COURT OF APPEALS OF VIRGINIA

Present: Chief Judge Felton, Judges Humphreys and Alston
Argued at Salem, Virginia

DAVID MIDKIFF, S/K/A
DAVID WILLIS MIDKIFF

v. Record No. 2393-07-3

COMMONWEALTH OF VIRGINIA

OPINION BY
CHIEF JUDGE WALTER S. FELTON, JR.
JUNE 30, 2009

FROM THE CIRCUIT COURT OF PITTSYLVANIA COUNTY
Charles J. Strauss, Judge

David W. Shreve for appellant.

Craig W. Stallard, Assistant Attorney General (Robert F. McDonnell, Attorney General, on brief), for appellee.

Following a jury trial, David Midkiff ("appellant") was convicted of one count of possession of child pornography and eighteen counts of possession of child pornography, second or subsequent offense, in violation of Code § 18.2-374.1:1. On appeal, he contends the trial court erred in denying his motion to suppress evidence seized from his home. He argues that the search warrant was invalid and that the trial court erred in applying the Leon[1] good-faith exception to find the search pursuant to that warrant was valid. He also contends the trial court erred by admitting into evidence photographic images copied from his computer's hard drive, arguing that doing so violated the best evidence rule. For the following reasons, we affirm the judgment of the trial court.

[1] United States v. Leon, 468 U.S. 897 (1984).

## I. BACKGROUND

"In reviewing the denial of a motion to suppress based on the alleged violation of an individual's Fourth Amendment rights, we consider the facts in the light most favorable to the Commonwealth. The burden is on the defendant to show that the trial court committed reversible error." Ward v. Commonwealth, 273 Va. 211, 218, 639 S.E.2d 269, 272 (2007) (citation omitted).

On August 3, 2006, pursuant to a search warrant issued earlier that day, Sergeant Rodney Thompson of the Bedford County Sheriff's Office and Investigator Boyd Arnold of the Pittsylvania County Sheriff's Office searched appellant's house for child pornography. Appellant was not home at the time the search warrant was executed.[2] However, the officers located a telephone number on his phone's "caller ID" inside his house and called him. They told appellant where they were and their purpose for being there. Appellant advised the officers that he had "purchas[ed] memberships to child pornography websites" and that child pornography was stored in "his computer." He told them where that computer was located in his house. The officers then seized the computer and sent it to the Department of Forensic Science in Richmond to determine whether child pornography was stored on the computer's hard drive. There, Kristen Scott, a digital evidence forensic scientist, located files containing suspected child pornography on the computer's hard drive. She copied those files to a data DVD. Those files were later copied to a CD from the data DVD.

In his motion to suppress the evidence seized from his home, appellant argued that the affidavit presented by the officers to the magistrate was so stale that it failed to provide probable cause to believe the items to be seized were located in his house and that the magistrate's reliance on that information to issue the search warrant was unreasonable. He also argued that

[2] The record on appeal does not indicate how the officers obtained entry into his home.

the affidavit for the search warrant was so defective as to make unreasonable any claim by the officers of good-faith reliance on the warrant under Leon. The trial court found the information in the affidavit to be stale, resulting in the warrant being defective. It nevertheless denied appellant's motion to suppress the seized evidence, finding that the officers relied in good faith on the judicially issued warrant.

At trial, the trial court admitted into evidence twelve photographic images and a CD containing four digital image files and three digital movie files, which had been reproduced from a CD which had been made from the DVD copy of the data found on the hard drive of appellant's computer. Appellant objected to the admissibility of that evidence, arguing that admitting those images violated the best evidence rule. He asserted that the best evidence rule required that the seized computer and its hard drive be brought into court and that any image files to be used as evidence be reproduced in court directly from that hard drive.

## II. ANALYSIS

### A. The Motion to Suppress

Appellant contends: (1) "the Trial Court Err[ed] in Refusing to Suppress the Evidence Seized at [his] Home on the Basis That the Information in the Affidavit for [the] Search Warrant was Deficient in That it Failed to State a Temporal Nexus or a Nexus With [his] Residence," and (2) "the Trial Court Err[ed] in It's [sic] Application of the Good Faith Exception to the Search Warrant Requirement to Salvage the Search of [his] Home."

"The Fourth Amendment of the United States Constitution requires that a search warrant be based upon probable cause." Sowers v. Commonwealth, 49 Va. App. 588, 595, 643 S.E.2d 506, 510 (2007). "[T]o support probable cause for a warrant to search a residence, an affidavit must establish, with a fair probability, a link between contraband and the residence to be searched." Id. at 596, 643 S.E.2d at 510.

Here, the affidavit for the search warrant, sworn before the magistrate by Sergeant Thompson on August 3, 2006, provided:

> [Sergeant] Rodney Thompson received a case report and evidence CD from Suffolk County, NY Police Department in reference to Operation Hardcore. In Feb. 2005, an undercover investigation into the Child Pornographic Website was begun. On 04/20/05, the Websites containing Child Pornography were seized and logs were recovered which recorded customer logon and Website activities. On 08/25/05, a forensic evaluation was performed by Det. Rory Forrestal with the Suffolk Co. Police Department of access logs (httpd-access.log and httpd-ss-request.log) pertaining to IP address 12.96.220.190. Forensic review showed this IP Address was downloading Child Pornography material from a computer having this IP address assigned. IP address is registered to Peoples Mutual Telephone Co. and an Administrative Subpoena was issued on 06/21/2005. The results advised that the IP address was registered to DAVID MIDKIFF of P.O. Box 85, Gretna, VA and physical address 123 Franklin Blvd., Gretna, VA 24557 and telephone number 434-656-9100. User Name: dav1dm. Autotrack records indicate DAVID WILLIS MIDKIFF (DOB: 06/10/1953) resides at 123 N. Franklin Street, Gretna, VA 24557. Address is located within Pittsylvania County. Investigators know from training and experience that individuals who possess, manufacture, or distribute child pornography are collectors and tend to keep their collection and not destroy it. Bedford County Sheriff's Office and Operation Blue Ridge Thunder are the Internet Crimes Against Children Task Force for the Commonwealth of Virginia and State of West Virginia. They are responsible for investigating crimes involving the Internet where the Sexual Exploitation of Children has occurred.

The affidavit described the place to be searched and listed the things to be searched for, including digital images of child pornography and any computers found in appellant's residence.

After considering the arguments of counsel, the trial court denied appellant's motion to suppress, noting that the affidavit appeared to be stale, rendering the search warrant defective, but that the officers conducting the search did so in good-faith reliance on the validity of the judicially issued search warrant. For the following reasons, we conclude the trial court did not err in denying appellant's motion to suppress.

In United States v. Leon, 468 U.S. 897 (1984), "the United States Supreme Court established a good-faith exception to the exclusionary rule, applicable when a search is conducted pursuant to a warrant subsequently determined to be defective for Fourth Amendment purposes," and "outlined four circumstances in which the good-faith exception to the exclusionary rule would not apply." Ward, 273 Va. at 222, 639 S.E.2d at 274.

> "(1) [W]hen the [magistrate] 'was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth'; (2) when 'the issuing magistrate wholly abandoned his judicial role in the manner condemned in Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979)'; (3) when 'an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable'; or (4) when 'a warrant [is] so facially deficient . . . that the executing officers cannot reasonably presume it to be valid.'"

Ward, 273 Va. at 222-23, 639 S.E.2d at 274 (quoting United States v. Perez, 393 F.3d 457, 461 (4th Cir. 2004) (quoting Leon, 468 U.S. at 923)) (alterations in original).

"'[S]uppression 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 the purposes of the exclusionary rule[,]' . . . 'to deter police misconduct.'" Polston v. Commonwealth, 255 Va. 500, 503, 498 S.E.2d 924, 925 (1998) (quoting Leon, 468 U.S. at 916, 918); see also Herring v. United States, 129 S. Ct. 695, 702 (2009) ("[t]o trigger the exclusionary rule, police [misconduct] must be sufficiently deliberate that exclusion can meaningfully deter it").

1. Judicial Role

Appellant first argues that the magistrate wholly abandoned his judicial role by examining the officer's affidavit and issuing the search warrant in a period of only two minutes after the affidavit was presented to him. We disagree.

The United States Supreme Court has held that the good-faith exception to the exclusionary rule will not apply where the issuing magistrate does not "purport to 'perform his

"neutral and detached" function and . . . serve[s] merely as a rubber stamp for the police.'" Leon, 468 U.S. at 914 (quoting Aguilar v. Texas, 378 U.S. 108, 111 (1964)). Here, Sergeant Thompson testified at the suppression hearing that, after he presented the search warrant affidavit by videoconference, the magistrate "turned his back" and "appeared to be reading the affidavit before he turned around and said that it was accepted or signed off on it." The trial court's factual finding, that "the magistrate read [and understood] the affidavit," which "really doesn't take long if you're a trained magistrate," is binding on appeal. See Ward, 273 Va. at 218, 639 S.E.2d at 272. From the record presented, we conclude that the magistrate did not wholly abandon his role as a neutral and detached judicial officer in determining from the affidavit that a search warrant should issue. See Sowers, 49 Va. App. at 603, 643 S.E.2d at 513 ("officer-affiant testified that the magistrate 'read the affidavit thoroughly,' which indicates that he considered the merits of the affidavit rather than blindly issuing the warrant").

2. Temporal and Geographical Nexus

Appellant also argues that the "warrant was so lacking indicia of probable cause as to render official belief in its existence unreasonable." He asserts that the officers lacked any reasonable basis to believe that child pornography images supposedly downloaded to a computer with his Internet protocol ("IP") address some sixteen months earlier were on a computer in his home.

"The third limitation to the Leon good-faith exception conditions reliance on the magistrate's probable-cause determination by police officers to those circumstances where that reliance is objectively reasonable." Ward, 273 Va. at 223, 639 S.E.2d at 275. "'In fact, Leon states that the third circumstance . . . prevents a finding of objective good faith only when an officer's affidavit is "so lacking in indicia of probable cause as to render official belief in its existence *entirely* unreasonable."'" Adams v. Commonwealth, 275 Va. 260, 274, 657 S.E.2d 87,

95 (2008) (quoting United States v. Bynum, 293 F.3d 192, 195 (4th Cir. 2002) (quoting Leon, 468 U.S. at 923)). In Anzualda v. Commonwealth, 44 Va. App. 764, 607 S.E.2d 749 (2005) (en banc), we noted that "as long as there is *some* indicia of probable cause in the underlying affidavit, we will apply the good faith exception [provided that] a reasonable police officer, after assessing the facts set forth in the affidavit, could have believed that the warrant was valid." Id. at 781, 607 S.E.2d at 757.

a.

The affidavit at issue here states that sometime prior to April 20, 2005 appellant is alleged to have downloaded child pornography to his computer. The affidavit also noted that "Peoples Mutual Telephone [Company]" records showed that the IP address to which the child pornography was downloaded was registered to appellant at the address to be searched. In determining whether police officers relied in good faith on a judicially issued warrant, we may "take into account information known to police officers that was not included in the search warrant affidavit." Adams, 275 Va. at 273, 657 S.E.2d at 94. Sergeant Thompson, the officer who obtained and executed the search warrant at appellant's residence, testified at the suppression hearing that information he received from the New York investigation revealed that child pornography had been downloaded to appellant's IP address March 25 through March 30 of 2005. We must determine whether a reasonable, well-trained officer, with knowledge of the alleged offense date, would have concluded the warrant, dated some sixteen months later, would be so lacking in probable cause as to render unreasonable his belief that the items described would still be located at appellant's physical address.

In his affidavit for the search warrant, Sergeant Thompson stated that, based on his training and experience as a member of the Internet Crimes Against Children Task Force, he knew that "individuals who possess, manufacture, or distribute child pornography are collectors

and tend to keep their collection and not destroy it." Based on Sergeant Thompson's training and experience in investigating child pornography, we conclude the trial court did not err in finding that the officer was not unreasonable in believing there was probable cause that the images of child pornography, downloaded sixteen months prior, could still be in appellant's possession at the physical address to which the IP address was registered. See Anzualda, 44 Va. App. at 783, 607 S.E.2d at 758-59 ("affidavit's failure to identify the specific dates upon which the described events occurred does not . . . render the affidavit so lacking in probable cause that a reasonable police officer could not have concluded that it was valid"); see also United States v. Prideaux-Wentz, 543 F.3d 954, 961 (7th Cir. 2008) (applying good-faith exception where a search warrant for digital images of child pornography was found stale, noting that "most child pornographers do not dispose of their collections"); United States v. Ricciardelli, 998 F.2d 8, 12 n.4 (1st Cir. 1993) ("history teaches that [child pornography] collectors prefer not to dispose of their dross, typically retaining obscene materials for years"); United States v. Rugh, 968 F.2d 750, 753-54 (8th Cir. 1992).[3]

b.

Appellant also argues that it was unreasonable for the officers to believe that the images of suspected child pornography would be found at his residence, asserting "there was absolutely no connection" between the IP address in the affidavit and his residence.

"For the [Leon] good faith [exception] to apply, the affidavit must provide some nexus between the evidence sought and the place to be searched." Sowers, 49 Va. App. at 604, 643 S.E.2d at 514. Here, the affidavit for the search warrant stated that images of child pornography

[3] Courts have also found that "[i]nformation a year old is not necessarily stale as a matter of law, especially where child pornography is concerned." United States v. Newsom, 402 F.3d 780, 783 (7th Cir. 2005); see also United States v. Harvey, 2 F.3d 1318, 1323 (3d Cir. 1993) (two to fifteen months not stale); United States v. Rabe, 848 F.2d 994 (9th Cir. 1988) (two years not stale).

were downloaded to an IP address registered through an Internet service provider to appellant, specifically listing his residence as the physical address associated with the Internet account.[4] While the affidavit here did not contain the date range the IP address at issue was assigned to appellant at his listed residence, we conclude it did "establish a nexus – however slight – between the item sought and the premises to be searched." Anzualda, 44 Va. App. at 784, 607 S.E.2d at 759 (applying good-faith exception where officer reasonably concluded contraband could still be found at accused's residence); see, e.g., United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) ("collectors . . . of child pornography value their sexually explicit materials highly, 'rarely if ever' dispose of such material, and store it 'for long periods' in a secure place, typically in their homes").

From the record on appeal, we conclude the trial court did not err in finding that the officers conducting the search pursuant to the judicially issued warrant "acted in good faith, and the deterrent function of the exclusionary rule would not be served by excluding the evidence seized." Ward, 273 Va. at 225, 639 S.E.2d at 276. Accordingly, we hold that the trial court did not err in denying appellant's motion to suppress the seized evidence.

---

[4] An IP address is a string of four integer numbers between 0 and 255 separated by periods that identifies the location of a specific computer connected to the Internet. While many Internet connections are permanent and, thus, are assigned fixed IP addresses, the IP address assigned to a personal computer accessing the Internet through a portal site is drawn from a pool of open addresses and identifies that computer only during the time that computer is connected to the Internet.

Am. Online, Inc. v. Nam Tai Elecs., Inc., 264 Va. 583, 587 n.3, 571 S.E.2d 128, 130 n.3 (2002). The record does not contain the type of IP address registered to appellant.

B. The Best Evidence Rule

1.

Appellant also contends the trial court erred in admitting into evidence the sixteen images and three digital movie files of suspected child pornography purportedly recovered from his computer. He argues that evidence was not the best evidence of data stored on his computer as it was "at least third generation removed from [his] computer hard drive." He asserts on appeal, as he did in objecting to that evidence being admitted at trial, that the hard drive of his computer, allegedly containing the offending images, is "what needs to be produced under the best evidence rule."[5]

We note that "[t]he admissibility of evidence is within the broad discretion of the trial court, and a ruling will not be disturbed on appeal in the absence of an abuse of discretion." Blain v. Commonwealth, 7 Va. App. 10, 16, 371 S.E.2d 838, 842 (1988). For the following reasons, we conclude the trial court did not abuse its discretion in admitting the images and digital movies of child pornography recovered from the computer hard drive seized from appellant's residence.

In Virginia, the best evidence rule has been limited to writings. Meade v. Commonwealth, 177 Va. 811, 815, 12 S.E.2d 796, 798 (1941) (best evidence rule in Virginia does not apply to "'anything but writings'" (quoting John H. Wigmore, Wigmore on Evidence §§ 1179-1183 (2d ed. 1923))); Randolph v. Commonwealth, 145 Va. 883, 889, 134 S.E. 544, 546 (1926) ("'where the contents of a *writing* are desired to be proved, the writing itself must be produced, or its absence sufficiently accounted for before other evidence of its contents can be

[5] Appellant does not argue that the photographic images admitted into evidence were not child pornography, nor does he argue that those images inaccurately reflect the digital image files contained on the DVD copy, and subsequent reproductions, Scott made of the hard drive of his computer. On appeal, he states that the contested evidence is "disgusting images of children in sexually explicit poses."

admitted'" (quoting 1 Greenleaf on Evidence 682 (16th ed. 1899)) (emphasis added)); see also Charles E. Friend, The Law of Evidence in Virginia § 16-1 (6th ed. 2003) ("*The rule applies only to writings or documents*. It is not applied to other forms of evidence."). We conclude the images and digital movies of child pornography admitted as evidence did not constitute "writings" under the best evidence rule. See Brown v. Commonwealth, 54 Va. App. 107, 116, 676 S.E.2d 326, ___ (2009) ("best evidence rule in Virginia applies only to writings and, clearly, a videotape is not a writing"); see also Friend, supra, § 15-1 (defining "writing" as "letters, contracts, deeds, and other documents normally thought of as 'writings,' or 'documents'").

2.

Appellant's objection to the admissibility of the evidence of the digital images, in effect, is couched in terms of "reliability," that is, whether the photographic images produced at trial were reliable depictions of what was stored on his computer's hard drive seized from his home.

This Court has recognized, as have other courts, that "[t]he potentially limitless application of computer technology to evidentiary questions will continually require legal adaptation." Penny v. Commonwealth, 6 Va. App. 494, 499, 370 S.E.2d 314, 317 (1988). "When a computer is used to create a data compilation, how much information will be required about data input and processing to authenticate the output will depend on the nature and completeness of the data, the complexity of the manipulation, and the routineness of the operation." 2 McCormick on Evidence § 227 (Kenneth S. Broun et al. eds., 6th ed. 2006). "'In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise.'" Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543 (D. Md. 2007) (quoting Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence § 900.06[3] (Joseph M. McLaughlin ed., 2d ed. 1997)).

Here, appellant admitted to officers that he had "purchas[ed] memberships to child pornography websites" and that child pornography was stored in "his computer." He "stipulate[d] the chain of custody to [that] computer" from the time it was seized from his residence to the time it was analyzed by Kristen Scott, a forensic scientist with the digital evidence section of the Department of Forensic Science. Appellant also "stipulate[d]" to Scott's expertise in digital forensic science. Scott testified that when she received appellant's computer, she made "an image" of one of its hard drives. She testified that a "hard drive is the basic storage system of a computer" and that an "image of a hard drive is a bit for bit copy. . . . When you make a bit for bit image of a hard drive you get the exact same thing each time." Relying on her training in examining computers, specifically in basic data recovery and acquisition, Scott used a data program and searched the data DVD copy she made of appellant's hard drive for "JPEG[6] as well as other types of image files."

Scott testified that she recovered digital image and movie files of suspected child pornography from the DVD copy of the hard drive of appellant's computer. She then gave that data DVD to Investigator Arnold. From that data DVD, Investigator Arnold copied sixteen digital image files and three digital movie files onto a CD for use at trial. Scott testified that the files Investigator Arnold copied from the data DVD she gave him were considered originals, "[b]ecause in computers and bit for bit digital copying, there is no such thing as generation. Each copy you create from the original is considered forensically to be an original."

After reviewing each of the photographic images offered into evidence at trial, Scott testified that she "recovered these images from [appellant's] computer." When asked whether the photographic images at trial "fairly and accurately represent what [she] found on [appellant's] computer as far as . . . how those images looked when [she] saw them," Scott

[6] She testified that a JPEG is a digital photograph file.

testified, "Yes, they did." She also testified that she did not change the file names of the digital image files and that the names listed on each photographic image at trial accurately corresponded to the names of each digital image file she recovered from appellant's computer. Investigator Arnold, likewise, testified that the photographic images offered at trial were the same as the digital image files he viewed on a data DVD from Scott.[7]

We have previously noted that a "computer decodes electronic records, converts them into a format understood by users and either prints them or displays them on a terminal. A person who can verify that [they] are authentic can present the evidence by testifying about what he saw displayed or by presenting a printed copy of the display."[8] Lee v. Commonwealth, 28 Va. App. 571, 577, 507 S.E.2d 629, 632 (1998).

Importantly, after considering the testimony at trial, the trial court found that four of the sixteen photographic images, offered as a collage, were inadmissible because they had been "combined" and did not appear as they did on appellant's computer.[9] It found the remaining twelve photographic images reliable reproductions of the digital image files on appellant's computer hard drive and admitted them into evidence.

---

[7] At trial, appellant "stipulate[d] that [both Scott's and Investigator Arnold's] testimony would be, . . . [the three digital movie clips] appear to be the same clips," by file name, "2.avi," "Lolitas R@YGOLD.avi," and "RAYGOLD_predoctor," recovered from a digital copy of the hard drive of appellant's computer.

[8] See also United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001) ("computer printouts were not the result of a 'process or system used to produce a result'; they were merely printouts of preexisting records that happened to be stored on a computer"); 2 McCormick on Evidence, supra, § 227 n.14; cf. Penny, 6 Va. App. at 498-99, 370 S.E.2d at 317 (where computer performs complex scientific analysis of data, "legal analysis concerning the results' admissibility . . . should focus on reliability of the device itself").

[9] It admitted those four images in their original individual digital image file format, as well as the three digital movie files, on a CD.

We conclude that the trial court did not err in finding that the images it admitted at trial were fair and accurate representations of the digital image files of child pornography on appellant's computer hard drive. Appellant admitted to the investigating officers that he purchased memberships in child pornography websites and that images of child pornography were on his computer. Accordingly, we conclude that the trial court did not abuse its discretion in admitting into evidence the images and digital movies reproduced from the digital files recovered from appellant's computer.

## III. CONCLUSION

For the foregoing reasons, we affirm appellant's convictions of possession of child pornography in violation of Code § 18.2-374.1:1.

Affirmed.