#27962-a-GAS
2017 S.D. 31

IN THE SUPREME COURT
OF THE
STATE OF SOUTH DAKOTA

* * * *

STATE OF SOUTH DAKOTA, Plaintiff and Appellee,

v.

TODD DAVID LINSON, Defendant and Appellant.

* * * *

APPEAL FROM THE CIRCUIT COURT OF
THE SECOND JUDICIAL CIRCUIT
MINNEHAHA COUNTY, SOUTH DAKOTA

* * * *

THE HONORABLE BRADLEY G. ZELL
Judge

* * * *

MARTY J. JACKLEY
Attorney General

MATTHEW W. TEMPLAR
Assistant Attorney General
Pierre, South Dakota

Attorneys for plaintiff and appellee.

BEAU J. BLOUIN
Minnehaha County Public
Defenders Office
Sioux Falls, South Dakota

Attorneys for defendant and appellant.

* * * *

CONSIDERED ON BRIEFS
ON APRIL 24, 2017
OPINION FILED 05/24/17

#27962

SEVERSON, Justice

[¶1.] Todd Linson appeals his conviction on five counts of possessing child pornography. He asserts that there was insufficient evidence to prove that he knowingly possessed child pornography. He also asserts that the statute defining possession of child pornography is unconstitutionally vague and that he was convicted multiple times for a single act or course of conduct, in violation of his right to be free from double jeopardy. We affirm.

Background

[¶2.] On the evening of March 3, 2013, Officers Mertes and Buss were dispatched to Linson's residence to investigate a report of possible child pornography found on a computer. Linson's wife and sister were at the residence when law enforcement arrived. They directed the officers to a computer that required a password to access. When Linson arrived home, he provided the login password so the officers were able to look at web browsing history. After discovering that Linson had searched for pornography using terms associated with child pornography and observing that several websites in the browser's history contained child pornography, the officers decided to seize the computer.

[¶3.] Law enforcement performed a forensic analysis on the computer seized from Linson's home. Two user profiles were found on the computer. Forty-one images of possible child pornography were found in the cache[1] on just one of those

1. "A cache (pronounced 'cash') is a storage mechanism designed to speed up the loading of Internet displays. When a computer user views a webpage, the web browser stores a copy of the page on the computer's hard drive in a folder or directory. That folder is known as the cache, and the individual files (continued . . .)

profiles—the one belonging to Linson. An additional 360 images of child pornography were found in the unallocated space of the computer.[2] On September 24, 2014, a grand jury indicted Linson on five counts of possessing, distributing, or otherwise disseminating child pornography in violation of SDCL 22-24A-3(3). The five images associated with those five counts were each found in the cache files of the computer. The analysis of the computer also revealed that the person using the computer used the following search terms in internet search engines: "preteen, nude preteen photos, free preteen photos, no tits, [and] Lolita."[3] There were also adult pornography searches that were done around the same time.

[¶4.] A two-day jury trial began on April 13, 2016. Before the case was submitted to the jury, the defense moved for a judgment of acquittal, which the circuit court denied. On April 14, 2016, the jury found Linson guilty on all five

---

(. . . continued)

within the cache are known as temporary Internet files. When the user later returns to a previously visited webpage, the browser retrieves the cached file to display the webpage instead of retrieving the file from the Internet. By retrieving the page from the cache, instead of the Internet, the browser can display the page more quickly." Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 Berkeley Tech. L.J. 1227, 1229-30 (2004) (footnotes omitted).

2. "When a computer user deletes a file, it is not simultaneously removed from her computer. The physical location on the hard disk where the deleted file resides is marked by the computer as unallocated file space, which allows it to be overwritten. The file is not actually removed from the computer until another file overwrites it. While the file is marked for deletion (but not yet overwritten), it exists in unallocated file space. Forensic software allows an investigator to search and view the contents of the unallocated file space." Howard, *supra* ¶ 3 n.1, at 1273.

3. "'Lolita' is often a code word for child pornography." *Unites States v. Grimes*, 244 F.3d 375, 379 n.7 (5th Cir. 2001).

counts. On July 28, 2016, the court sentenced Linson to five years in the penitentiary on each count, to run consecutively. It suspended two years on count 1, all five years on count 2, four years on count 3, all five years on count 4, and all five years on count 5. Linson appeals his conviction, raising the following three issues:

1. Whether the evidence was sufficient to prove Linson knowingly possessed the images found in the temporary-internet-file cache of the computer.

2. Whether SDCL 22-24A-3 is unconstitutionally vague in violation of Linson's due process rights under the United States and South Dakota Constitutions.

3. Whether Linson's double jeopardy rights were violated because Linson was penalized multiple times for the same offense or course of conduct.

Analysis

1. Whether the evidence was sufficient to prove Linson knowingly possessed the images found in the temporary-internet-file cache of the computer.

[¶5.] "We review the denial of a motion for judgment of acquittal as a question of law under the de novo standard." *State v. Bausch*, 2017 S.D. 1, ¶ 25 889 N.W.2d 404, 411 (quoting *State v. Overbey*, 2010 S.D. 78, ¶ 12, 790 N.W.2d 35, 40). "We consider the evidence in the light most favorable to the verdict and will not set aside a guilty verdict on appeal 'if the state's evidence and all favorable inferences that can be drawn therefrom support a rational theory of guilt.'" *Id.* (quoting *Overbey*, 2010 S.D. 78, ¶ 12, 790 N.W.2d at 40).

[¶6.] To prove the crime possessing, distributing, or otherwise disseminating child pornography under SDCL 22-24A-3(3), the State needed to establish that

Linson "[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 an act." Linson concedes that the images depict child pornography. He only disputes whether he knowingly possessed those images. Although *possession* is not statutorily defined, this Court (in a possession of marijuana case) has stated that it "signifies dominion or right of control over [contraband] with knowledge of its presence and character." *State v. Barry*, 2004 S.D. 67, ¶ 9, 681 N.W.2d 89, 92 (per curiam). "[P]ossession can either be actual or constructive and need not be exclusive." *Id.* It may be proven by circumstantial evidence. *Id.* ¶ 11, 681 N.W.2d at 93.

[¶7.] This Court has not previously considered whether cached images are themselves the contraband that a defendant possesses or whether they are merely evidence of possession of child pornography. Here, where there was no evidence that Linson knew how the cache operated, he cannot be said to have known what images were present in his cache or to have had dominion or control over those cached images. Other courts have held that the presence of cached images or files, standing alone, is not sufficient to establish that a defendant knowingly possessed those cached images or files. *See Marsh v. People*, 389 P.3d 100, 108 (Colo. 2017) ("[T]he presence of photos in the internet cache alone does not automatically establish knowing possession." (citing *United States v. Winkler*, 639 F.3d 692, 698-99 (5th Cir. 2011))). The Colorado Supreme Court explained some of the reasons for such a holding:

> advances in internet technology have made it easier to access child pornography and have also facilitated cyber-attacks like

> viruses and hacking. Such intrusions could conceivably result in a computer displaying sexually exploitative images without the knowledge of that computer's owner, even where the owner has exclusive physical access to the computer.

Id. The Eighth Circuit has also noted the problematic nature of files such as those that are cached. It explained that "[t]he presence of Trojan viruses and the location of child pornography in inaccessible internet and orphan files[4] can raise serious issues of inadvertent or unknowing possession." *United States v. Kain*, 589 F.3d 945, 949 (8th Cir. 2009) (citing *United States v. Romm*, 455 F.3d 990, 998-1001 (9th Cir. 2006)). The Eighth Circuit concluded that "[t]he presence of child pornography in temporary internet and orphan files on a computer's hard drive is *evidence* of prior possession of that pornography, though of course it is not conclusive evidence of knowing possession and control of the images." *Id.* at 950. And it determined that issues of inadvertent or unknowing possession are "issues of fact, not of law." *Id.* at 949.

[¶8.] We agree with those courts holding that the mere presence of child pornography in a computer's cache is not sufficient to establish that a defendant knowingly possessed it; the cached images are not themselves the contraband. Instead, cached images or files are evidence of possession. The State notes that we have defined constructive possession as the dominion or control over either the contraband or the *premises* in which the contraband was found. *See State v. Riley*, 2013 S.D. 95, ¶ 16, 841 N.W.2d 431, 436. In this case, Linson had dominion or

4. A detective in *Kain* explained that "orphan files" are "files 'that were on the computer somewhere saved' but were subsequently deleted, 'so the computer doesn't know exactly where they came from.'" *Kain*, 589 F.3d at 948.

control over the premises where the images were found—the computer and user profile—thus, the State asserts, the element of possession is met. We reject such an approach; it would make a computer owner strictly liable for anything that inadvertently loads on a computer, and it leaves unaddressed the concerns that other courts have highlighted, such as viruses and pop-ups. Those issues are ones reserved for a fact-finder.

[¶9.] Linson contends that using cached images as evidence of possession amounts to the punishment of viewing child pornography, especially here where there was no evidence introduced that Linson exercised his ability to control the images that he retrieved, that he knew about his computer's cache, or that he knew how to access images in the cache. The federal government and other states have prohibited viewing child pornography, but it is not explicitly prohibited by South Dakota's statutes. *See* 18 U.S.C. § 2252A(a)(5)(B) (2012) ("(a) Any person who— (5) either— (B) knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography . . . shall be punished as provided in subsection (b)."). Linson refers us to various cases in support of his argument that he could not possess images found only in his cache. A couple of the cases he cites determined that their respective legislatures did not intend to criminalize behavior such as Linson's. *See State v. Barger*, 247 P.3d 309, 567 (Or. 2011) (concluding "that the acts at issue here—navigating to a website and bringing the images that the site contains to a computer screen—are not acts that the legislature intended to criminalize"); *Worden v. State*, 213 P.3d 144, 147 (Alaska Ct. App. 2009) ("[T]he

evidence supported the inference that [defendant] had viewed child pornography on certain websites at some point in the past. . . . But . . . the Alaska Statute prohibiting the knowing possession of child pornography does not criminalize merely viewing images of child pornography on a computer."). The courts in several other cases he has cited considered whether a defendant knew about the computer's cache.[5] Knowledge about the functioning of the cache or how to access the images

---

5. *See United States v. Flyer*, 633 F.3d 911, 919 (9th Cir. 2011) ("The government concedes that it presented no evidence that Flyer knew of the presence of the files on the unallocated space of his Gateway computer's hard drive. The government also concedes it presented no evidence that Flyer had the forensic software required to see or access the files. . . . Our precedent relating to cache files suggests that a user must have knowledge of and access to the files to exercise dominion and control over them."); *United States v. Dobbs*, 629 F.3d 1199, 1204-05, 1207 (10th Cir. 2011) ("[T]he government presented no evidence that [defendant] had accessed the files stored in his computer's cache, including the two images at issue. And, more tellingly, there was no evidence that he even knew about his computer's automatic-caching function." And prosecution did not show that defendant conducted search for child pornography "immediately prior to the creation of those two images in the cache." "[F]or th[e] evidence to be probative of the question of *knowing* receipt, the government needed to present proof that [defendant] at least knew of the automatic-caching process."); *United States v. Kuchinski*, 469 F.3d 853, 862 (9th Cir. 2006) ("[T]here was no evidence that [defendant] was sophisticated, that he tried to get access to the cache files, or that he even knew of the existence of the cache files."); *People v. Kent*, 970 N.E.2d 833, 841 (N.Y. 2012) ("The People did not demonstrate that defendant knew that the page, or any other, for that matter, had been cached [nor] [t]hat defendant . . . . controlled the image while it was on his screen. . . . Thus, the evidence was insufficient to show that defendant knowingly possessed the . . . Web page, either in the form of the cached file or as an image on his screen. It follows, therefore, that there was not sufficient evidence that defendant procured the . . . page; defendant did not 'get possession of the page by particular care or effort' as by downloading it." (quoting *People v. Keyes*, 552 N.E.2d 617, 619 (N.Y. 1990)); *Barton v. State*, 648 S.E.2d 660, 663 (Ga. Ct. App. 2007) ("[T]he State was required to show that [defendant] had knowledge of the images stored in his computer's cache files."). *But see New v. State*, 755 S.E.2d 568, 575 (Ga. Ct. App. 2014) ("*Barton* cannot be read to foreclose the State's ability to prosecute and

(continued . . .)

contained therein is irrelevant when the cached images are evidence of possession and do not themselves conclusively establish possession. *See* Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 Berkeley Tech. L.J. 1227, 1257 (2004) (explaining that under the "evidence of" approach, "criminal liability arises not from the cached images themselves, but rather from the images that the user originally searched for, selected, and placed on his computer screen"). Accordingly, those cases, which do not follow the evidence of possession approach, are largely inapplicable to our analysis.

[¶10.] Drawing a line between the mere viewing of images on a potentially mobile electronic device such as a computer and possessing those images highlights the difficulty of applying older legal concepts rooted in a brick-and-mortar world to today's virtual world. *See generally* Audrey Rogers, *From Peer-to-Peer Networks to Cloud Computing: How Technology is Redefining Child Pornography Laws*, 87 St. John's L. Rev. 1013 (2013). Various courts treating cached images as evidence of possession find relevant whether the defendant navigated to websites containing child pornography (through conduct such as performing searches containing terms associated with child pornography) and the control that technology gives defendant over the images retrieved. The Pennsylvania Supreme Court, using the Black's Law dictionary definition of *control*, explained as follows:

(. . . continued)

> convict a defendant for prior possession of child pornography when automatic backup files, in addition to other direct or circumstantial evidence, establish same.").

> An individual manifests such knowing control of child pornography when he purposefully searches it out on the internet and intentionally views it on his computer. . . . [T]he viewer may, *inter alia*, manipulate, download, copy, print, save or e-mail the images. It is of no import whether an individual actually partakes in such conduct or lacks the intent to partake in such activity because intentionally seeking out child pornography and purposefully making it appear on the computer screen—for however long the defendant elects to view the image—itself constitutes knowing control.

Commonwealth v. Diodoro, 970 A.2d 1100, 1107 (Pa. 2009), *cert. denied*, 558 U.S. 875, 130 S. Ct. 200, 175 L. Ed. 2d 127 (2009); *see also New v. State*, 755 S.E.2d 568, 575-76 (Ga. Ct. App. 2014) ("[A] computer user who intentionally accesses child pornography images on a website 'gains actual control over the images, just as a person who intentionally browses child pornography in a print magazine "knowingly possesses" those images, even if he later puts the magazine down.'" (quoting *Kain*, 589 F.3d at 950)).

[¶11.] Similar to those cases, there was evidence introduced that Linson entered multiple search terms associated with child pornography, repeatedly seeking it out. The officers investigating the computer at his house reported that they had to wait for Linson to arrive before they could access his user profile, which contained the child pornography. Linson's wife testified that those reports were inaccurate and that she and Linson's sister had access to his user profile. But the jury is tasked with making a credibility determination. And based on the evidence introduced, it could infer that Linson had exclusive access to the computer profile on which the images were found. One of the responding officers testified that Linson initially claimed that pop-ups were to blame for the child pornography on his computer's history. He told the officer that he searched for and viewed adult

pornography when the child pornography was displayed in a pop-up. The officer further testified that "after some conversation back and forth, I don't recall the exact conversation, but he did admit that he typed some of those terms into there[.]" The detective performing the computer analysis testified that she found an additional 360 images of child pornography in the unallocated space of the computer. Thus, the jury could also infer that Linson consciously sought out and retrieved the images that were introduced. In taking such actions, he gained control over the images that he ultimately accessed and thus knowingly possessed them. *See State v. Mercer*, 782 N.W.2d 125, 139 (Wis. Ct. App. 2010) ("[Defendant's] *repetitive* searches for and navigation within child pornography websites show that this was not a person doing a search for a benign topic who just happened to mistakenly click on a website featuring child pornography."). Some of the various actions that Linson could take in regard to the images include printing, taking a screenshot, emailing, uploading to a cloud-based service, or copying. This is not a case involving mere viewing of child pornography or one in which it was clear that the images found on the computer had been placed there inadvertently.[6]

---

6. On this point, a Wisconsin appellate court found a hypothetical from a journal helpful. It explained:

> We disagree with [defendant] that this case falls so far on the viewing end of the possession-viewing spectrum that it represents a "pure view" case. The following hypothetical, advanced by a commentator in a legal journal, aptly describes what comes to our minds when we think of a "pure view" case. The same hypothetical also neatly contrasts "pure view" from what we ultimately believe is the situation in this case:
>
> > Patrick Pedophile logs onto his computer and opens his web browser. He goes to a common search engine, like Google or
>
> (continued . . .)

The evidence indicated affirmative actions by Linson to seek out child pornography and place it on his computer at one point in time and for whatever duration he chose, bringing it under his control.[7] *See State v. McKinney*, 2005 S.D. 74, ¶ 13,

---

(. . . continued)

> Lycos, and types in several search terms including "lolita," "preteen nude pics," and "underage sex kittens." Upon receiving his search results, Patrick clicks on a particular website, which contains thumbnail images of child pornography. He then clicks on several of the thumbnail images to enlarge them and views them at his desk. As he is doing so, Patrick's coworker, Ian Innocent, happens to walk by Patrick's desk, where he stops to chat for a moment. When Ian arrives, he looks directly at Patrick's computer screen and views the precise same image that Patrick is viewing for several seconds.
>
> The distinction between Patrick and Ian's conduct is clear. Regardless of Ian's intent or knowledge about the images on Patrick's computer screen, Ian did not possess them. He had no control or dominion over them. He could not guide those images' destinies. He had no ability to move, alter, save, destroy, or choose the images. Ian merely viewed them. Contrast Ian's conduct with Patrick's conduct. Unlike Ian, Patrick sought the images out and affirmatively placed them on his computer screen. He had the ability to move, alter, copy, save, destroy, and otherwise manipulate the image. Patrick had total ability to control and guide the image. In every sense, Patrick possessed the image at that time—and his possession was captured "on videotape" by his computer's cache file.
>
> We do not consider [defendant] to be in the same shoes as the fictional Ian. This is not a "pure view" case.

Mercer, 782 N.W.2d at 132 (citation omitted) (quoting Howard, *supra* ¶ 3 n.1, at 1267-68).

7. A justice on the Supreme Court of Oregon, who disagreed with the court's determination that Oregon did not prohibit purposefully seeking out child pornography on a computer, noted that such a decision ignores the realities of today's technology. Justice Kistler explained:

> [T]oday's iPhone is yesterday's photograph. There is no difference between a person who uses his iPhone to pull an image of child
>
> (continued . . .)

699 N.W.2d 460, 465 ("[T]here is no amount of time these images must be in a defendant's possession before a conviction can be upheld."). Such conduct, as found by the jury, amounts to constructive possession of the child pornography.

2. Whether SDCL 22-24A-3 is unconstitutionally vague in violation of Linson's due process rights under the United States and South Dakota Constitutions.

[¶12.] Linson contends that SDCL 22-24A-3 is unconstitutionally vague because it fails to put the public on notice that viewing child pornography falls within the purview of the statute. We review challenges to the constitutionality of a statute de novo. *See State v. Myers*, 2014 S.D. 88, ¶ 6, 857 N.W.2d 597, 599. However, Linson did not present this issue to the circuit court, and therefore our review is limited to plain error. *See* SDCL 23A-44-15. As explained above, this case is not one in which the viewing of child pornography is being criminalized. *Supra* ¶ 11. Linson obtained constructive possession of the images that he affirmatively sought out and brought under his control on the computer. *See State v. Martin*, 2003 S.D. 153, ¶ 32, 674 N.W.2d 291, 301 ("[V]agueness challenges are usually

---

(. . . continued)

> pornography off the Internet and then passes that image, displayed on his iPhone, around for his friends to see and a person who passes a photograph of the same image to his friends. Both persons possess or control the image. The fact that the person has not saved the image to his iPhone does not mean that the person does not possess or control it. . . .
>
> . . . .
>
> . . . [W]hen the computer displaying the image is portable, as an iPhone, iPad, or Droid is, then the user can take that displayed image with him or her, move the image from one place to another, and show it to others in different locations, all without ever saving the image to the user's hard drive.

State v. Ritchie, 248 P.3d 405, 411, 413 (Or. 2011) (Kistler, J., dissenting).

'examined in light of the facts of the case at hand.'" (quoting *United States v. Whiting*, 165 F.3d 631, 634 (8th Cir. 1999)). Accordingly, there is no plain error for this Court to notice. *See State v. Fischer*, 2016 S.D. 1, ¶ 15, 873 N.W.2d 681, 687 ("We invoke our discretion under the plain error rule cautiously and only in 'exceptional circumstances.'" (quoting *State v. Nelson*, 1998 S.D. 124, ¶ 8, 587 N.W.2d 439, 443)).

3. Whether Linson's double jeopardy rights were violated because Linson was penalized multiple times for the same offense or course of conduct.

[¶13.] Linson's remaining argument is that his convictions violate his right to be free from double jeopardy because he was penalized multiple times for the same offense or course of conduct. "A defendant cannot receive two convictions for one crime unless the Legislature intended multiple punishments." *State v. Chavez,* 2002 S.D. 84, ¶ 15, 649 N.W.2d 586, 593 (quoting *State v. Well*, 2000 S.D. 156, ¶ 23, 620 N.W.2d 192, 197). "Multiple charges and punishments in a single prosecution will not violate double jeopardy if the Legislature plainly intended to impose cumulative punishments." *Martin*, 2003 S.D. 153, ¶ 38, 674 N.W.2d 291, 302 (quoting *State v. Dillon*, 2001 S.D. 97, ¶ 14, 632 N.W.2d 37, 43-44). Again, because Linson did not raise this issue with the circuit court, our review is limited to plain error.

[¶14.] Linson concludes that multiplicity exists in this case because several of the images were placed in the cache around the same time. The detective performing the analysis on the computer testified that the images being charged came from March 1, 2013, at 10:45 p.m. to 11:06 p.m., and March 2, 2013, at 10:01

p.m. As explained above, however, the cached images are only evidence of past possession of contraband; they are not contraband in themselves. We have previously determined that the Legislature intended to impose separate punishments for each instance of possessing an image of child pornography. *See id.* ¶ 41, 674 N.W.2d at 303. Accordingly, the time at which the images were placed in the cache is not the relevant inquiry.

[¶15.] Even so, Linson maintains that the images here were not affirmatively downloaded and thus *Martin* is inapplicable. However, to hold that *Martin* only covers those images which have been downloaded on a computer would be too narrow of a reading. Such a reading ignores that Linson had constructive possession of each of those images and assumes that downloading is the only way to possess an electronic image of child pornography. The underlying rationale of criminalizing child pornography is "the protection of the children who would otherwise be exploited during the production process of such material. This protection rationale extends to each child in each picture found on [defendant's] computer[]." *Id.* ¶ 42, 674 N.W.2d at 303. SDCL 22-24A-3(3) prohibits the possession of "any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act." Similar to *Martin*, Linson was convicted of possession of five separate images, each of which contained a different child. Accordingly, this case falls within the purview of our decision in *Martin*, and Linson's conviction on all five counts does not violate double jeopardy. There is no plain error for this Court to notice.

Conclusion

[¶16.] From the evidence introduced at trial, the jury could find that Linson knowingly possessed the five images of child pornography for which he was charged. There is no plain error for this Court to notice with regard to the constitutionality of SDCL 22-24A-3 or double jeopardy.

[¶17.] GILBERTSON, Chief Justice, and ZINTER, WILBUR, and KERN, Justices, concur.