#26354-a-DG

**2013 S.D. 95**

IN THE SUPREME COURT
OF THE
STATE OF SOUTH DAKOTA

* * * *

STATE OF SOUTH DAKOTA, Plaintiff and Appellee,

v.

JAMES DUANE RILEY, Defendant and Appellant.

* * * *

APPEAL FROM THE CIRCUIT COURT OF
THE SEVENTH JUDICIAL CIRCUIT
CUSTER COUNTY, SOUTH DAKOTA

* * * *

THE HONORABLE JEFF W. DAVIS
Judge

* * * *

MARTY J. JACKLEY
Attorney General

TIMOTHY J. BARNAUD
Assistant Attorney General
Pierre, South Dakota

Attorneys for plaintiff
and appellee.

PAUL R. WINTER
MATTHEW L. SKINNER of
Skinner & Winter, Prof., LLC
Rapid City, South Dakota

Attorneys for defendant
and appellant.

* * * *

ARGUED ON MARCH 18, 2013
REASSIGNED AUGUST 16, 2013
OPINION FILED **12/18/13**

GILBERSTON, Chief Justice (on reassignment).

[¶1.] James Riley was convicted by a jury of possessing child pornography in violation of SDCL 22-24A-3(3) and was sentenced to eight years in the penitentiary. Riley now appeals his conviction, arguing the evidence was insufficient to establish he possessed child pornography. We affirm.

## FACTS AND PROCEDURAL HISTORY

[¶2.] To combat Internet-based child exploitation and abuse, the South Dakota Internet Crimes Against Children Task Force (Task Force) conducts undercover online investigations to identify individuals distributing or possessing child pornography. Detectives from the Task Force begin their investigation by using software that populates a list of internet protocol (IP) addresses[1] that recently possessed visual depictions of child pornography. Detectives then input those IP addresses into an enhanced version of LimeWire[2] developed by the FBI, known as

---

1. "[An] IP address is a unique identifier assigned by an Internet service provider . . . to a subscriber that can be used to determine the physical location of the subscriber[.]" *United States v. Conner*, 521 F. App'x 493, 495 (6th Cir. 2013).

2. LimeWire is a publicly available peer-to-peer file-sharing program that allows users to download a file directly from other users for free. As recently explained by the Ninth Circuit:

> LimeWire . . . connect[s] network participants directly and allow[s] them to download files from one another. To download a file, a LimeWire user opens the application and inputs a search term. LimeWire then displays a list of files that match the search terms and that are available for download from other LimeWire users. When a user downloads a file using the LimeWire network, he or she causes a digital copy of a file on another user's computer to be transferred to his or her own computer.

(continued . . . )

"enhanced peer-to-peer software" (EP2P). EP2P allows detectives to view and download files that a particular IP address has available for download because, unlike LimeWire, which pieces together file fragments from multiple IP addresses that are currently using the file-sharing program, EP2P is a single-source download program that limits downloads to a specific IP address.

[¶3.] Using the special software employed by the Task Force, Detective Derek Kuchenreuther conducted an undercover investigation on October 20, 2009, to locate individuals distributing or possessing visual depictions of child pornography. His search revealed that 79 video files with titles suggestive of child pornography were being shared through LimeWire by an IP address in Hermosa, South Dakota. Kuchenreuther downloaded an entire video file (full video) and confirmed that it contained child pornography. He also downloaded a portion of a video file (partial video), which did not contain child pornography, but depicted an adult female removing the pants of a female child. Although the partial video did not portray child pornography, based on prior child pornography investigations, Kuchenreuther recognized the video file as one that contained child pornography.

[¶4.] After serving a subpoena on the Internet service provider, Kuchenreuther traced the IP address to James Riley's residence. Based on this

---

( . . . continued)

> *United States v. Flyer*, 633 F.3d 911, 913 (9th Cir. 2011) (internal citations omitted). By default, LimeWire stores downloaded files in a shared folder that is accessible to other LimeWire users. *United States v. Budziak*, 697 F.3d 1105, 1108 (9th Cir. 2012).

information, an agent with the South Dakota Division of Criminal Investigation, Brent Gromer, applied for and obtained a warrant to search Riley's residence.

[¶5.] On January 15, 2010, Gromer and several other investigators executed the warrant at Riley's residence. Lori Wenzlick, Riley's girlfriend, was the only person home at that time. Wenzlick informed investigators that Riley was out-of-state, had his computer with him, and would return home around midnight. Gromer advised Wenzlick that they would return the next day at approximately 6:00 a.m. to execute the search warrant and instructed Wenzlick not to tell Riley. Riley returned home at approximately 1:00 a.m. on January 16, 2010. Contrary to Gromer's instructions, Wenzlick informed Riley that investigators had been at the residence and that they would be returning at 6:00 a.m.

[¶6.] At approximately 6:30 a.m., investigators executed a second search warrant at Riley's residence. Riley, a former IBM employee of 25 years, was visibly intoxicated when investigators arrived, but agreed to speak with Gromer. Riley admitted he used LimeWire to download music, "glanced at" child pornography, and saw the downloaded portion of the partial video. He denied seeing the full video. Further, Riley remarked, "[i]t's gone[,]" when Gromer mentioned that he knew Riley was sharing 79 video files containing child pornography.[3] However, Riley never admitted he downloaded, possessed, or purposefully deleted videos of child pornography. Investigators seized a laptop computer, two thumb drives, a MP3

3. Riley also stated he "looked at it" and "didn't know it was illegal to look." It is unclear whether Riley was referring to child or adult pornography when he said he "looked at it," but the record is clear Riley was referring to child pornography when he said he "didn't know it was illegal to look."

player, and three DVDs, but did not take a second computer that was also located in Riley's residence.

[¶7.] Investigators completed a forensic analysis of the items seized from Riley's residence. No visual depiction of child pornography was found on any of the items seized by investigators, nor were LimeWire or other peer-to-peer programs discovered on Riley's computer.

[¶8.] In July 2010, a grand jury indicted Riley on two counts of possession of child pornography in violation of SDCL 22-24A-3(3). Count I alleged possession of the full video and Count II alleged possession of the partial video.

[¶9.] A jury trial was held in January 2012. At trial, Kuchenreuther described his undercover investigation, and Gromer testified that he interviewed Riley while executing the search warrant at Riley's residence. Additionally, Wenzlick testified that Riley was the only household member who used the computer,[4] that he used the Internet, and that he used LimeWire to download music. Wenzlick also testified that when Riley arrived home on January 16, 2010, she informed him that investigators had been at the home and would be returning at 6:00 a.m. At some point, Riley informed Wenzlick that his computer had crashed in California. Wenzlick told the jury that she observed Riley access his computer after he had returned home, but before investigators arrived, but was unable to determine what Riley was doing with the computer.

4. Wenzlick also told the jury that two computers were present at the residence but only one was functioning.

[¶10.] Russ Eisenbraun, a detective with the Rapid City Police Department, testified about the results of the forensic analysis. Eisenbraun explained that neither evidence of LimeWire nor any visual depiction of child pornography was found on Riley's computer, including the unallocated space[5] and cache.[6] According to Eisenbraun, his examination revealed that there were several bad sectors[7] on the

---

5. The Ninth Circuit defined unallocated space as:

> space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software. Such space is available to be written over to store new information. Even if retrieved, all that can be known about a file in unallocated space (in addition to its contents) is that it once existed on the computer's hard drive. All other attributes—including when the file was created, accessed, or deleted by the user—cannot be recovered.

*Flyer*, 633 F.3d at 918.

6. The cache is a folder which stores a copy of webpages viewed by a user.

> When a computer user views a webpage, the computer automatically stores a copy of that webpage in a folder known as the cache. The copy is retained in a file called a temporary internet file. When the user revisits that webpage, the computer can load the page more quickly by retrieving the version stored in the cache. The computer automatically deletes temporary internet files when the cache—which has limited storage space—becomes full. Once full, the computer begins to delete the files on a "first in, first out" basis. Users also may manually delete files from the cache, or use commercial software to remove the files.

*United States v. Moreland*, 665 F.3d 137, 142 (5th Cir. 2011) (internal citations omitted).

7. Riley's expert witness, Dan Meinke, testified that bad sectors are sectors on a computer's hard drive that have been physically damaged.

computer and that the operating system on Riley's computer had been reinstalled at approximately 5:37 a.m. on January 16, 2010. Eisenbraun explained that a computer does not automatically reinstall the operating system, but has to be directed to do so, and that the reinstallation could override any information previously contained on the unallocated space of the hard drive. Further, Eisenbraun testified that his examination revealed a significant amount of music was taken off the computer and transferred to thumb drives shortly before the operating system reinstallation occurred and that the computer only had a basic file structure that made it look "brand new."

[¶11.] Eisenbraun also testified that he used a screen shot from Kuchenreuther's investigation to perform a text-string search, which searched Riley's computer for strings of words corresponding to file names generated during Kuchenreuther's investigation. Eisenbraun's search produced several hits, meaning that he found multiple text strings within the unallocated space of the computer's hard drive that matched a file name or variation of a file name generated during Kuchenreuther's investigation. Eisenbraun also found multiple text strings that matched the file name or a variation of the file name for the full video. Eisenbraun explained that a text string was "a file title clearly that suggests child pornography. It doesn't mean that it is and doesn't mean that it isn't. It's just what it is, a text that suggests."

[¶12.] Riley's expert witness, Dan Meinke, testified that numerous users and computers can use one IP address, and an investigator, such as Kuchenreuther, would have no way of knowing by simply looking at an IP address "how many

devices are behind [the] IP address" or "who's using it." Meinke also testified that Eisenbraun appeared to have done a careful investigation of Riley's computer. He agreed with Eisenbraun that Riley's computer contained numerous bad sectors and that the operating system had been reinstalled. Meinke explained that "[t]he installation of an operating system on a computer in itself would not delete any – would not delete most user created files, not to say it couldn't delete some of them[,]" and that as the owner of a computer store he "reinstall[s] operating systems on customer computers on a daily basis without ever losing their data." Finally, Meinke explained that LimeWire users can assign a file whatever name and file extension they wish. As a result, a Microsoft Word document could appear to be a video file and vice versa.

[¶13.] Riley moved for a judgment of acquittal at the close of the State's case-in-chief and renewed the motion prior to closing arguments. Both motions were denied. The jury ultimately found Riley guilty of Count I, relating to the full video, but failed to reach a verdict as to Count II, relating to the partial video. Riley was sentenced to eight years in the penitentiary. He appeals the trial court's denial of his motion for judgment of acquittal.

## STANDARD OF REVIEW

[¶14.] "We review the denial of a motion for judgment of acquittal as a question of law under the de novo standard." *State v. Danielson*, 2012 S.D. 36, ¶ 8, 814 N.W.2d 401, 405 (quoting *State v. Overbey*, 2010 S.D. 78, ¶ 12, 790 N.W.2d 35, 40). "On appeal, the question before this Court is whether the evidence was sufficient to sustain the conviction[]." *Id.* (quoting *Overbey*, 2010 S.D. 78, ¶ 12, 790

N.W.2d at 40). "In measuring the sufficiency of the evidence, we ask whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Id.* (quoting *State v. Stark*, 2011 S.D. 46, ¶ 21, 802 N.W.2d 165, 172). "We accept the evidence and the most favorable inferences fairly drawn therefrom, which will support the verdict." *Id.* (quoting *Stark*, 2011 S.D. 46, ¶ 21, 802 N.W.2d at 172). Finally, "[w]e will not resolve conflicts in the evidence, assess the credibility of witnesses, or reevaluate the weight of the evidence." *State v. Hauge*, 2013 S.D. 26, ¶ 12, 829 N.W.2d 145, 149 (quoting *State v. Morgan*, 2012 S.D. 87, ¶ 10, 824 N.W.2d 98, 100) (internal quotations marks omitted).

**ANALYSIS AND DECISION**

[¶15.] Riley was convicted of possession of child pornography in violation of SDCL 22-24A-3(3). For the crime of possession of child pornography, the State must prove, beyond a reasonable doubt, that the individual "[k]nowingly possesse[d], distribute[d], or otherwise disseminate[d] any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such act." SDCL 22-24A-3(3). Riley argues the trial court erred in denying his motion for judgment of acquittal because the evidence was insufficient to establish the possession necessary to support a conviction under SDCL 22-24A-3(3). Riley emphasizes the fact that no visual depiction of child pornography was found on his computer.

[¶16.] "The term 'possession' is not statutorily defined in South Dakota." *State v. Barry*, 2004 S.D. 67, ¶ 9, 681 N.W.2d 89, 92 (citing *State v. Goodroad*, 442 N.W.2d 246, 251 (S.D. 1989)). However, we have previously stated that

"[p]ossession requires that an individual be aware of the presence and character of the [contraband] and intentionally and consciously possess such [contraband]." *State v. Mattson*, 2005 S.D. 71, ¶ 22, 698 N.W.2d 538, 547 (quoting *State v. Hanson*, 1999 S.D. 9, ¶ 16, 588 N.W.2d 885, 890). Possession can be either actual or constructive. *Hauge*, 2013 S.D. 26, ¶ 13, 829 N.W.2d at 150 (citing *Overbey*, 2010 S.D. 78, ¶ 28, 790 N.W.2d at 43). Constructive possession is the "dominion or control" over either the contraband or the premises in which the contraband was found. *Barry*, 2004 S.D. 67, ¶ 9, 681 N.W.2d at 92-93 (citing *Goodroad*, 442 N.W.2d at 251).

[¶17.] Generally, in cases where courts are called upon to review a defendant's conviction for possession of child pornography, a visual depiction of child pornography is found on the defendant's computer. Here, the State presented no direct evidence that Riley possessed the full video, but rather relied on circumstantial evidence to convict Riley. Thus, the relevant inquiry is whether there is substantial evidence establishing that Riley exercised dominion or control over the video to support his conviction for possession of child pornography.

[¶18.] "If the evidence, including circumstantial evidence and reasonable inferences drawn therefrom sustains a reasonable theory of guilt, a guilty verdict will not be set aside." *Hauge*, 2013 S.D. 26, ¶ 12, 829 N.W.2d at 149 (quoting *Morgan*, 2012 S.D. 87, ¶ 10, 824 N.W.2d at 100). "All elements of a crime, including intent . . . , may be established circumstantially." *State v. Shaw*, 2005 S.D. 105, ¶ 45, 705 N.W.2d 620, 633 (quoting *State v. Guthrie*, 2001 S.D. 61, ¶ 48, 627 N.W.2d 401, 421). "[P]ossession may [also] be proved by circumstantial evidence." *Barry*,

2004 S.D. 67, ¶ 11, 681 N.W.2d at 93. "Direct and circumstantial evidence have equal weight." *State v. Webster*, 2001 S.D. 141, ¶ 13, 637 N.W.2d 392, 396 (citation omitted). In fact, in some instances "circumstantial evidence may be more reliable than direct evidence." *Id.*

[¶19.] The "settled law on reasonable doubt suffices to determine if circumstantial evidence is sufficient to prove the elements of an offense." *State v. LaPlante*, 2002 S.D. 95, ¶ 32, 650 N.W.2d 305, 313 (citation omitted). "The State is not required 'to exclude every hypothesis of innocence' in order to support a conviction based [on] circumstantial evidence." *Shaw*, 2005 S.D. 105, ¶ 45, 705 N.W.2d at 633 (quoting *Guthrie*, 2001 S.D. 61, ¶ 49, 627 N.W.2d at 421). "Instead, this Court is required to 'review the evidence cumulatively to see whether in its totality it is enough to rule out'" reasonable doubt. *Id.* (quoting *Guthrie*, 2001 S.D. 61, ¶ 49, 627 N.W.2d at 421).

[¶20.] The dissent reasons that each piece of evidence is, by itself, susceptible to an innocent explanation and therefore, the evidence cannot sustain a guilty verdict. However, the required cumulative review of the evidence "precludes this sort of divide-and-conquer analysis." *See United States v. Arvizu*, 534 U.S. 266, 274, 122 S. Ct. 744, 751, 151 L. Ed. 2d 740 (2002) (noting that a review under the totality of the circumstances test precludes evaluating each factor in isolation in order to create a susceptible innocent explanation that entitles that factor to no weight). The applicable standard of review is "whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Danielson*, 2012

S.D. 36, ¶ 8, 814 N.W.2d at 405 (citation omitted). This Court is precluded from reevaluating the weight of the evidence. *Id.*

[¶21.] Here, Kuchenreuther testified that he downloaded the full video from the IP address leased to Riley. Kuchenreuther explained to the jury that the video file was located in a shared folder within the LimeWire file-sharing program that was using Riley's IP address. Riley admitted that he used LimeWire and introduced no evidence that someone else was using his IP address. Riley's girlfriend testified that he used LimeWire and that he was the only one who used the computer and the Internet at their home. She further testified that only one computer in the house was working. From this evidence, the jury could reasonably infer that Riley had exclusive access to the computer associated with his IP address and downloaded the full video. Moreover, during Riley's interview with Gromer, Riley admitted that he glanced at child pornography, and his responses to Gromer's questions suggested Riley was aware that pornographic videos had been on his computer. For example, when Gromer asked Riley how many images or pictures[8] he has seen, Riley responded, "You mean videos? A whole bunch."

[¶22.] Further, Riley's girlfriend testified that she informed Riley at 1:00 a.m. that investigators had been at the house and that they would return at 6:00 a.m. She also testified that after she informed Riley the officers would be returning, and before the officers arrived, she observed Riley working on his computer but did not know what he was doing. The jury heard testimony from Eisenbraun that the

8. Gromer did not specify whether he was referring to adult pornography or child pornography when he asked this question.

forensic evaluation revealed the computer's operating system had been reinstalled at 5:37 a.m., approximately one hour before officers arrived at Riley's residence. Eisenbraun testified that in his opinion, this reinstallation likely overwrote the files containing videos of child pornography on Riley's computer. Additionally, Riley admitted to using LimeWire, but LimeWire was not found on his computer. Eisenbraun also testified that a significant amount of music had been taken off of Riley's computer prior to the operating system reinstallation. From this evidence, the jury could reasonably infer Riley deleted a number of items, including the full video Kuchenreuther downloaded on October 20, 2009, and reinstalled the operating system before law enforcement arrived, effectively deleting the video.

[¶23.] Finally, Eisenbraun testified that he used a screen shot from Kuchenreuther's investigation to perform a text-string search, which searched Riley's computer for text strings corresponding to file names generated during Kuchenreuther's investigation. Eisenbraun found multiple text strings, including text strings related to the full video, on the unallocated space of Riley's computer. Eisenbraun testified that these text strings, or file names, "clearly . . . suggest[] child pornography." From this evidence, the jury could reasonably infer that child pornography had been present on Riley's computer on October 20, 2009, when Kuchenreuther located the files and successfully downloaded the full video.

[¶24.] Reviewed cumulatively, an inference of guilt is rational when we consider: (1) the reinstallation of the operating system, the deletion of numerous other files, and Riley's past employment with IBM together with Riley's knowledge that the police were coming to search his computer, (2) Riley's admission that he

used LimeWire and "glanced at" child pornography, (3) his statement that "it's gone" in regards to the 79 video files containing child pornography, (4) the text strings suggesting child pornography, and (5) the evidence that he was the only user of the computer at issue on an IP address that was downloading child pornography. In reviewing the evidence as a whole and in the light most favorable to the verdict, we conclude there was sufficient evidence for a rational jury to find Riley guilty beyond a reasonable doubt.

[¶25.] Judgment of conviction is affirmed.

[¶26.] KONENKAMP, and ZINTER, Justices, concur.

[¶27.] SEVERSON, and WILBUR, Justices, dissent.

WILBUR, Justice (dissenting).

[¶28.] I respectfully dissent. The circuit court erred in denying Riley's motion for judgment of acquittal because a rational trier of fact could not have "found the essential elements of the crime beyond a reasonable doubt." *State v. Danielson*, 2012 S.D. 36, ¶ 8, 814 N.W.2d 401, 405 (quoting *State v. Stark*, 2011 S.D. 46, ¶ 21, 802 N.W.2d 165, 172). One of the essential elements of possession of child pornography cannot be found beyond a reasonable doubt—"any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act." SDCL 22-24A-3(3). Indeed, no visual depiction of child pornography was ever found in Riley's possession or on devices possessed by Riley. And while "any visual depiction" of child pornography may be inferred from circumstantial evidence, "a conviction cannot be sustained on mere suspicion or possibility of guilt." *State v.*

*Toohey*, 2012 S.D. 51, ¶ 22, 816 N.W.2d 120, 130 (quoting *United States v. Plenty Arrows*, 946 F.2d 62, 65 (8th Cir. 1991)).

[¶29.] The circumstantial evidence presented here, even when viewed cumulatively and in a light most favorable to the State, did not establish, beyond a reasonable doubt, the presence of any visual depiction of child pornography in Riley's possession. The inferences of guilt that the majority uses to support its conclusion are subject to speculation.

[¶30.] In arguing that circumstantial evidence supports Riley's conviction of possession of child pornography, the majority contends that Riley "was the only user of the computer at issue on an IP address that was downloading child pornography." However, the fact that Riley had exclusive access to the seized computer fails to establish that Riley's computer was connected to the IP address Kuchenreuther identified on October 20, 2009. Kuchenreuther was unable to determine what device was connected to the IP address on the date of his investigation, where the device was located, or who was using the device. Further investigation revealed nothing on Riley's hard drive linking it to the videos Kuchenreuther discovered on October 20, 2009.

[¶31.] Additionally, Riley's statements do not establish that he possessed visual depictions of child pornography, specifically the full video, on his computer. In support of its argument that Riley's statements are inferences of his guilt, the majority opinion emphasizes Riley's statement that "It's gone[,]" when investigators questioned Riley about the 79 video files seen by Kuchenreuther on October 20, 2009, and Riley's statement to investigators that he had viewed the *partial* video.

These "admissions," however, hardly reach the level of admission present in a similar case where the defendant was convicted and no visual depiction was found on the defendant's computer. *See State v. Garbaccio*, 214 P.3d 168, 172 (Wash. Ct. App. 2009) (noting that at trial, where the defendant was convicted of possession of child pornography when no visual depiction of child pornography was found on the defendant's computer, "[the defendant] and the State entered into a stipulation that [the defendant] had in fact downloaded images of child pornography"). And, furthermore, Riley's statement that he had viewed the *partial* video, the charge for which he was acquitted, does not amount to an "admission" of possession of visual depictions of child pornography (the full video).

[¶32.] Lastly, the text strings found by Eisenbraun on Riley's computer do not establish that visual depictions of child pornography existed on Riley's computer on October 20, 2009. As the record demonstrates, text strings or file titles are just words, not images or videos. Text strings can be manipulated by the user, meaning that a computer user can assign a file any name and file extension he chooses. Thus, a Microsoft Word document could appear to be a video file and vice versa. Even Eisenbraun testified that a text string "doesn't mean that it is [child pornography] and it doesn't mean that it isn't [child pornography]."

[¶33.] Because the circumstantial evidence, when viewed cumulatively in a light most favorable to the State, is speculative and does not rise to the level of proof beyond a reasonable doubt, I would reverse the conviction.

[¶34.] SEVERSON, Justice, joins this dissent.