) (same); *United States v. Brooks*, 427 F.3d 1246, 1252-53 (10th Cir. 2005) (same), *cert. denied*, 546 U.S. 1222 (2006); *United States v. Simpson*, 152 F.3d 1241, 1248 (10th Cir. 1998) (same); *United States v. Lacy*, 119 F.3d 742, 746-47 (9th Cir. 1997) (same), *cert. denied*, 523 U.S. 1101 (1998). *Cf. United States v. Sherman*, 372 F. App'x 668, 675-76 (8th Cir. 2010) (unpublished opinion) (upholding search of computers found in business suspected of criminal activity); *United States v. Khanani*, 502 F.3d 1281, 1290 (11th Cir. 2007) (upholding search of multiple computer hard drives seized from multiple locations of a business suspected of criminal activity). In some instances, the agents suspected that a location had a computer device engaging in criminal activity and the search warrant was issued to cover all computer devices at the premises. *See United States v. Meeks*, 290 F. App'x 896, 901-02 (6th Cir. 2008) (unpublished opinion) (upholding search of computer disks in home where internet service had been used to download child pornography); *United States v. Cartier*, 543 F.3d 442, 447-48 (8th Cir. 2008) (upholding search of computer and hard drives found in home that was linked to an ISP address known to be downloading child pornography), *cert. denied*, 129 S. Ct. 1390 (2009); *Upham*, 168 F.3d at 535 (upholding search of computer found in home that was linked to an ISP address known to be downloading

comparable situations to the facts at hand, where the government sought to search space shared by many users, and both of these cases counsel against a blanket rule permitting searches of entire servers in all situations.

In *Guest*, state police had probable cause to believe that obscene material was being posted to two different electronic bulletin boards.[6] 255 F.3d at 336-37. Each bulletin board was run by a single person from his home. The police were able to identify the addresses of those individuals and in both cases seized the computer servers being used to operate the boards. The *Guest* case has no bearing on the facts of this case because in both instances in *Guest* the owners of the servers themselves were suspected of involvement in the criminal activity. The search was therefore appropriate with respect to suspicions relating to the owners of the servers. Additionally, the plaintiffs "[did] not dispute in their briefs that defendants had probable cause to search for evidence of crimes on the computers." *Id.* The government's reliance on *Guest* to justify wholesale seizure of any server is therefore misplaced. Appellee Br. at 32.

A more relevant comparison could be made to *United States v. Adjani*, 452 F.3d 1140, 1146 (9th Cir.), *cert. denied*, 549 U.S. 1025 (2006). In *Adjani*, the court upheld the search of someone else's computer in executing a search warrant at a suspect's residence. Upon first determining that probable cause existed to search computers found at the suspect's residence, the court next addressed whether the probable cause extended to a computer on the premises known to belong to the suspect's roommate. The court found that it did. "The agents, acting pursuant to a valid warrant to look for evidence of a computer-based crime, searched computers found in Adjani's residence *and to which he had apparent access*. That one of the computers actually belonged to [the

---

child pornography). Although this more closely resembles the instant facts, the key is that the agents in *Meeks*, *Cartier*, and *Upham* were still searching only computer devices that were accessible by the unidentified individual. If the address associated with the ISP had been an apartment building and no more, it seems indisputable that a warrant would not permit searching every computer in every individual apartment.

[6]One of the bulletin boards was a large online community where users, who accessed the site via an individual account and password, could e-mail each other, participate in chat rooms, play games, and post and read messages on a variety of topics. *Guest*, 255 F.3d at 330. The second bulletin board was smaller site where users could log in only one at a time to post and read content. *Id.* at 331.

roommate] did not exempt it from being searched, especially given her association with Adjani and participation (however potentially innocuous) in some of his activities as documented in the agent's supporting affidavit." *Id.* (emphasis added).[7]

All of these cases emphasize that the person suspected of criminal activity, whether identifiable or anonymous, had the ability to hide the illegal files anywhere on the computers or hard drives that were ultimately searched. *United States v. Mann*, 592 F.3d 779, 784 (7th Cir.) (broad search reasonable because defendant "could have images of women in locker rooms virtually anywhere on his computers"), *cert. denied*, 130 S. Ct. 3525 (2010); *United States v. Stabile*, 633 F.3d 219, 234 (3d Cir. 2011) ("[A] broad seizure was required because evidence of financial crimes could have been found in any location on any of the six hard drives, and this evidence very likely would have been disguised or concealed somewhere on the hard drive."), *cert. denied*, --- S. Ct. ---, No. 10-10825, 2011 WL 2182609 (Oct. 11, 2011); *Adjani*, 452 F.3d at 1146 (permitting search of all computers that suspect could access, even if not his); *United States v. Sherman*, 372 F. App'x 668, 675-76 (8th Cir. 2010) (unpublished opinion) ("[Defendant] fails to acknowledge he had access to all components of the computer system used in his business and that the computer data could be manipulated, stored in different formats, or stored outside of the [specific program suspected of misuse].").

Here, neither the warrant nor the supporting affidavit indicates a reason to believe that the owner of JustinsFriends had access to the entire server. The majority views the lack of knowledge regarding who was the administrator and whether the server was leased to one person or shared as counseling in favor of allowing unfettered access to the whole server.[8] I cannot agree. Absent probable cause to search the whole server, the agents must limit their search to the areas they have reason to believe someone at JustinsFriends could have placed child pornography. Based on the statements in the

---

[7]The court specifically disclaimed reliance on an argument that the two roommates maintained "joint computers." *Adjani*, 452 F.3d at 1145 n.3.

[8]The government makes no effort to hide this point: "[B]efore the search, the government did not know whether the server was shared or dedicated, and, if shared, whether any websites were related, how the directory was organized, and whether any users had access to the entire server." Appellee Br. at 35-36.

warrant and the supporting affidavit, that would be limited to the JustinsFriends directory and any unallocated space on the server.[9]

That is not to say that a warrant to search the entire server may never be "as specific as the circumstances and the nature of the activity under investigation permit." *United States v. Ables*, 167 F.3d 1021, 1033 (6th Cir.) (quoting *Henson*, 848 F.2d at 1383), *cert. denied*, 527 U.S. 1027 (1999). Indeed, probable cause might have been established in this case had the FBI agent requesting the warrant included additional facts in the warrant or supporting affidavit known at the time. We know from the evidence presented at the suppression hearing and later at trial that BlackSun provided FBI agents at least some information regarding the structure of Server #4 at the time the warrant was issued. BlackSun indicated that they leased the entire server to one individual, last name unknown. James Fottrell testified that when a server is leased in its entirety to one person or entity, it is more likely that the websites on that server are related. Had this information been included in the supporting affidavit, there may have been sufficient probable cause to search the entire server even without knowing anything else about the internal structure of the server.

FBI agents may not always be able to obtain such details about the internal structure of a server prior to imaging it. But the majority's position excuses the investigating agents from asking such simple questions as "Who leases this server?" and "What other websites are on this server?" When such answers are not forthcoming, the FBI could issue an administrative subpoena in order to gain more information about the structure of the server in question. Alternatively, the warrant itself could be structured to require computer personnel to make an initial determination based solely by looking at the user accounts as to what areas someone affiliated with the suspect site had access. Upon making such a determination, only those directories would be imaged for

[9]Richards does not contest the search of the unallocated space. When a website operator deletes content, the remains of the deleted file sit in the unallocated space on the server. Thus when the agents have probable cause to search a specific site, they should be able to search the unallocated space as well.

searching, or if already imaged due to on-site difficulties, any non-affiliated directories would be returned.[10]

The Ninth Circuit has already counseled a similar approach in instances where the suspect data is intermingled on the same server with other, non-target data. In *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc), a warrant was issued to obtain drug test results for ten specific baseball players from a third-party drug testing facility. The warrant specifically required that "'computer personnel' conduct the initial review of the seized data and segregate materials not the object of the warrant for return to their owner." *Id.* at 1171. Instead, the government imaged an entire directory and the case agent subsequently "rooted out information pertaining to *all* professional baseball players and used it to generate additional warrants and subpoenas to advance the investigation." *Id.* The court upheld several lower court determinations that the property was unlawfully seized and must be returned, rejecting the government's theory that the information was in "plain view." Because one cannot know the contents of a computer file without opening it, the court acknowledged, "everything the government chooses to seize . . . automatically come[s] into plain view. Since the government agents ultimately decide how much to actually take, this will create a powerful incentive for them to seize more rather than less." *Id.* The court ended with a cautionary note:

> The advent of fast, cheap networking has made it possible to store information at remote third-party locations, where it is intermingled with that of other users. . . . As a result, people now have personal data that are stored with that of innumerable strangers. Seizure of, for example, Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions.

Id. at 1176. The rule advanced by the majority in this case could also jeopardize the privacy of innumerable strangers to the crime. Here, the FBI agents made no showing

[10]This cannot be an overly burdensome requirement considering that the government presented evidence at trial indicating how it was able to determine that user accounts affiliated with JustinsFriends did indeed have administrative rights over the whole server. At the suppression hearing, however, the government's expert had not bothered to look at access rights yet, making a point of saying that his first priority was to find the child pornography anywhere on the server.

that they had probable cause to believe that every directory on Server #4 was accessible to the operators of JustinsFriends. They also made no effort to determine first what directories on Server #4 were accessible to the operators of JustinsFriends, or whether the operators were also administrators. Requiring such a preliminary showing when possible, or at a minimum requiring an initial inquiry before searching, allows legitimate interests of law enforcement to be advanced while still maintaining safeguards against the privacy of people who signed up for web hosting services and were never told that their site shared space with a child pornographer on the other side of the country.

When the government has probable cause to search for drugs in a specific apartment, we have never held that the existence of a landlord with keys to every other apartment in the building creates probable cause to search every apartment. But if the landlord happens to live in the very apartment suspected of containing drugs, his universal access may become relevant. Here, however, the warrant provided no probable cause to believe that someone connected to JustinsFriends had access to the entire server. I would therefore hold the search warrant unconstitutional because it was overly broad.

II. GOOD-FAITH EXCEPTION APPLIES

The only remaining question is whether the agents are entitled to rely on an invalid warrant under the good-faith exception in *United States v. Leon*, 468 U.S. 897, 914-15 (1984).[11] I agree that they are, but for different reasons than the majority. The only potential *Leon* situation applicable here is whether the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable

[11]The government's failure to raise this argument before the district court would normally counsel against addressing this issue. *United States v. Williams*, 615 F.3d 657, 668 (6th Cir. 2010); *see also United States v. Hahn*, 922 F.2d 243, 247-48 (5th Cir. 1991) (declining to consider good-faith exception raised for the first time on appeal). However, the relevant *Leon* exception here requires evaluating only the four corners of the affidavit and an objective reasonableness standard. *See United States v. Weaver*, 99 F.3d 1372, 1378 (6th Cir. 1996) ("In determining whether an affidavit is 'bare bones,' the reviewing court is concerned exclusively with the statements contained within the affidavit itself."). No further record development is necessary because unlike in *Hahn*, Richards's arguments are based solely on the deficiencies of the affidavit and not on the underlying facts. *See* Appellant Reply Br. at 25-26. We therefore may exercise our discretion to consider this issue. *Williams*, 615 F.3d at 668.

. . . ." *United States v. Schultz*, 14 F.3d 1093, 1098 (6th Cir. 1994) (quoting *Leon*, 468 U.S. at 923).[12]

Whether an affidavit lacks indicia of probable cause "is a less demanding showing than the 'substantial basis' threshold required to prove the existence of probable cause in the first place." *United States v. Carpenter*, 360 F.3d 591, 595 (6th Cir.) (en banc) (internal quotation marks omitted), *cert. denied*, 543 U.S. 851 (2004). The inquiry is whether an agent reading the warrant in a "practical, common sense manner" would be able to detect the deficiency. *United States v. Van Shutters*, 163 F.3d 331, 337 (6th Cir. 1998) (internal quotation marks omitted), *cert. denied*, 526 U.S. 1077 (1999). In *Van Shutters*, we upheld reliance on an affidavit describing both the criminal activity and a location with such particularity that a reasonable executing agent would make the "common sense inference" that the affiant had verified a nexus between the two. *Id.*

In this case, I disagree with the majority that the affidavit explains why it was necessary to image the entire server. Majority Op. at 20. The only area of the server for which the affidavit explains why a search is necessary relates to the unallocated space:

> I have been informed by James Fottrell, that the entirety of the unallocated space of the servers on which materials relating to IP address [xyz] are found should be searched because the unallocated space of those servers is likely to contain relevant evidence of materials that have been deleted or otherwise moved from the servers.

R. 87-1 (BlackSun Aff. at ¶ 55). An explanation like the one above is never offered as to why probable cause exists to image the whole server; only the details of how the server is going to be imaged are given. The remaining parts of the affidavit, however, suggest a sufficient nexus between the illegal activity and the server as a whole to support a good-faith belief in the warrant's validity even though probable cause was ultimately lacking, particularly given the level of detail in the affidavit and the technical nature of the search.

---

[12]The other three exceptions are inapplicable because the evidence does not suggest that the supporting affidavit was made in bad faith, that the magistrate judge abandoned his duties, or that the warrant was so facially deficient that it could not reasonably be presumed valid. *See United States v. Higgins*, 557 F.3d 381, 390-91 (6th Cir.), *cert. denied*, 130 S. Ct. 817 (2009).

The affidavit describes at length the probable cause for suspecting that the JustinsFriends sites are engaging in the production and distribution of child pornography. The affidavit then briefly explains how the FBI agents were able to determine that the JustinsFriends sites were located on a single server at BlackSun. The affidavit indicates a FBI Special Agent spoke to BlackSun representatives and was told the content was hosted on Server #4, and that Server #4 was "owned and leased" by BlackSun. *Id.* at ¶ 47. The affidavit then describes BlackSun's website as advertising "colocation" services.[13] The affidavit concludes by stating that "[m]embers of the justinsfriend website(s) are able to access servers through the use of a computer and computer modem or other connection device." *Id.* at ¶ 48. Although the use of the word "leased" may indicate to a technically savvy agent that this server in question was not necessarily owned entirely by JustinsFriends, the emphasis immediately following is on the colocation services offered at the BlackSun facility. That, coupled with the authorization to search the entire server, permit a common-sense inference of a sufficient connection between JustinsFriends and the entire server.

I would therefore hold that the good-faith exception in *Leon* justifies affirming the district court's decision to deny the motion to suppress, despite the invalidity of the underlying warrant. I therefore concur in the judgment.

[13]Colocation is a service whereby the web hosting company provides space at its facility for a customer to house its own server. R. 87-1 (BlackSun Aff. at ¶ 8(h)). For example, the second search warrant executed in this case was for a server housed at another ISP. When the officers called to preserve the content of the server in question, they were told that that ISP was "unable to preserve the content on the servers because the servers are password protected and are owned directly by [abc]." R. 87-2 (Aff. at ¶ 48).