No. _____

In the Supreme Court of the United States

JAMES DUANE RILEY,
Petitioner,

v.

STATE OF SOUTH DAKOTA,
Respondent.

On Petition for Writ of Certiorari to the Supreme Court of South Dakota

PETITION FOR WRIT OF CERTIORARI

ROBERT L. SIRIANNI, JR.
Counsel of Record
ANDREW B. GREENLEE
BROWNSTONE, P.A.
201 North New York Ave.
Suite 200
P.O. Box 2047
Winter Park, FL 32790
(407) 388-1900
robert@brownstonelaw.com

Counsel for Petitioner

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

QUESTION PRESENTED

A state law enforcement officer downloaded two videos from a public IP address associated with the residence of James Riley. One was an incomplete, non-pornographic video of a woman removing the pants of a child. The other, a full video, contained child pornography.

When law enforcement officers searched Mr. Riley's computer and residence, they recovered no child pornography. During his interrogation, Mr. Riley, who was drunk and only marginally coherent, admitted to having viewed the partial, non-pornographic video. He denied ever viewing the video depicting child pornography.

The state charged Riley with two counts of possession of child pornography. The jury acquitted him of the count associated with the partial video, but convicted him for possession of the full video.

1. Did the South Dakota Supreme Court offend the Due Process Clause when it affirmed Mr. Riley's conviction for possessing child pornography, where the only *corpus delicti* of the crime consisted of a video downloaded from a public IP address?

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

PETITION FOR WRIT OF CERTIORARI

Petitioner, James Duane Riley, respectfully petitions the Court for a writ of certiorari to review the Opinion of the South Dakota Supreme Court affirming his Judgment of Conviction for possessing child pornography.

STATEMENT OF JURISDICTION

This Court's jurisdiction rests on 28 U.S.C. § 1254(1).

DECISIONS BELOW

On January 25, 2012, after entering a plea of not guilty, Mr. Riley stood for trial on charges that he possessed child pornography in violation of SDCL § 22-24A-3(3). App. 6. The trial court denied his motions for judgment of acquittal at the close of the state's case and after the close of evidence. App. 9. Riley renewed his request for judgment of acquittal by written motion, arguing that no jury could have reasonably concluded beyond a reasonable doubt that he committed the charged offense. On April 10, 2012, the trial court entered the Judgment of Conviction. App. 16.

Mr. Riley appealed the Judgment of Conviction directly to the South Dakota Supreme Court. App. 9. Citing *Jackson v. Virginia*, 443 U.S. 307 (1979) and the Due Process Clause of the Fourteenth Amendment, Mr. Riley again argued that no reasonable jury could find him guilty beyond a reasonable doubt. App. 10; Brief of Appellant at 8.

The South Dakota Supreme Court affirmed on December 18, 2013. App. 2. Two of the five justices

dissented. App. 15. The Opinion is published at 2013 S.D. 95 and reproduced at App. 1. This petition follows.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Section One of the Fourteenth Amendment to the United States Constitution:

> All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

STATEMENT OF THE CASE

In October of 2009, the South Dakota Internet Crimes against Children Task Force discovered 79 video files with titles suggestive of child pornography were being shared through LimeWire, a peer-to-peer file-sharing program that allows users to download files from other users. App. 2-4.

Law enforcement traced the internet protocol address ("IP Address") to a residence in Hermosa, South Dakota. The detective downloaded an entire video file that contained child pornography from the public IP Address (the "full video"). App. 4. Law enforcement also downloaded a portion of a video file that did not contain child pornography, but depicted an

adult female removing the pants of a female child (the "partial video"). *Id*.

Law enforcement subpoenaed records from the internet service provider and learned that Mr. Riley's residence leased the IP Address. App. 4. Based on this information, law enforcement applied for and obtained a warrant to search Mr. Riley's house. *Id*.

Law enforcement executed the warrant on January 15, 2010. *Id.* Mr. Riley's girlfriend, Lori Wenzlick, informed law enforcement that Riley was out-of-state at the time, had taken his computer with him on his trip, and would return around midnight. *Id*. Law enforcement warned her not to inform Mr. Riley of the search. *Id*.

Ms. Wenzlick did not heed this admonition. App. 5. Instead, when Riley arrived at approximately 1:00 a.m., she informed him that law enforcement came to the house and would return. *Id.* Law enforcement obtained a second search warrant and executed it the following morning at 6:30 a.m. *Id.* The officers seized a computer, two thumb drives, three DVDs, and an MP3 player from Mr. Riley's residence. *Id*. During their interrogation, Mr. Riley, who was drunk, admitted having seen the non-pornographic, partial video. He denied viewing the full video. *Id*.

No visual depiction of child pornography was ever found during the search. *Id.* Nor was LimeWire or evidence of any other peer-to-peer program ever discovered on his computer. *Id.* Nevertheless, the State indicted Mr. Riley on July 26, 2010, for two counts of violating SDCL § 22-24A-3(3), which forbids the knowing possession, distribution or other

dissemination of any visual depiction of a minor engaging in prohibited sexual acts or simulating such acts. App. 6. The first count alleged Mr. Riley possessed the full video. *Id.* The second count alleged he possessed the partial video. *Id*.

The matter proceeded to a jury trial on January 25, 2012. *Id.* At trial, law enforcement testified about the investigation that precipitated the search, the execution of the warrant, and the interrogation of Mr. Riley. *Id*. Ms. Wenzlick testified that Mr. Riley was the only person in the house to use the seized computer and that he used LimeWire to download music. *Id.* She also testified that Mr. Riley accessed his computer after arriving home because he said it crashed in California. *Id.* However, she did not know what he was doing on the computer. *Id*.

Detective Russ Eisenbraun testified about the results of the forensic analysis. *Id.* He confirmed that the State found no evidence of LimeWire or any visual depiction of child pornography on the computer, even in the unallocated space and the cache. *Id.* His examination revealed, consistent with Ms. Wenzlick's testimony, that there were several "bad" or damaged sectors on the hard drive and that the operating system on the computer had been reinstalled at approximately 5:37 a.m. App. 7.

Detective Eisenbraun also testified music was transferred from the hard drive to the thumb drives shortly before the reinstallation, which made the computer look "brand new." App. 8. Finally, Eisenbraun testified that he used a screen shot from the investigation to perform a "text-string search." *Id.* This enabled him to search the computer for a string of

words that corresponded to the file name or a variation of the file name for the full video. *Id.* The search produced a hit. *Id.* Eisenbraun explained, however, that the text string only identifies suggestive words: "It doesn't mean that it is [child pornography] and doesn't mean that it isn't. It's just what it is, a text that suggests." *Id.*

Mr. Riley's own expert, Dan Meinke, testified that numerous users and computers can use one IP address, and an investigator 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." *Id.* Meinke agreed with Eisenbraun that the operating system had been reinstalled. App. 9.

Yet, as Meinke explained, "[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." *Id.* Meinke testified that he "reinstall[s] operating systems on customer computers on a daily basis without ever losing their data." *Id.* Finally, Meinke explained that LimeWire users can assign a file whatever name and file extension they wish. *Id.* As a result, a Microsoft Word document could appear to be a video file and vice versa. *Id*.

Mr. Riley moved for judgment of acquittal at the close of the State's case-in-chief and renewed the motion prior to closing arguments. *Id.* The trial court denied both motions. *Id.* The jury found Riley guilty of the count relating to the full video, but failed to reach a verdict on the count relating to the partial video. *Id.* Mr. Riley was sentenced to eight years in the state penitentiary. *Id*.

On appeal, the South Dakota Supreme Court affirmed the Judgment of Conviction. The court relied on the following evidence five pieces of evidence:

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, in response to law enforcement's suggestion that he viewed child pornography, that he "glanced to see";

3. Riley's statement that "It's gone" in response to law enforcement's suggestion that he shared 79 video files containing child pornography;

4. The text strings, which corresponded to words related to 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."

App. 15. From this evidence, the court concluded that "there was sufficient evidence for a rational jury to find Riley guilty beyond a reasonable doubt." *Id*.

Justice Wilbur, joined by Justice Severson, dissented from the opinion. *Id.* According to the dissent, a rational trier of fact could not have found the essential elements of the crime beyond a reasonable doubt. *Id.* The dissent stressed that the state failed to carry its burden of establishing the existence of a visual depiction of child pornography because "no visual depiction of child pornography was ever found in

Riley's possession or on devices possessed by Riley." App. 16.

The dissent also disputed the inference that Riley "was the only user of the computer at issue on an IP address that was downloading child pornography." *Id.* Justice Wilber pointed out that the state failed to establish that Riley's computer was connected to the IP address in question, since the state's own forensic expert testified he 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. *Id.* Thus, according to the dissent, no evidence linked the downloaded videos to Riley's computer. *Id.*

The dissent also took umbrage with the majority's reliance on Riley's statements to law enforcement. App. 17. With respect to Riley's statement suggesting that he had seen the partial video, the dissent noted that Riley was acquitted of the charge associated with that video. *Id.* In addition, the dissent noted that Riley's response to a question regarding the 79 videos the expert believed to be on his computer—"It's gone"—hardly qualified as an admission. *Id.*

Finally, the dissent criticized the majority's reliance on "text strings," which only consist of strings of words that are (1) susceptible to manipulation by a user; and (2) are not probative of the existence of any video files. *Id.*

REASONS FOR GRANTING THE WRIT

I. THIS COURT SHOULD CLARIFY WHETHER THE *CORPUS DELICTI* RULE REMAINS A VIABLE SAFEGUARD AGAINST DUE PROCESS VIOLATIONS.

In *Opper v. United States*, 348 U.S. 84 (1954), this Court confirmed that in federal criminal prosecutions, a conviction must rest on more than the uncorroborated confession or admissions of a defendant. The rule announced in *Opper* has its roots in the *corpus delicti* doctrine, which arose in the Seventeenth Century to "prevent the conviction of the coerced and the mentally unstable for fictitious crimes." David A. Moran, In Defense of the *Corpus Delicti* Rule, 64 OHIO ST. L.J. 817, 817 (2003).

The concerns underlying the *corpus delicti* rule remain valid today. The Innocence Project estimates that 25% of all DNA exonerations stem from the false confessions of innocent defendants. The Innocence Project, Understanding the Causes: False Confessions, *available at* www.innocenceproject.org/understand/False-Confession.php (last visited March 17, 2014). And, in the past several months, at least two major news outlets have published stories highlighting the continued problems posed by false confessions. Adam Cohen, *Case Study: Why Innocent Men Make False Confessions*, TIME (Feb. 11, 2013); Douglas Starr, *The Interview: Do Police Interrogation Techniques Produce False Confessions?*, THE NEW YORKER (December 9, 2013).

However, in the wake of *Opper*, courts seem confused as to the continued viability of the *corpus*

delicti rule. According to the Seventh Circuit, the "*corpus delicti* rule no longer exists in the federal system." *United States v. Kerley*, 838 F.2d 932, 940 (7th Cir. 1988). Likewise, the Colorado Supreme Court abandoned the *corpus delicti* rule last year, finding the rule "originally erroneous" and "no longer sound." *People v. LaRosa*, 293 P.3d 567, 574-75 (Colo. 2013).

In contrast, the Sixth Circuit recently declared that the "corroboration rule" of *Opper* differs from *corpus delicti* "in form but not in function." *United States v. Brown*, 617 F.3d 857, 860 (6th Cir. 2010). And, just last year, the Ninth Circuit equated the *corpus delicti* rule with the rule announced in *Opper*, *United States v. Hilger*, 728 F.3d 947, 949 (9th Cir. 2013).

This Court should resolve the confusion regarding the role of the *corpus delicti* in criminal law. Equally important, this Court should determine whether a conviction secured without a *corpus delicti* or in contravention of the *Opper* rule violates a defendant's right to due process.

Several federal appellate courts, in the habeas context, have affirmed the constitutionality of convictions obtained in violation of state *corpus delicti* rules. *See*, *e.g.*, *Autry v. Estelle*, 706 F.2d 1394, 1407 (5th Cir. 1983) ("a state rule of '*corpus delicti*' has no independent constitutional footing").

However, under *Jackson v. Virginia*, 443 U.S. 307 (1979), all criminal convictions must be sustained by proof beyond a reasonable doubt. And the language of *Opper* suggests that the rule of corroboration implicates a defendant's fundamental due process rights:

> In our country the doubt persists that the zeal of the agencies of prosecution to protect the peace, the self-interest of the accomplice, the maliciousness of an enemy or the aberration or weakness of the accused under the strain of suspicion may tinge or warp the facts of the confession. Admissions, retold at a trial, are much like hearsay, that is, statements not made at the pending trial. They had neither the compulsion of the oath nor the test of cross-examination.

Opper, 348 U. S. at 89-90.

In this case, the circumstances surrounding Mr. Riley's "admissions" raise serious doubts about the trustworthiness of the statements used to obtain his conviction. Cursory review of the transcript of his interrogation reveals that Mr. Riley was highly intoxicated and minimally coherent during his interview.

This case highlights the need for the *corpus delicti* requirement. Law enforcement never found any child pornography in Riley's possession, and there was otherwise insufficient "substantial independent evidence which would tend to establish the trustworthiness of the statement." *Opper*, 348 U.S. at 93. Therefore, this case raises serious questions as to whether Mr. Riley's conviction violates his due process rights under *Jackson v. Virginia*.

II. THE COURT SHOULD RESOLVE THE CONFUSION REGARDING THE PROBATIVE WEIGHT OF EVIDENCE DOWNLOADED FROM A PUBLIC IP ADDRESS.

The Court should also address the probative weight of evidence downloaded from a *public*, as opposed to a *private*, IP address. "An Internet Service Provider (ISP) generally assigns a single, public IP address to every subscriber." *Voltage Pictures, LLC v. Does 1-31*, 291 F.R.D. 690, 692 (S.D. Ga. 2013) (citing F. Audet & Cullen Jennings, Network Address Translation (NAT) Behavioral Requirements for Unicast UDP, (Jan. 2007)).

Because "a public IP address is shared among many devices and users, any one of a home's users can do things on the internet that others on that network may not know about. And nearby neighbors (whether permitted or unauthorized) may also 'surf' using a homeowner's wireless network." *Id*.; *see also United States v. Stanley*, Crim. No. 11-272, 2012 WL 5512987 (W.D. Pa. Nov. 14, 2012).

By contrast, a private IP address can be used to identify the specific "devices connected to the internet via that wireless router. Each device connected to the wireless router has a different private IP address." *Stanley*, 2012 WL 5512987 at *4; *see also*, *e.g.*, *United States v. Forrester*, 512 F.3d 500, 510 n. 5 (9th Cir. 2008).

Unfortunately, most courts fail to understand the distinction between a public and a private IP address, referring to both under the umbrella term "IP address." *Compare Forrester*, 512 F.3d at 510 n.5 ("every

computer or server connected to the Internet has a unique IP address") *with John Wiley & Sons, Inc. v. Doe Nos. 1-30*, 284 F.R.D. 185, 190 (S.D.N.Y. 2012) (An "'IP address provides only the location at which one of any number of computer devices may be deployed,' and it is therefore less likely than in the past that a 'subscriber to an IP address carried out a particular computer function' associated with that IP address.").

This lack of clarity explains the divergence between the majority and the dissent in Mr. Riley's case. The majority, apparently relying on *United States v. Conner*, 521 F. App'x 493, 495 (6th Cir. 2013), concluded that Mr. Riley "was the only user of the computer at issue on an IP address that was downloading child pornography." App. 15. This suggests that the majority believed that the term "IP address" in this case referred to a private IP address.

Conversely, the dissent noted that the state's own expert conceded that he 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." App. 16. Thus, unlike the majority, the dissent understood the distinction between a public and a private IP address, and realized that the downloaded videos carried little probative weight regarding whether Mr. Riley ever possessed the pornography.

Since the pornography originated from a public IP address, it could have come from any one of Mr. Riley's neighbors, *see*, *e.g.*, *Stanley*, 2012 WL 5512987 at *7-8, or even a laptop user in a car parked on the curb availing himself of Riley's wireless signal. *See id*. As such, there was no evidence in this case that the

pornography that law enforcement downloaded originated from Mr. Riley's computer.

But the importance of distinguishing between public and private IP addresses extends well beyond the particular facts of this case. As illustrated by the *Stanley* decision, the distinction also impacts judicial determinations as to whether probable cause supports the issuance of a warrant.

In *Stanley*, law enforcement learned that a certain computer was sharing child pornography. *Id*. at *2. The law enforcement officers determined that the public IP address was leased to one Kozikowski. *Id*. at *3. The officers executed a warrant on his address, but they soon learned that neither of the two computers at the residence contained child pornography or the internet file-sharing software in question. *Id*.

Thus, law enforcement concluded that Kozikowski had not engaged in distributing child pornography. *Id*. Thereafter, law enforcement, using a geo-location software called "Moocherhunter," came to suspect that Kozikowski's neighbor living directly across the street possessed the computer that had shared the contraband. *Id*. at *6-7. After obtaining a subsequent search warrant, law enforcement discovered that the neighbor, Richard Stanley, and not Kozikowski, possessed the computer in question. *Id*. at *10.

As demonstrated by the facts of *Stanley*, whether an "IP address" is a public or private address can make a difference in whether or not probable cause exists to search a residence. And affiants should make this distinction in applying for search warrants.

The *Stanley* decision also demonstrates the existence of reasonable doubt in this case. As was the case with Kozikowski, law enforcement found neither child pornography nor any sort of file-sharing program on Mr. Riley's computer. Thus, there was neither a *corpus delicti* on the element of possession, nor, under *Opper*, was there sufficient evidence to corroborate Mr. Riley's inherently untrustworthy, drunken admissions.

Unlike Kozikowski, however, Mr. Riley now sits in a penitentiary. Because no rational jury could conclude *beyond a reasonable doubt* that Mr. Riley committed the offense for which he was convicted, this Court should grant certiorari review on the question presented.

CONCLUSION

For the reasons described herein, the Petitioner, James Duane Riley, respectfully request that this Court grant this petition for a writ of certiorari, and review the proceedings below.

Respectfully submitted on this 18th day of March, 2014.

Robert L. Sirianni Jr., Esq.
Counsel of Record
Andrew B. Greenlee
BROWNSTONE, P.A.
201 North New York Avenue, Ste 200
P.O. Box 2047
Winter Park, FL 32790-2047
Telephone: (407) 388-1900
robert@brownstonelaw.com

APPENDIX

APPENDIX

TABLE OF CONTENTS

APPENDIX A

2013 S.D. 95

IN THE SUPREME COURT OF THE STATE OF SOUTH DAKOTA

No. 26354-a-DG

[Filed December 18, 2013]

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 22-244-3(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 "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.

---

[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.
>
> *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. Budziah*, 697 F.3d 1105, 1108 (9th Cir. 2012).

[¶ 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 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 amived, 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 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.

---

[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."

[¶ 8.] In July 2010, a grand jury indicted Ritey 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.

[¶ 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

---

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

[5] The Ninth Circuit defined unallocated space as:

> space on a hard drive that contains deleted data, usually

to Eisenbraun, his examination revealed that there were several bad sectors[7] on the 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

---

> 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.

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, 119, 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 *Overbe*y, 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 427). "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.

---

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

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 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 ofchild 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.

APPENDIX B

IN CIRCUIT COURT
SEVENTH JUDICIAL CIRCUIT

FILE NO.:16C10000113A0

[Filed April 10, 2012]

STATE OF SOUTH DAKOTA	)
	) ss
COUNTY OF CUSTER	)
STATE OF SOUTH DAKOTA,	)
	)
Plaintiff	)
	)
vs.	)
	)
JAMES DUANE RILEY,	)
	)
Defendant	)
	)

JUDGMENT OF CONVICTION AND ORDER OF TRANSPORTATION

An Indictment was filed with this Court charging the Defendant with the crime of POSSESSION OF CHILD PORNOGRAPHY, SDCL 22-24A-3(3). The Defendant, with his attorney, Matthew Skinner, and Tracy L. Kelley, prosecuting attorney, appeared at the Defendant's arraignment. The Defendant, having been advised of all constitutional and statutory rights pertaining to the charge filed against him, including but not limited to the right to confront witnesses called against him, the right to subpoena witnesses on his

behalf, the right to a Jury Trial, the privilege against self incrimination, and the right to counsel, entered a plea of not guilty to the charge of POSSESSION OF CHILD PORNOGRAPHY, SDCL 22-24A-3(3).

On the 26th day of January, 2012, a Jury Trial commenced. The Jury returned a verdict of Guilty to the Charge of POSSESSION OF CHILD PORNOGRAPHY, in violation of SDCL 22-24A-3(3).

It is the determination of this Court that the Defendant has been regularly held to answer for said offense; that the Defendant was represented by competent counsel, and that a factual basis existed for the verdict.

It is, therefore, the Judgment of this Court that the Defendant is Guilty of the offense of POSSESSION OF CHILD PORNOGRAPHY, in violation of SDCL 22-24A-3(3).

SENTENCE

On the 10th day of April, 2012, the Court asked the Defendant is any legal cause existed to show why the Judgment should not be pronounced. There being no cause offered, the Court thereupon pronounced the following sentence:

IT IS ORDERED that the Defendant, JAMES DUANE RILEY, shall be sentenced to eight (8) years in South Dakota State Penitentiary; and it is further

ORDERED that the Defendant pay court costs in the amount of $104.00; and it is further

ORDERED that the Defendant shall receive credit for the seven (7) days already served in jail and any

time served while awaiting transport; and it is further

ORDERED that the Defendant shall reimburse Custer County for the costs of the computer forensic technician in the amount of $7,325.00; and it is further

ORDERED that the Defendant shall reimburse Custer County for the costs of the psycho-sexual evaluation in the amount of $1,100.00; and it is further

ORDERED that the Defendant shall reimburse Custer County for the costs of the grand jury in the amount of $136.25; and it is further

ORDERED that the Defendant shall reimburse Custer County for the costs of court appointed attorney fees in an amount to be determined, and it is further

ORDERED that all costs incurred by Custer County associated with the Defendant's incarceration in the Pennington County Jail, shall be entered as a lien against the Defendant by the County of Custer; and it is further

ORDERED that the Defendant shall be remanded to the immediate custody of the Custer County Sheriff for transport to the Pennington County Jail to await Pennington County Sheriff to be transported to the South Dakota State Penitentiary; and it is further

ORDERED that any and all bond posted in this matter shall be discharged and the bondsman exonerated; that the bond may be applied to fine and court costs herein.

DATED this 10 day of April, 2012, and entered nunc pro tunc the 10th day of April, 2012.

BY THE COURT
/s/ Jeff W. Davis
HONORABLE JEFF W. DAVIS
CIRCUIT COURT JUDGE

ATTEST:
/s/ Debbie Salzoieder
Clerk of Courts
By: /s/
Deputy
(SEAL)

NOTICE OF RIGHT TO APPEAL

You, JAMES DUANE RILEY, are hereby notified that you have a right to appeal as provided by SDCL 23A-32-15, which you must exercise by serving a written notice of appeal upon the Attorney General of the State of South Dakota and the State's Attorney of Custer County and by filing a copy of the same, together with proof of such service with the Clerk of this Court within Thirty (30) days from the date that this Judgment is filed with said clerk.

FILE NAME: JAMES DUANE RILEY

FILE NO.: 16C10000113A0