

August 11, 2009

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

No. 08-8053

DAVID BURGESS,

Defendant - Appellant.

**Appeal from the United States District Court
for the District of Wyoming
(D.C. No. 1:07-CR-00298-ABJ-1)**

James C. Anderson, Assistant United States Attorney (Kelly H. Ranking, United States Attorney, with him on the briefs) Cheyenne, Wyoming, for Plaintiff-Appellee.

Norman R. Mueller (Ty Gee with him on the briefs) of Haddon, Morgan, Mueller, Jordan, Mackey & Foreman, P.C., Denver, Colorado, for Defendant-Appellant.

Before **TACHA, O'BRIEN**, and **McCONNELL**, Circuit Judges.

O'BRIEN, Circuit Judge.

Following a traffic stop and a canine alert, police searched David Burgess' motor home for drugs and evidence of drug trafficking. The search led to the

discovery of a laptop computer and two external hard drives. The hard drives contained thousands of pictures of child pornography, which Burgess moved to suppress, arguing the warrant authorizing their search lacked sufficient particularity and the search exceeded the scope of the warrant. The district court denied the motion. Burgess continues to press his arguments here and also challenges the admission of 404(b) evidence and the length of his sentence. We affirm.

I. FACTS

A. Introduction

On July 24, 2007, Wyoming Trooper Matt Arnell observed a motor home with Nevada license plates at a restaurant parking lot in Evanston, Wyoming. It was towing a trailer bearing an expired Wyoming license plate. Arnell was aware (from a prior briefing) the motor home was associated with the Hell's Angels motorcycle club. He verified that the trailer plate was expired but did nothing more until the motor home was driven on to Interstate 80 heading east. As Arnell followed the vehicle, he called for a drug canine to be brought to the area. He then stopped the motor home to issue a citation for the expired plate. When the driver, Shayne Waldron, stepped out, Arnell smelled the odor of burnt marijuana. As Arnell spoke with Waldron, a passenger in the motor home, David Burgess, joined the conversation. Burgess said he was the owner of the motor home and both men acknowledged the trailer's license plate was expired. Burgess explained

the trailer belonged to a person who permitted them to use it and they were traveling to another town in Wyoming to update the registration and obtain current plates.

As Arnell was issuing a citation for the expired plate, Deputy David Homar and his canine, Blitz, arrived. Blitz (who had never given a false alert to the presence of drugs) alerted at the doors of the motor home. Trooper Arnell informed Burgess he was going to search the vehicle. Burgess said he would rather Arnell get a warrant. Nevertheless, because of the suspicions raised by Blitz's alert and the smell of marijuana, Arnell entered the motor home where he found some marijuana, a pipe, and two bags of cocaine – each containing approximately seven grams. Arnell advised Waldron and Burgess of their rights per the *Miranda* decision.¹ When Arnell said he had found marijuana, Burgess admitted the marijuana was his. Arnell resumed the search. He noticed a laptop computer and a Seagate hard drive in the bedroom. After approximately fifteen to thirty minutes, Arnell left the motor home and arranged to have it towed to a Wyoming Department of Transportation shop for further inspection.

In the meantime, Agent Russell Schmitt, a narcotics officer with the Green River, Wyoming, police department arranged to meet Arnell at the shop. The two officers went to the Department of Criminal Investigations office in Evanston to

¹ *Miranda v. Arizona*, 384 U.S. 436 (1966).

prepare an affidavit and request for a search warrant. Paragraph 17 of the affidavit stated in relevant part: “Based upon training and experience, your Affiant [Schmitt] knows that persons involved in trafficking or the use of narcotics often keep photographs of coconspirators or photographs of illegal narcotics in their vehicle.” (R. Vol. I at 133.) Arnell and Schmitt’s team leader, Agent Webster, reviewed the documents. Arnell and Schmitt then took the documents to the county attorney for review and approval. Finally, they presented the affidavit and request for a warrant to the county judge, who incorporated the affidavit into the warrant and authorized a search for:

The property and premises of a white, 1999, Freightliner Motorhome . . . [for] certain property and evidence to show the transportation and delivery of controlled substances, which may include but not limit[ed] to, cash, or proceeds from the sale of controlled substances, Marijuana, Cocaine, Methamphetamine, or other illegal controlled substances, along with associated paraphernalia to include but not limited to pipes, bongs, syringes, packaging material, computer records, scales, laboratory dishes, flasks, beakers, tubes, pie tins, electrical timers, containers to be used for storing , manufacturing and selling, chemicals used in the creation of illegal narcotics as well as their diluting agents, items of personal property which would tend to show conspiracy to sell drugs, including pay-owe sheets, address books, rolodexes, pagers, firearms and monies.

(*Id.* at 130.) The warrant authorized a search on July 24, 2007, “or within ten days thereafter.” (*Id.*)

After serving the warrant, the officers returned to the search of the motor home. Arnell discovered a Maxtor hard drive pushed underneath the couch in the living room. The Maxtor drive along with the laptop and the Seagate drive

discovered earlier were seized and transported to Cheyenne, Wyoming, for forensic examination. Agent Scott Hughes, special agent with the Internet Crimes Against Children Division² was assigned to the case on August 1, 2007. When Hughes went to retrieve the material from the evidence locker, the associated paperwork was not present. Hughes immediately requested the paperwork, which he received on August 21, 2007. After reviewing the warrant, Hughes was concerned about the time delay (the items were seized on July 24). He contacted a DCI staff attorney who advised he could search for evidence of controlled substances, but if he found evidence of any other crime, he must stop and request a new warrant to continue his search. The search of the hard drives was commenced on September 6, 2007.

Hughes began with the Maxtor hard drive using a program called EnCase. The protocol is to first make a byte-for-byte copy of the hard drive. After the contents of the original hard drive are copied, the original drive is secured and the copied material is examined – this process ensures evidence is not corrupted. Hughes planned to contact the investigating agent to see if there were any special key or code words which may have been found during the investigation to facilitate further search once the copying process was complete.

Copying the files can take up to twelve hours but EnCase allows an

² Agents from this division are trained in computer examinations and work on cases from many different law enforcement divisions, including narcotics.

investigator to “preview” files as they are being copied. (*Id.* at 246.) Hughes decided to take advantage of the preview feature to look for “trophy photos,” *i.e.*, pictures of a “person holding the controlled substance in front of a stack of money,” similar to the kinds of photographs described in Paragraph 17 of Schmitt’s affidavit. (*Id.*) The images are shown in a “gallery view,” an option where multiple reduced size photos are displayed on one page. (*Id.*) After viewing 200-300 digital images of personal photographs, Hughes came upon an image depicting child sexual exploitation. He immediately closed the preview program and secured a new warrant authorizing a search for evidence of child sexual exploitation. He then searched all three devices, the laptop, the Seagate hard drive and the Maxtor hard drive. While the laptop did not contain child pornography, his search revealed approximately 166,000 images, including movies and texts, between the two hard drives. Hughes stopped counting the number of child pornography files when the count exceeded 1,300. His conservative estimate was 30% to 45% of the files contained child pornography, approximately 70,000 images. Some of the same pornographic pictures were on both the Maxtor and the Seagate hard drives.

A grand jury indicted Burgess for knowing transportation of child pornography across state lines in violation of 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (Count One) and knowing possession of child pornography transported in interstate commerce in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)

(Count Two). Both charges were based on the images found in the Maxtor hard drive “including, but not limited to,” six specific images.

B. Pretrial Motions

Burgess moved to suppress the evidence claiming the original search of the Maxtor hard drive violated his rights under the Fourth Amendment. He maintained the first warrant (authorizing a search for drug trafficking evidence) lacked specificity and the search constituted an impermissible general search.³ The government claimed, even if the warrant was defective, the search was permissible under the automobile exception to the general presumption that warrantless searches are unreasonable. The district court denied Burgess’ motion, concluding both the seizure and the search of the computer equipment was supported by probable cause, the seizure was valid under the automobile exception and the search warrant was sufficient to allow a search of the computer equipment for evidence of drug trafficking. Finally, the court held the search did not exceed the scope of the warrant.

Prior to trial, Burgess said he planned to defend against the charges by testing the government’s ability to prove he knowingly possessed the images charged in the indictment and found on the Maxtor hard drive. In response the government filed a motion declaring its intent to introduce 78 images from the

³ Burgess claims the second search warrant (authorizing a search for child pornography) was tainted by the first search, but raises no other issues with respect to the second warrant or the resulting search.

Seagate hard drive, including numerous pictures of R.C., a fourteen-year-old female ward of Burgess' friend, Rebecca Deshaise. Numerous pictures of R.C. were found on both hard drives and trial testimony revealed R.C. had spent many hours at Burgess' home over the years.

Some of the pictures of R.C., found only on the Seagate drive, were taken in May, 2007, in a motel room in Winnemucca, Nevada, while Burgess attended the Run-A-Mucca motorcycle rally. R.C. and two of her friends accompanied Deshaise and Burgess to the rally. Among the pictures were nude and seminude images of her (some showing her exposed genitalia), which also contained lurid text suggesting Burgess was the photographer and/or describing inappropriate sexual contact between R.C. and "Uncle David." (*e.g.* Sealed Vol. II, Exh. 816.) The government offered the evidence to prove motive, intent, knowledge, and identity under Rule 404(b) of the Federal Rules of Evidence. The government's motion generated objections and motions in limine prompting hearings prior to and during the trial. Eventually, the parties stipulated to the admissibility of four of the child pornographic images charged in the indictment — those four pictures were found on both the Maxtor and Seagate hard drives.⁴ The pictures of R.C. were not among those admitted by stipulation.

⁴ The images are clearly child pornography. They show a pre-pubescent girl wearing nothing but a light dress pulled up over her chest: Exhibits 805-808 show the nude child in various poses centering on her genitalia. One image shows her with an adult male.

C. Trial

During the government's case in chief the court admitted four pictures of R.C. found on the Seagate drive⁵ and gave a limiting instruction to the jury.⁶

⁵ These exhibits include one nude image of R.C. taking a shower and several semi-nude pictures of R.C. dressed only in a towel. The images appear with graphic and vulgar superimposed text. For example, one image is R.C. sitting cross-legged on a bed wearing only a short towel (genitalia exposed) with superimposed text referring to "Uncle David's . . . Princess." (R. Sealed Vol. II, Exh. 816.) The nude shower image contains the superimposed statement, "I think this is one of the sexiest pictures in my collection." (*Id.*, Exh. 834.)

6

Ladies and gentlemen of the jury, the two charges contained in the Indictment in this case refer to the Maxtor hard drive. I need and wish to caution you at this point concerning evidence as to the Seagate hard drive.

Evidence that an act was done or that an offense may have been committed by the defendant at some other time is not, of course, any evidence or proof whatever that at another time the defendant performed a similar act or committed a similar offense, including the offenses charged in this Indictment. Evidence of a similar act or offense may not be considered by the jury in determining whether the defendant actually performed the physical acts charged in this Indictment, nor may such evidence be considered for any other purpose whatever unless the jury first finds beyond a reasonable doubt, from other evidence in the case standing alone, that the defendant physically did the acts charged in the Indictment. If the jury should find beyond a reasonable doubt from other evidence in the case the defendant did the act or acts alleged in the counts under consideration, the jury may then consider the evidence as to an alleged earlier act of a like nature in determining the state of mind or intent with which the defendant actually did the act or acts charged in the Indictment.

It is also offered for the purpose of identity, that it was the defendant that did the acts, as well as knowledge on the part of the defendant that the acts have been performed.

Of course, I want to again emphasize that you will hear evidence of other digital images contained in the Government's 800 series of exhibits that

According to the government the superimposed text on the photographs directly connected Burgess to the images of R.C., showed he was aware of the contents of the Seagate drive, and, because some of the child pornography on the Seagate Drive was identical to that on the Maxtor drive, was evidence from which the jury could infer he had knowledge of the contents of the Maxtor drive, specifically the pictures charged in the indictment.

Burgess called several witnesses who testified he never acted inappropriately around children. One of these witnesses was Deshaise, R.C.'s legal guardian and chaperone of all three girls at the Runna-A-Mucca motorcycle rally. Deshaise testified she was with the girls at all times in the motel room and they were never alone with Burgess. On cross examination the government questioned Deshaise regarding the circumstances surrounding twelve more images of R.C. taken in the motel room in Winnemucca and also found on the Seagate hard drive (they were in addition to the four already admitted).⁷ The government

were found on the Seagate hard drive that the Government alleges were possessed by the defendant. You may consider this evidence only as it bears on the defendant's intent, the identity of the defendant, the defendant's knowledge and the absence of a mistake, and for no other purpose. Of course, the fact that the defendant may have possessed these images does not mean that the defendant necessarily committed the act charged in this case.

(R. Vol. II at 615-16.)

⁷ Some of these images include the same image of R.C. contained in Exhibits 816 and 834, but with additional material. In Exhibit 832 an oval containing a much younger

offered the pictures to rebut Deshaise's testimony that the girls were adequately chaperoned and Burgess could not have taken the pictures. The pictures were admitted over Burgess' objection and without explanation.

The jury found Burgess guilty of both counts.

D. Sentencing

The presentence report (PSR) calculated a total offense level of 37 and a criminal history category I.⁸ Burgess objected to the PSR's use of both an enhancement under USSG §2.2(b)(4) (vulnerable victim) and an enhancement under USSG § 3A1.1(b)(1) (vulnerable victim) as double counting. He also claimed an enhancement under USSG §2.2(b)(5) (use of a computer) was not applicable because the hard drive was not a computer. Finally, he claimed he was entitled to a two-level reduction of his offense level under USSG § 2G2.2(b)(1). The court rejected the objection regarding use of a computer but agreed as to the vulnerable victim enhancement and therefore reduced the total offense level to 35.⁹ The court further determined Burgess was not entitled to a two point

picture of R.C. is superimposed to the side of the sexually explicit picture of R.C. The same picture appears again in Exhibit 848 without text. Exhibit 833 is a composite of R.C. as well as a friend, both in various states of undress; the superimposed text reads, "Gee . . . you think this might be the reason why your daddy doesn't want his 14-yr-old daughter spending the night in a motel room with me." (R. Sealed Vol. II, Exhs. 827, 832, 848.)

⁸ The November 1, 2007 Edition of the United States Sentencing Guidelines Manual was used for sentencing.

⁹ The district court ruling on these objections is not at issue on appeal.

reduction under U.S.S.G § 2G2.2(b)(1) in light of his conviction for transporting the child pornography across state lines. It declined to sentence Burgess below the guideline recommendation, imposing a sentence of 180 months imprisonment on Count One and 120 months imprisonment on Count Two, the sentences to run concurrently.

Burgess appeals from the denial of his motion to suppress evidence, the admission of 16 images from the Seagate hard drive and the length of his sentence.

II. DISCUSSION

A. Motion to Suppress

1. *Standard of Review*

“When reviewing the district court’s denial of a motion to suppress, we view the evidence in the light most favorable to the government and accept the district court’s factual findings unless they are clearly erroneous.” *United States v. Grimmatt*, 439 F.3d 1263, 1268 (10th Cir. 2006). “The ultimate question of reasonableness under the Fourth Amendment is a legal conclusion that we review de novo.” *Id.* Burgess claims the search of his hard drive amounted to a general search prohibited by the Fourth Amendment and the original warrant lacked sufficient particularity to justify the agent’s search of the images on his hard drive. The government maintains the search was within the scope of the warrant and, in any event, a warrant was unnecessary because the hard drives and laptop

could be searched as well as seized pursuant to the automobile exception.

2. *Computer Search*

a. Automobile Exception

The Fourth Amendment protects the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” “[I]t is a cardinal principle that ‘searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment--subject only to a few specifically established and well-delineated exceptions.’” *United States v. Ross*, 456 U.S. 798, 825 (1982) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). One of these specifically established exceptions is the “automobile exception” which allows the police to “search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained.”¹⁰ *California v. Acevedo*, 500 U.S. 565, 580 (1991).

“The scope of a warrantless search based on probable cause is no narrower — and no broader — than the scope of a search authorized by a warrant supported by probable cause. Only the prior approval of the magistrate is waived; the search otherwise is as the magistrate could authorize.” *Ross*, 456 U.S. at 823.

¹⁰ “[T]he justification to conduct such a warrantless search does not vanish once the car has been immobilized,” *Michigan v. Thomas*, 458 U.S. 259, 261 (1982), and “[t]here is no requirement that the warrantless search of a vehicle occur contemporaneously with its lawful seizure.” *United States v. Johns*, 469 U.S. 478, 484 (1985).

“When a legitimate search is under way, and when its purpose and its limits have been precisely defined, nice distinctions between closets, drawers, and containers, in the case of a home, or between glove compartments, upholstered seats, trunks, and wrapped packages, in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand.” *Id.* at 821.

Against this legal backdrop, and relying on our holding in *United States v. Andrus*, 483 F.3d 711 (10th Cir. 2007), *cert. denied*, 128 S. Ct. 1738 (2008), the government urges us to apply the automobile exception not only to the seizure of the laptop and hard drives but to the search of those items as well. *Andrus* involved a father’s actual or apparent authority to consent to the search of a computer located in their shared residence but belonging to his absent adult son. In discussion of reasonable expectations of privacy we likened a computer to a suitcase or briefcase. *Id.* at 718. Because “[a] personal computer is often a repository for private information the computer’s owner does not intend to share with others” and “intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy.” *Id.* (quotations omitted). The government constructs this syllogism: 1) the expectation of privacy of computer contents has been likened to that of a suitcase or briefcase (*Andrus*); 2) the automobile exception to the warrant requirement permits, with probable cause, the search of containers found in the automobile –

even locked suitcases and briefcases, *Acevedo*, 500 U.S. at 580; therefore 3) police may (with probable cause, but without a warrant) search computers and hard drives found in automobiles, Burgess' motor home included.

Burgess does not quarrel about the search of his motor home for drugs.¹¹ Rather, he contends the application of the automobile exception to search the computer and hard drives found in his motor home would grant police “the authority to forensically analyze and conduct a general search of any computer found in any automobile which was subject to a valid search under the automobile exception.” (Appellant’s Reply Br. at 2.) While a computer may be a container, because of the amount of personal information stored within, Burgess argues it is a virtual home. He says in this “age of the laptop computer,” such an “extraordinary expansion” of the automobile exception would “destroy a citizen’s expectation of privacy in his or her computer.” (*Id.*)

The Supreme Court’s Fourth Amendment jurisprudence has not directly addressed this issue. Moreover, the parties have cited no case law which either allows or prohibits computer equipment searches under the automobile exception and our research has failed to uncover such authority.

¹¹ See *United States v. Stewart*, 473 F.3d 1265, 1270 (10th Cir. 2007) (“A canine alert gives rise to probable cause to search a vehicle. This is so even when the dog alert occurs during a warrantless sniff on the exterior of a vehicle during a lawful traffic stop because such sniffs do not implicate the Fourth Amendment.” (citation and quotations omitted)).

At first blush, there appears no reason to treat computers differently than, for instance, a locked briefcase in the locked trunk of an automobile. There is a privacy expectation for a briefcase or suitcase, which may contain very personal and confidential papers – particularly when well secured in the trunk of a car. Yet the automobile exception subjects the briefcase to search. So why not the computer? What is the difference between a file cabinet, suitcase or briefcase and a computer? It might lie in the sheer range and volume of personal information the computer may contain. *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (“development of personal computer . . . increases . . . ability to conduct a wide-ranging search”).

“[A]nalogies to closed containers or file cabinets may lead courts to ‘oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.’” *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (quoting Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994)); *see also* *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) (“analogies to other physical objects . . . do not often inform the situations we now face as judges when applying search and seizure law”); *United States v. Campos*, 221 F.3d 1143, 1148 (10th Cir. 2000) (“the storage capacity of computers may require law enforcement officers to take a special approach”). In *Andrus*, we “tentative[ly]” characterized a computer as a container akin to a suitcase or locked footlocker,

but we did so to emphasize the high expectation of privacy for this particular type of “container,” not to permit promiscuous searches under the automobile exception. 483 F.3d at 718. And a notable distinction may exist between authority to seize a computer and authority to search its contents.

In *Carey*, we stated,

Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought.

172 F.3d at 1275. Historically, there is substantial support for the notion a warrantless seizure is valid but a warrantless search is not.

[I]f there is probable cause to believe [an object] contains contraband, the owner’s possessory interest in the container must yield to society’s interest in making sure that the contraband does not vanish during the time it would take to obtain a warrant. The item may be seized temporarily. It does not follow, however, that the container may be opened on the spot. Once the container is in custody, there is no risk that evidence will be destroyed. Some inconvenience to the officer is entailed by requiring him to obtain a warrant before opening the container, but that alone does not excuse the duty to go before a neutral magistrate.

Texas v. Brown, 460 U.S. 730, 749-50 (1983) (plurality) (J. Stevens, concurring).

That, of course, was the rationale underlying *United States v. Chadwick*, 433 U.S.

1 (1977) (search of double locked footlocker found in automobile unreasonable),

and *Arkansas v. Sanders*, 442 U.S. 753 (1979) (search of seized suitcase found in

taxi unreasonable), but that rationale was rejected in *California v. Acevedo*, 500 U.S. 565, 579 (1991), in favor of a bright line rule: “We therefore interpret *Carroll* as providing one rule to govern all automobile searches. The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained.” *Acevedo* involved a paper bag full of marijuana in the trunk of a car but the court saw no reason to distinguish that sack, which would be an unlikely container of private papers, from a briefcase, which very well might. In a concurring opinion Justice Scalia noted anomalies in dealing with vehicle searches, saying:

I agree with the dissent that it is anomalous for a briefcase to be protected by the "general requirement" of a prior warrant when it is being carried along the street, but for that same briefcase to become unprotected as soon as it is carried into an automobile. On the other hand, I agree with the Court that it would be anomalous for a locked compartment in an automobile to be unprotected by the "general requirement" of a prior warrant, but for an unlocked briefcase within the automobile to be protected. I join in the judgment of the Court because I think its holding is more faithful to the text and tradition of the Fourth Amendment, and if these anomalies in our jurisprudence are ever to be eliminated that is the direction in which we should travel.

Id. at 581.

Practically speaking, the forensic search of a hard drive (or its equivalent, such as a flash drive¹²) will rarely be conducted at the “site” while searching an

¹² “Flash drives” are solid state memory devices that can comfortably be carried on a key chain. They can be used, usually thru a USB port, much like an external hard drive. They hold tremendous amounts of data, commonly having 2 to 32 GB of memory. One manufacturer has recently announced the release of a 256 GB flash card, which

automobile, given the potential to corrupt or lose evidence. Arguably, requiring the government to secure a warrant prior to searching the contents of a properly seized computer is typically not overly burdensome in light of the privacy interests at stake. However, sometimes the police may not resort to forensic programs like EnCase. Assuming probable cause to do so, they might simply turn the computer on and conduct a superficial search. Nothing in *Acevedo* suggests either type of search (limited or on site forensic) would be impermissible without a warrant, but seemingly well settled matters are subject to change.¹³ Last term in *Arizona v. Gant*, 129 S. Ct. 1710, 1722 (2009), the Court retreated from clear language in *New York v. Belton*, 453 U.S. 454 (1981). *Belton* said, “when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile.” 453 U.S. at 460 (footnote omitted). After *Gant* the rule is “Police may search a vehicle incident to a recent occupant’s arrest only if the arrestee is within reaching distance of the passenger compartment at the

would equal or exceed the hard drive capacity of many contemporary laptop computers. *See*, <http://www.physorg.com/news167461888.html>.

¹³ Doing so would be much like searching a cell phone for recent calls (in and out), information contained in the address book, image files (still or digital video), audio files (including phone messages) or other digital information. The memory cards, available in some cell phones can, like flash drives, hold vast amounts of information, including image and data files. *See*, for instance [http://www.sandisk.com/Products/Item\(2537\)-SDSDQ-8192-A11M-SanDisk_microSDHC_8GB_Card_with_SD_Adapter.aspx](http://www.sandisk.com/Products/Item(2537)-SDSDQ-8192-A11M-SanDisk_microSDHC_8GB_Card_with_SD_Adapter.aspx).

time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest.” *Gant*, 129 S. Ct. at 1723. In spite of clear language in *Acevedo*, one might speculate whether the Supreme Court would treat laptop computers, hard drives, flash drives or even cell phones as it has a briefcase or give those types of devices preferred status because of their unique ability to hold vast amounts of diverse personal information. Interesting as the issue may be, we need not now resolve it because the search of Burgess’ hard drives was authorized by a warrant.

b. Validity of the Warrant

Burgess argues the initial search warrant authorizing a search of “computer records” and “items of personal property which would tend to show a conspiracy to sell drugs” was overbroad. (R. Vol. I at 130.) “The Fourth Amendment requires not only that warrants be supported by probable cause, but that they particularly describ[e] the place to be searched, and the persons or things to be seized.” *Otero*, 563 F.3d at 1131 (quotations omitted). “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.” *Id.* at 1132. “Because of this, our case law requires that warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes

or specific types of material.” *Id.* (quotations omitted). However, we must keep in mind “[a] reviewing court is to interpret search warrant affidavits in a common sense and realistic fashion.” *Grimmett*, 439 F.3d at 1270.

We agree with the district court; “the pertinent documents could have been more artfully prepared.” (*Id.* at 88.) We also agree the officers had probable cause to seize the computer equipment and could do so without a warrant under the automobile exception. Although a closer call, we further agree the warrant to search “contained sufficiently particularized language” creating “a nexus” with the crime to be investigated – drug trafficking – and therefore was not overly broad. *Id.* at 1271. The warrant authorized the search of Burgess’ motor home for “certain property and evidence to show the transportation and delivery of controlled substances, which may include but [is] not limited to” controlled substances, paraphernalia, chemicals, and containers. (*Id.* at 130.) It also authorized a search for “computer records” and for “items of personal property which would tend to show conspiracy to sell drugs, including pay-owe sheets, address books, rolodexes, pagers, firearms and monies.” (*Id.*)

The inclusion of “computer records” amongst a host of other physical items might seem to be an anomaly. Nevertheless, the warrant authorizes such a search and provides context for determining its scope. The issue here relates to the breadth of the search authorized. If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth

Amendment's particularity requirement. *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005);¹⁴ *United States v. Leary*, 846 F.2d 592, 600 (10th Cir. 1988). But "a word is known by the company it keeps." *S.D. Warren Co. v. Maine Bd. of Envtl. Prot.*, 547 U.S. 370 (2006) (dealing with statutory construction). The search, in general, was limited to evidence of drugs and drug trafficking and, as it relates to the computer, was limited to the kind of drug and drug trafficking information likely to be found on a computer, to wit (as the warrant says): "pay-owe sheets, address books, rolodexes" and "personal property which would tend to show conspiracy to sell drugs." (*Id.* at 130.) The latter could reasonably include "trophy photos."

Paragraph 17 of Schmitt's affidavit explicitly included "photographs of coconspirators or photographs of illegal narcotics" among the types of items to be included in the requested search. (*Id.* at 133.) The warrant, itself, does not

¹⁴ In *Riccardi*, we held the seizure of computer equipment was permissible, but the subsequent warrant authorizing the search "was not limited to any particular files, or to any particular federal crime" and therefore violated the Fourth Amendment. 405 F.3d at 862. The warrant authorized the search of Riccardi's computer:

and all electronic and magnetic media stored therein, together with all storage devises [sic], internal or external to the computer or computer system, **including** but **not limited to** floppy disks, diskettes, hard disks, magnetic tapes, removable media drives, optical media such as CD-ROM, printers, modems, and any other electronic or magnetic devises used as a peripheral to the computer or computer system, and all electronic media stored within such devises.

Id. (emphasis added).

explicitly instruct officers to look for image files on the hard drive, but the affidavit was incorporated into the warrant and is, at least, an aid to interpretation of the term used in the warrant – computer records.

Our reading of the scope of the “computer records” subject to search, narrowing it to looking for drug related evidence, comes from the text of the warrant, with due regard to context, coupled with the specifics of the supporting affidavit, *see Grimmett*, 439 F.3d at 1271; *United States v. Brooks*, 427 F.3d 1246 (10th Cir. 2005), and is reinforced by the executing officer’s (Hughes) understanding of and respect for the narrow scope authorized by the search warrant. Hughes was only looking for “trophy photos” when he came upon the child pornography.¹⁵

c. Scope of Search

Burgess claims the scope of the search violated the Fourth Amendment under our holding in *Carey*, because Agent Hughes “employed none of the

¹⁵

“While the warrant does not explicitly instruct officers to look solely for those text files containing child pornography, in context-and certainly in the view of the officers conducting the search-the restrictions placed upon searches for image files also apply to the other types of files. In other words, although the language of the warrant may, on first glance, authorize a broad, unchanneled search through Brooks's document files, as a whole, its language more naturally instructs officers to search those files only for evidence related to child pornography. In this light, the warrant should be-and was-read by officers to implicitly place the same restriction (i.e., to locate child pornography) on the scope of the entire search.”

Brooks, 427 F.3d at 1252.

methods suggested by this Court in *Carey* to avoid searching files which would not be related to any drug offense.” (Appellant’s Reply Br. at 7.) And it is true that Hughes began his search by previewing photographs contained in the Maxtor hard drive.

As in this case, the officer in *Carey* inadvertently discovered an image of child pornography while searching for electronic evidence of drug activity. After opening the first file, the officer in *Carey* temporarily abandoned the search for drug evidence and proceeded to look through the hard drive for more images of child pornography. We determined the extension of the search to locate further evidence of child pornography exceeded the scope of the warrant authorizing a search for evidence of drug crimes. Here Hughes immediately stopped the preview upon seeing an instance of suspected child pornography and obtained another warrant to search for pornography. Beyond that obvious and significant difference between this case and *Carey*, it is tempting, as Burgess suggests, to over read *Carey*. But the *Carey* holding was limited. Both the majority and the concurring opinions were careful to warn that the case was fact intense. *Carey*, 172 F.3d at 1276 (“[W]e are quick to note these results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result.”).

While “[o]fficers 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,” *Walser*, 275 F.3d at 986, “a computer search may be as extensive as reasonably required to locate the items described in the warrant” based on probable cause. *Grimmett*, 439 F.3d at 1270 (quotation omitted). And “[t]his Court has never required warrants to contain a particularized computer search strategy.” *Brooks*, 427 F.3d at 1251. *Carey* dicta suggested methods to constrain searches, keying on the type of files identified in the warrant, file names, key word searches, directory structure (file organization), etc. 172 F.3d at 1276. The warrant here did not direct the search by describing file name extensions (.doc,. wpd, .txt, .jpg, .gif, etc.),¹⁶ file names or directory structure. Rather the limitation on the scope of this search was explicitly constrained by content – computer files containing evidence of drug use or trafficking. Such files could take many forms. Pay-owe sheets could be generic text files (.txt) or word processing documents, e.g. Microsoft Word (.doc, .docx, .dot, .dotx, etc.), Corel WordPerfect (.wpt, .wpk, .wpd, .wp7, etc.), or other word processing programs and, of course, there is the ubiquitous .pdf from Adobe.¹⁷ Address

¹⁶ A file extension consists of one to five characters and informs a computer’s operating system what program to utilize in order to open a particular file. There are thousands of filename extensions.

<http://www.sharpened.net/glossary/definition.php?fileextension>.

¹⁷ Open-source applications like Abiword (.abw), KWord (.kwd), and OpenOffice (.odt, .odm, .odf, etc.), or newer online word processors like Google Docs (which allows you to download the document in a number of file formats) complicate the issue even further.

books or the electronic version of a rolodex might be found in Outlook (.pst) or other Email program files or they could be in spreadsheets such as Excel (.xls, .xlsb, .xltx, etc.), Lotus 1-2-3 (.wks, .wk4, etc.), Quattro Pro (.qpw) Quicken (.qsd, .qdf, .qel, etc.), or OpenOffice (.ods, .ots, etc.). Or they could be database files like Access (.accdb, .mdb, .maf, .mar, etc.) or Paradox (.db).

It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods – that process must remain dynamic. While file or directory names may sometimes alert one to the contents (*e.g.*, "Russian Lolitas," "meth stuff," or "reagents"), illegal activity may not be advertised even in the privacy of one's personal computer – it could well be coded or otherwise disguised.¹⁸ The directory structure might give hints as to an effective search strategy, but could just as well be misleading and most often could not effectively, or even reasonably, be described or limited in a warrant. Keyword searches may be useful in locating suspect files, but not always. In this case, for instance, some of the pictures of R.C. contained lurid text (*see* n.5 & 7), which, if searchable, might lead an investigator to those images by use of keyword searches. But that text does not appear in the filename, meaning it would not be revealed by a filename

¹⁸ Hughes testified to having seen computer files in other cases describe pay-owe sheets as “auto repair bills,” marijuana as “green paint,” and cocaine as “white paint.” (R. Vol. I at 248.) There was no evidence of deliberate concealment in this case; some of the filenames are incriminating. *See* n.16. However, other file names gave little or no indication of the file’s content. *See* discussion on the next page.

search. And if the text was an embedded graphic (rather than embedded text) it might not be revealed even in a word search of the entire document. Moreover some of the pictures of R.C. (Exhibits 830-834) had the following path: 07 301 8\8Hold\RC2007\May\252627\Towel\ and indelible filenames, such as `Img_5777_875.jpg`. The path and filename of one particularly graphic image (Exhibit 816 – lurid text superimposed) was: 07 301 8\8\Als_u621x2a.jpg. On the other hand the path and/or filename may sometimes give an obscure hint as to the content. For instance three of the pornographic child pictures from the Maxtor and Seagate hard drives (Exhibits 805, 807 and 808) had this path: 07 301 8\8\Files\SG\Kp\Amateur Access\DCP\ (emphasis added). But the file names, such as `DCO01352.jpg`, gave no hint as to file content

In summary, 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 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).¹⁹

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. 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.

We have not abandoned the concerns expressed in *Carey*. See *Otero*, 563 F.3d at 1135-36; *Brooks* 427 F.3d at 1251-52; *Riccardi*, 405 F.3d at 862; *Walser*, 275 F.3d at 986 (agent used a clear search methodology searching records where

¹⁹ We recognize a unique case might justify looking at tax returns for evidence of payments related to drug activities such as purchases of manufacturing supplies or equipment.

evidence might logically be found); *Campos*, 221 F.3d at 1148. The preview technique may be problematic in other contexts but we are not prepared to condemn it in this case. We must be guided by practical realities and several are readily apparent. First, Hughes was not previewing all files, only image files and his search was properly targeted – “trophy photos.” Second, had Hughes omitted the preview and, instead, waited to do a structured search on the copied files (for instance, by looking at the filenames of .jpg files) his search for "trophy photos" would eventually and inevitably have led to discovery of the charged images.²⁰ Third, as our cases seem to require, Hughes immediately closed the gallery view when he observed a possible criminal violation outside the scope of the warrant's search authorization and did not renew the search until he obtained a new warrant. Fourth, in general a structured approach may provide only the illusion of protecting privacy interests, particularly when the search target is image files. When a computer search for drug related evidence reveals filenames strongly

²⁰ As trial evidence demonstrated some of the file names in Burgess' hard drive were particularly descriptive and a review of the names would have legitimately aroused the suspicions of an agent trained in child pornography and inevitably led to the second search warrant. *See United States v. White*, 326 F.3d 1135, 1138 (10th Cir. 2003) (“the exclusionary rule is inapplicable if the evidence inevitably would have been discovered by lawful means.”). For example, one folder named “Nastiest11yoSeries” had a subfolder titled “Sausage” containing pornographic images of a young girl. (R. Vol. II at 574.) Another folder titled “AGE” contained subfolders titled “03,” “04,” “05,” “06,” “07,” “08,” “09,” “10” and “11.” (*Id.* at 569-70.) Each subfolder folder contained images of children the same age as described in the title engaged in sexually exploitive conduct. One file was entitled “Lolita,” a term which Agent Hughes testified is often seen in the investigation of child pornography. (*Id.* at 573-74.)

suggesting pornography an officer might be required to get another warrant before proceeding. But if the suggestive file names did not amount to probable cause he could keep searching for drug evidence, ultimately resulting in opening most files to make sure they were not deceptively labeled. And eventually the child pornography would be revealed. The only difference is that it would be discovered later, rather than earlier. That is particularly true in this case where the search was for image files, which could be buried almost anywhere.²¹ Fifth, Burgess complains the particular methodology used in this case was overbroad, yet he offers no alternative methodology that would protect his legitimate interests and also permit a thorough search for evidence of drug trafficking. *See Brooks*, 427 F.3d at 1251 (“[N]or has Brooks suggested how the search in this case would have been different with a scripted search protocol.”).

On these facts, we cannot say the Fourth Amendment was violated.

²¹ It would seem odd to require an officer who merely suspects pornography to stop the search for evidence of drug trafficking. The concurring opinion in *Carey* suggests it would not be necessary. “[I]f the record showed that Detective Lewis had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, I think a different result would be required.” 172 F.3d at 1277. It would also seem odd to require the officer to attempt to obtain a pornography warrant before confirming his suspicions about a file. Especially so in this case because if the suspicions did not, in the view of a judge, amount to probable cause the officer could continue his structured search for evidence of drug trafficking and eventually return to and open the suspicious file (and multiple others) to guard against deceptive labeling.

d. *Leon* Good Faith

Even if the warrant was not sufficiently particularized to comply with the Fourth Amendment, the evidence need not be excluded if the search qualified under the good faith doctrine of *United States v. Leon*, 468 U.S. 897 (1984). Whether the “good faith exception” to the exclusionary rule should be applied is a question of law, subject to de novo review by this Court.²² *Leary*, 846 F.2d at 606. In *Leon*, the Supreme Court held the purpose of the exclusionary rule is to deter police misconduct and “suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further” that purpose. 468 U.S. at 918. “Where an officer acting with objective good faith obtains a search warrant from a detached and neutral magistrate and the executing officers act within its scope, there is nothing to deter.” *United States v. Nolan*, 199 F.3d 1180, 1184 (10th Cir. 1999).

Burgess argues the *Leon* exception does not apply here because the warrant was “so facially deficient . . . the executing officers [could] not [have] reasonably presume[d] it to be valid.” *Leon*, 468 U.S. at 923. It is the government’s burden to prove “its agents’ reliance upon the warrant was objectively reasonable.” *United States v. Corral-Corral*, 899 F.2d 927, 932 (10th Cir. 1990) (quotations

²² The parties briefed and argued the issue in the district court, which did not reach it, and it was briefed on appeal. Thus, we may consider it. See *United States v. Harrison*, 566 F.3d 1254, 1256 (10th Cir. 2009) (proceeding directly to *Leon* analysis not decided by the district court).

omitted).

“Just as reviewing courts give ‘great deference’ to the decisions of judicial officers who make probable-cause determinations, police officers should be entitled to rely upon the probable-cause determination of a neutral magistrate when defending an attack on their good faith for either seeking or executing a warrant.” *Id.* at 939.

It is the magistrate’s responsibility to determine whether the officer’s allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment. In the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination or his judgment that the form of the warrant is technically sufficient.

Leon, 468 U.S. at 921.

Burgess cites to two district court cases from other circuits to demonstrate these officers could not reasonably believe the warrant was valid. In *United States v. Clough*, the warrant authorized a search of computers for “a. text documents of any variety, including e-mail, websites, records of chat sessions, correspondence or shipping records; and b. digital images of any variety, including still images and videos.” 246 F. Supp. 2d 84, 87 (D. Me. 2003). As the court found, the warrant contained no restrictions on the search, no references to statutes, and no references to crimes or illegality. *Id.* Again, in *United States v. Fleetwood Mgm’t Ltd.*, the warrant authorized a computer search for “any and all data from the three seized computers, including, but not limited to certain types of

data relating to the Ship's operation, engineering, maintenance, pollution control equipment, navigational charts, and crew." 521 F. Supp. 2d 436 (E.D. Pa. 2007) (quotations omitted). In neither case was the search restricted in any way by the warrant. These cases only underscore the officers' reasonable reliance on the language of the warrant in this case limiting the search to evidence of drug trafficking.

Contrary to Burgess' assertions, Agent Hughes did not contact the agency attorney because he was confused about the scope of his search, he emphatically stated his concern was the delay. Hughes knew he was looking for evidence of drug possession and distribution and that such evidence would very likely be contained in the digital images on the hard drive. At each step of the investigation, the officers made every effort to comply with the law. Therefore, even if the warrant was deficient, exclusion of the evidence would not be necessary.

e. Timeliness of Search

Burgess argues the forty-four day delay in searching the computer violated the Fourth Amendment. Because this issue was not raised below, we review for plain error. Fed. R. Crim. P. 52(b).

To notice plain error under Rule 52(b), the error must:

- (1) be an actual error that was forfeited;
- (2) be plain or obvious;
- and (3) affect substantial rights, in other words, in most cases the error must be prejudicial, i.e., it must have affected the outcome

of the trial. . . . Given plain error that affects substantial rights, an appellate court should exercise its discretion and notice such error where it either (a) results in the conviction of one actually innocent, or (b) seriously affect[s] the fairness, integrity or public reputation of judicial proceedings.

Walser, 275 F.3d 985. “We apply the plain error rule less rigidly when reviewing a potential constitutional error.” *Id.*

Because the warrant had expired by its own terms prior to the time Agent Hughes began his forensic search of the hard drive, Burgess maintains the search was warrantless and violated his Fourth Amendment rights. “The Fourth Amendment does not specify that search warrants contain expiration dates.” *United States v. Sims*, 428 F.3d 945, 955 (10th Cir. 2005); *see also United States v. Johns*, 469 U.S. 478, 487 (1985) (while police officers may not indefinitely retain possession of a vehicle and its contents before they complete a valid warrantless search, the owner of the property must prove delay in the completion of a search was unreasonable because it adversely affected a privacy or possessory interest). Specific time limits are imposed by the Federal Rules of Criminal Procedure which require that a “warrant must command the officer to . . . execute the warrant within a specified time no longer than 10 days.” Fed. R. Crim. P. 41(e)(2)(A)(i). “The restrictions in Rule 41 not only ensure that probable cause continues to exist, but also that it is the neutral magistrate, not the executing officers, who determines whether probable cause continues to exist.” *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005) (quotation omitted).

But “violations of Rule 41 alone should not lead to exclusion unless (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.” *Sims*, 428 F.3d 955 (quotations omitted). The same analysis applies whether it is “a violation of the warrant itself,” or “a violation of Rule 41 per se.” *Id.* There is no evidence either of these conditions were met here.

Burgess points us to *United States v. Mitchell* where the Eleventh Circuit held an initial seizure of a hard drive was permissible, but “the detention of the hard drive for over three weeks *before a warrant was sought* constitute[d] a significant interference with Mitchell’s possessory interest.” 565 F.3d 1347, 1351 (11th Cir. 2009) (emphasis added). The court held the delay in securing a warrant was unreasonable because the government had no compelling excuse. *Id.* Here, the warrant to search was secured prior to the hard drives being seized²³ and there is no indication the officers were not diligent in executing the search. Probable cause to search was unaffected by the delay and the reasons to search the computer and hard drives did not dissipate during the month and a half the items sat in an evidence locker. Burgess has not identified any prejudice from the delay and the only readily apparent concern is that Burgess was temporarily denied

²³ The motorhome was seized before the search warrant was issued. In a broad sense, then, so was the computer equipment. But neither the laptop nor the hard drives were separately seized (or searched) until after the warrant issued.

access to his property. Moreover, any delay was due to Agent Hughes' efforts to make sure the job was done right. Our plain error analysis ends at the first step, suppression of the evidence from the computer equipment is not required – there was no error.

B. Admission of Evidence

Burgess claims the court erred in admitting sixteen digital images from the Seagate hard drive (four images admitted in the prosecution's case-in-chief, and twelve images admitted for impeachment of defense witness Dechaise – these exhibits ought not be confused with the four pictures stipulated into evidence). Early on, the defense stipulated to the admission of four pornographic pictures of a child (*see* n.4), which appeared on both the Seagate drive and the Maxtor drive (the four images on the Maxtor drive were specifically named in the indictment). The images at issue here were only on the Seagate drive.

As is his right, Burgess decided to put the government to its proofs, among them that he intentionally possessed the charged pornographic images found on the Maxtor drive, in effect denying knowledge of those images on his hard drives. The government offered the Seagate pictures in order to show Burgess was aware the Seagate drive, and inferentially the Maxtor drive, contained pornographic pictures. The file structure on both drives was highly organized, both drives contained child pornographic images and both drives had duplicate images and other files personal to Burgess. One could reasonably infer that Burgess was

aware of the contents of both drives. But the Seagate drive had an additional tie; it contained many pictures of R.C. that were sexually suggestive or borderline pornographic. Some of the photos of her had other pictures and/or lewd text superimposed upon them, suggesting Burgess had taken the photographs and/or had superimposed the text upon them. Tying him to those pictures might, inferentially, tie him to the charged child pornography. Burgess claims the admission of the pictures and text, while perhaps “marginally relevant” to show Burgess knew the child pornography was on his hard drive, were unnecessary and unduly prejudicial because their admission encouraged the jury to speculate about Burgess’ perverted interest in a young girl with whom he had a trusting relationship. (Appellant’s Br. at 24.)

We review the district court’s admission of evidence under Rules 404(b) and 403 for abuse of discretion. *United States v. Cerno*, 529 F.3d 926, 933 (10th Cir. 2008) (Rule 403), *cert. denied*, 129 S.Ct. 1905 (2009); *United States v. Mares*, 441 F.3d 1152, 1156 (10th Cir. 2006) (Rule 404(b)). “We will not reverse a district court’s ruling if it fall[s] within the bounds of permissible choice in the circumstances and is not arbitrary, capricious or whimsical.” *Mares*, 441 F.3d at 1157 (quotations omitted).

Federal Rule of Evidence 404(b) provides:

Evidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show action in conformity therewith. It may, however, be admissible for other purposes, such

as proof of . . . intent, . . . plan, knowledge, . . . or absence of mistake.

We “consider four factors in weighing the admissibility of evidence under Rule 404(b): (1) whether the evidence is offered for a proper purpose, (2) its relevancy, (3) that the probative value of the evidence is not substantially outweighed by its prejudicial effect, and (4) a limiting instruction is given if the defendant so requests.” *Mares*, 441 F.3d at 1157 “Rule 404(b) is considered to be an inclusive rule, admitting all evidence of other crimes or acts except that which tends to prove *only* criminal disposition.” *United States v. Tan*, 254 F.3d 1204, 1208 (10th Cir. 2001) (quotations omitted).

However, even if relevant and offered for a proper purpose, Rule 404(b) evidence may still be excluded under Rule 403 if its probative value “is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury. . . .” Fed. R. Evid. 403. “In determining whether evidence is properly admitted under Rule 403, we consider (1) whether the evidence was relevant, (2) whether it had the potential to unfairly prejudice the defendant, and (3) whether its probative value was substantially outweighed by the danger of unfair prejudice.” *Cerno*, 529 F.3d at 933. To be inadmissible under rule 403, evidence must do more than “damage the Defendant’s position at trial,” it must “make[] a conviction more likely because it provokes an emotional response in the jury or otherwise tends to affect adversely the jury’s attitude

toward the defendant *wholly apart* from its judgment as to his guilt or innocence [sic] of the crime charged.” *Tan*, 254 F.3d at 1211-12 (quotations omitted).

Burgess essentially argues the court erred in admitting the first four images because the government already presented evidence sufficient to show knowledge, identity and intent to possess the charged images on the Maxtor hard drive. He points to the government’s evidence suggesting he, in effect, admitted ownership of the hard drives. The numerous photos of Burgess and his home along with his personal correspondence on both the Seagate and Maxtor hard drives connected him to both drives and some of the non-pornographic photos found on the Maxtor drive were posted on Burgess’ website. Therefore, according to Burgess, the highly prejudicial nature of the evidence relating to R.C. which implied an improper relationship with a minor was not “vital” to the government’s proof. *See United States v. Garot*, 801 F.2d 1241, 1247 (10th Cir. 1986) (“exhibits were vital to proof of appellants’ knowledge”). Thus, Burgess maintains the images and text were far more prejudicial than probative and allowed the jury to convict Burgess, not for possession and transportation, but for other uncharged crimes. Although it may be a factor, the test is not necessarily whether the evidence is vital to the government’s case. Vitality is often a matter of perspective. Within limits delineated in the Federal Rules of Evidence the government is entitled to introduce all relevant, probative evidence at its disposal. The defense cannot be heard to complain that the government has produced too much evidence of guilt.

The Rule 403 test balances the probative value of (not necessarily the need for) the evidence against its potentially unfairly prejudicial effect. That balancing is for the trial judge. The remaining twelve images, some with accompanying text, were not offered until Dechaise testified that Burgess had no opportunity to take the pictures of the girls and her suggestion that the girls took the pictures themselves. These twelve pictures were much like the four previously admitted. According to the government, they were admissible to rebut the testimony of defense witnesses who testified as to the defendant's exemplary conduct around children. These witnesses testified they had never seen Burgess behave inappropriately with children and could not believe the man they knew as David Burgess would be capable of possessing vast amounts of child pornography. The government also claims they were admissible to impeach Deshaise's testimony – that Burgess was not alone with the young girls and the girls were sufficiently chaperoned during the motorcycle rally. Burgess further complains these photos were admitted without a limiting instruction. Such an instruction, however, was never requested.

In *United States v. Schene*, we affirmed the district court's admission of uncharged child pornography images to show intent and knowledge. 543 F.3d 627, 643 (10th Cir. 2008). We held the evidence was relevant and proper, specifically noting the district court gave a limiting instruction on the matter. *Id.*; see also *United States v. Simpson*, 152 F.3d 1241, 1249 (10th Cir.1998)

(affirming the district court's decision to admit similar evidence "to prove that (1) [the defendant's] possession of child pornography on his computer was not a mistake or accident, and (2) he had knowledge of the nature of the material he was receiving."). We agree the first four pictures were admissible to show Burgess' knowledge and possession. As in *Schene* and *Simpson*, the district court here carefully reviewed the entirety of the evidence the government wished to offer and excluded all but what the court believed necessary to government's case. In addition, the court gave an instruction prior to the introduction and in the instruction package sent to the jury explaining the very limited purpose for which it was offered and admonishing the jury to consider it for no other purpose. We find no abuse of discretion.

The twelve additional photos with accompanying text is a closer call. Their value for impeachment may have been cumulative; these twelve pictures were much the same as the four pictures previously admitted over Burgess' objection. But the government's position was that Burgess took the photographs. Its arguments in that regard were undermined by the testimony of one of R.C.'s companions at Winnemucca; the girl said she took the pictures. So the superimposed captions on the photographs, suggesting Burgess took or edited them, gained new importance and some of the twelve new photos contained captions not present in the other four.

On the other hand Burgess' conduct with real children was not the issue in this trial; nor was his conduct at the motorcycle rally. The government does not explain why it was necessary to introduce twelve rather than one or two additional images for impeachment purposes (especially given the district court's determination that the four stipulated images and four additional Seagate images were sufficient to prove Burgess' intent and lack of mistake). Nonetheless, we "afford great deference to the district court; review of a cold record is a poor substitute for a trial judge's intimate familiarity with the evidence and its role in the context of the trial as a whole." *United States v. Hubenka*, 438 F.3d 1026, 1036 (10th Cir. 2006) (quotations omitted). Considering whether to admit "more of the same" is a judgment call best made by the trial judge. It is most difficult for us to look at a cold record and decide if eight would be sufficient or four or two. We may have reached a different conclusion but that does not make the trial court's decision an abuse of discretion.

In any event, the admission of these photographs and texts does not call into question the jury's guilty verdict. Any error in admitting the photographs was harmless. "A non-constitutional error, such as a decision whether to admit or exclude evidence, is considered harmless 'unless a substantial right of [a] party is affected.'" *United States v. Charley*, 189 F.3d 1251, 1270 (10th Cir. 1999) (quoting Fed. R. Evid. 103(a)). An error affecting a substantial right of a party is an error which had a "substantial influence" on the outcome or which leaves one

in “grave doubt” as to whether it had such effect. *United States v. Rivera*, 900 F.2d 1462, 1469 (10th Cir.1990) (quoting *Kotteakos v. United States*, 328 U.S. 750, 765 (1946)). “[W]e review the record as a whole.” *Charley*, 189 F.3d at 1270. “The question is not whether, omitting the inadmissible statements, the record contains sufficient evidence for a jury to convict the defendant,” but whether the evidence had a substantial influence on the jury’s decision. *United States v. Tome*, 61 F.3d 1446, 1455 (10th Cir. 1995).

The jury was presented with evidence Burgess possessed thousands of images of child pornography, among them the charged images, which were present on both hard drives. The hard drives also contained Burgess’ personal photos and files. All the material on both hard drives, both legal and illegal, was organized in a singular and sophisticated fashion. Putting aside all inferences of an improper fascination with R.C., no reasonable jury could have reached a conclusion other than the one reached here. There can be no doubt, let alone a grave doubt, that Burgess knowingly possessed child pornography as he traveled from Nevada into Wyoming.

C. Sentencing

Under *Gall v. United States*, the Supreme Court set the procedure for the district court’s imposition of a sentence:

[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range. As a matter of administration and to secure nationwide consistency, the Guidelines

should be the starting point and the initial benchmark. The Guidelines are not the only consideration, however. Accordingly, after giving both parties an opportunity to argue for whatever sentence they deem appropriate, the district judge should then consider all of the § 3553(a) factors to determine whether they support the sentence requested by a party. In so doing, he may not presume that the Guidelines range is reasonable. He must make an individualized assessment based on the facts presented After settling on the appropriate sentence, he must adequately explain the chosen sentence to allow for meaningful appellate review and to promote the perception of fair sentencing.

552 U.S. 38, 128 S. Ct. 586, 596-97 (2007).

We review a sentence for abuse of discretion. *Id.* at 600. We review the court’s legal conclusions de novo and its factual findings for clear error. *United States v. Kristl*, 437 F.3d 1050, 1055 (10th Cir. 2006). A sentence is procedurally unreasonable if the district court “fail[ed] to calculate (or improperly calculate[ed]) the Guidelines range, treat[ed] the Guidelines as mandatory, fail[ed] to consider the § 3553(a) factors . . . or fail[ed] to adequately explain the chosen sentence.” *Gall*, 552 U.S. at 597.

1. *Procedural Error*

a. USSG §2.G2(b)

Burgess claims the district court erred as a matter of law in interpreting USSG § 2G2.2(b)(1) to prohibit the reduction of his offense level by two points. This section provides if a defendant is convicted of a child pornography offense with a base offense level of 22, the court will decrease the offense level by two points if “the defendant’s conduct was limited to (B) the receipt or solicitation of

material involving the sexual exploitation of a minor; and (C) the defendant did not intend to traffic in, or distribute such material.” USSG § 2G2.2(b)(1). The district court determined that, because Burgess’ conduct included transportation of child pornography, not only receipt, he did not qualify for the reduction even though Burgess did not intend to distribute the material.

Burgess claims the court’s interpretation is in error because it is contrary to guideline commentary defining distribution. “Distribution” is defined as:

[A]ny act, including possession with intent to distribute, production, advertisement, and transportation, related to the transfer of material involving the sexual exploitation of a minor.

USSG § 2G2.2(b)(1)(C), cmt. n.1 (2007). Burgess argues the definition’s alignment of the word “transportation” with the concept of “transfer” of child pornography demonstrates the drafters’ intention to apply the two level reduction to defendants who transport material without intending it be transferred to anyone else.

The Sixth Circuit has rejected this argument in a case nearly identical to this one. See *United States v. Fore*, 507 F.3d 412 (6th Cir. 2007). In *Fore*, it was uncontested there was “insufficient evidence that defendant intended to ‘distribute’ the images found in his vehicle,” but the government maintained “the simple fact that defendant’s criminal conduct . . . also involved the interstate transportation of child pornography in violation of 18 U.S.C. § 2252(a)(1), disqualifie[d] defendant from receiving the reduction.” *Id.* at 415. The court

began with the plain language of the guideline, recognizing “[s]entencing guidelines should be read as they are written.” *Id.* (quotations omitted). The court stated:

The wording of U.S.S.G. § 2G2.2(b)(1) is neither complicated nor ambiguous. By its express terms, this Guideline permits a two-level reduction in the offense level only if a defendant meets three requirements: (1) his base offense level must be 22, in accordance with subsection (b)(1)(A); (2) under subsection (b)(1)(B), his conduct must be “limited” in scope of the receipt or solicitation of material involving the sexual exploitation of a minor; “and” (3) under subsection (b)(1)(C), he did not intend to traffic in or distribute such material. Here, defendant’s undisputed base offense level is 22. However, defendant has not met the second requirement because his criminal conduct was not limited to the receipt or solicitation of pornographic materials, but also encompassed the transportation of materials involving the sexual exploitation of a minor in interstate commerce in violation of 18 U.S.C. § 2252(a)(1), an offense that is separate and distinct from, and goes beyond, the mere receipt or solicitation of pornography proscribed by 18 U.S.C. § 2252(a)(4)(B). We further note that U.S.S.G. § 2G2.2(b)(1) is devoid of any language suggesting that the offense of transporting child pornography in interstate commerce otherwise qualifies for the two-level decrease in a defendant’s offense level.

Id. For these reasons, the court held the district court properly denied defendant’s request for a decrease in his base offense level. We find the Sixth Circuit’s reasoning without flaw and adopt it here. The district court did not err in denying Burgess’ request for a reduction under USSG § 2G2.2(b)(1).

b. Other Procedural Issues

On appeal, Burgess claims the district court treated the guidelines as mandatory because, at sentencing, the court stated:

I do look at the other cases that have been prosecuted before this Court and really have to look in this case at the guidelines for guidance in imposing sentence in this case and will be imposing the sentence within the guideline range that has been . . . established.

(R. Vol. II at 1025.) Burgess also claims the court failed to provide a sufficient explanation of the reasons for his sentence.

Our review of the record reveals the district court's statement regarding its intention to sentence within the guideline range followed a complete analysis of the evidence in this case as it bears on the § 3553(a) factors. The court then continued to thoroughly assess the facts relevant to Burgess' conduct. There is no evidence the court considered the guidelines mandatory or failed to consider the sentence in light of the § 3553(a) factors. Indeed, the court went well beyond what we require. *See United States v. Tindale*, 519 F.3d 1057, 1065 (10th Cir. 2008) ("A one-sentence explanation accompanying a within-guidelines sentence -- in the absence of the need to address specific § 3553(a) arguments brought to the district court's attention -- satisfies the district court's duty to impose a procedurally reasonable sentence."). The sentence is procedurally reasonable.

2. *Substantive Error*

The substantive aspect of a sentence relates to the length of the sentence and we ask "whether the length of the sentence is reasonable considering the statutory factors delineated in . . . § 3553(a)." *United States v. Hamilton*, 510 F.3d 1209, 1217-18 (10th Cir. 2007), *cert. denied*, 128 S. Ct. 1922 (2008).

Stripped to its essence, Burgess argues his sentence was too long and points to several cases and articles criticizing the guideline recommendations as too harsh compared to the five-year minimum allowed under the statute. While recognizing the district court correctly calculated Burgess' guideline range as 168 to 210 months imprisonment, he claims the court unreasonably sentenced him to 180 months because he was merely "a first-time offender prosecuted for having a private collection of pornography with him in his travels." (Appellant's Br. at 43.) We are not convinced by this characterization of the crime and the relevant conduct appropriately considered by the district court. In this case, we could, but need not, presume the district court's guidelines sentence was reasonable. *See United States v. Navarreata-Medina*, 554 F.3d 1312, 1313 (10th Cir. 2009) (a sentence falling within a correctly calculated advisory range is entitled to a rebuttable presumption of reasonableness). The district court's extensive and reasoned consideration of the facts and law is more than evident in the record. Burgess' sentence is not substantively unreasonable.

AFFIRMED.