

**COURT OF APPEALS OF WISCONSIN
PUBLISHED OPINION**

Case No.: 2008AP1763-CR

†Petition for Review filed

Complete Title of Case:

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

BENJAMIN W. MERCER,

DEFENDANT-APPELLANT.†

Opinion Filed: March 31, 2010

Oral Argument: December 17, 2009

JUDGES: Brown, C.J., Neubauer, P.J., and Snyder, J.

Concurred:

Dissented:

Appellant

ATTORNEYS: On behalf of the defendant-appellant, the cause was submitted on the briefs of and oral argument by *Steven P. Sager* of *Sager, Colwin, Samuelsen & Associates, S.C.* of Fond du Lac.

Respondent

ATTORNEYS: On behalf of the plaintiff-respondent, the cause was submitted on the brief of *Christopher G. Wren*, assistant attorney general, and *J.B. Van Hollen*, attorney general. There was oral argument by Christopher G. Wren.

**COURT OF APPEALS
DECISION
DATED AND FILED**

March 31, 2010

David R. Schanker
Clerk of Court of Appeals

NOTICE

This opinion is subject to further editing. If published, the official version will appear in the bound volume of the Official Reports.

A party may file with the Supreme Court a petition to review an adverse decision by the Court of Appeals. See WIS. STAT. § 808.10 and RULE 809.62.

**Appeal No. 2008AP1763-CR
STATE OF WISCONSIN**

Cir. Ct. No. 2005CF306

IN COURT OF APPEALS

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

BENJAMIN W. MERCER,

DEFENDANT-APPELLANT.

APPEAL from a judgment of the circuit court for Fond du Lac County: DALE L. ENGLISH, Judge. *Affirmed.*

Before Brown, C.J., Neubauer, P.J., and Snyder, J.

¶1 BROWN, C.J. The issue in this case is whether individuals who purposely *view* digital images of child pornography on the Internet, even though the images are not found in the person's computer hard drive, nonetheless *knowingly possess* those images in violation of WIS. STAT. § 948.12(1m) (2007-

08).¹ In the last decade, courts across the country have repeatedly decided that data recovered from a defendant's computer hard drive is evidence of possession. The evidence against Benjamin W. Mercer, however, comes from monitoring software that tracked his Internet browsing; there is no evidence that the contraband was in his computer hard drive. Mercer argues that this difference is significant because he interprets past cases as requiring evidence of an image in his computer hard drive in a place he knew could be accessed later, as well as further evidence that he manipulated the image. We disagree that the past cases present some kind of threshold regarding the evidence which must exist in order for the government to prove that a person knowingly possessed child pornography. Rather, those past cases merely chronicle the facts found in those cases, with the bottom line being that the defendant in each case affirmatively reached out for and obtained images of child pornography and had the ability to control those images. Since the monitoring software showed that Mercer repeatedly searched for and navigated within websites to click on images of child pornography and that Mercer had the ability to control those images, there was sufficient evidence for a jury to find knowing possession. Because we also reject Mercer's other challenges, we affirm.

BACKGROUND

¶2 Mercer was the human resources director for the city of Fond du Lac, which, in December 2002, installed on its employees' work computers (including Mercer's) Sergeant Laboratories monitoring software. Mercer did not

¹ All references to the Wisconsin Statutes are to the 2007-08 version unless otherwise noted.

know about the monitoring software. Every time he logged in to his computer, the software collected information about what he did on his computer. The software tracked general information about computer use: the computer being used, which user was logged into that computer at any particular time, the amount of time the computer was used each day, and the program(s) being used. The city originally used the software to decide which computers to upgrade.

¶3 In 2004, the city found out that the software also had an alert function which would send an e-mail alert to the city whenever a user typed in an offensive or inappropriate word. The city activated the alert function and used the software's built-in dictionary. Then, if someone typed the keys spelling a word in the dictionary, the software would pick it up as questionable and send an e-mail alert to the city's information systems employees. The e-mail alert included information about which computer was the subject of the alert, the user's identity, the word that was typed, and the program that was being used. The software was capable of alerting on this information because, in addition to the general information mentioned above, the software kept a log of more specific information: every mouse click or keyboard stroke; if a keyboard stroke, which key was hit; the words in the title bar² of the program at the moment of that click or keystroke; and the time that action took place.

¶4 After the city started using the alert function, the information systems employees regularly received alerts regarding Mercer's computer use. The alerts suggested a pattern of Mercer surfing the Internet for, among other

² The title bar is the horizontal bar that is generally displayed at the top of a computer program window. It bears the name of the program and a description of the contents displayed.

subjects, possible adult pornographic websites and pornographic websites involving children.

¶5 On June 15, 2004, one of the city's information systems employees met with a police officer to review and recreate the content in the software logs for Mercer's computer use. The employee and officer reviewed the logs for Mercer's Internet Explorer use from June 2004 back through part of March 2004. They learned that Mercer had typed words such as "preteens," "preteen super models," "preteen hardcore," "lolita," and "lolidus"³ into the Yahoo!, Google, and MSN search engines and hit the enter key or clicked enter to get search results for those words. Based on the information from the title bar at each click, which was sometimes the actual web address, the information systems employees were able to use Internet Explorer to view the same websites that Mercer visited. The content of those websites included stories about children engaged in sexual acts and images of children in sexual situations. Then they expanded the time period to December 2002 through July 1, 2004, and reviewed what Mercer searched for with search engines like Yahoo!, Google, and MSN from December 2002 to July 1, 2004. They found that on fifty different days Mercer had performed numerous searches for "preteen," "lolita," and "lolidus," among other variations of those words, and clicked on links in the search results.

³ "Lolita" is a term known for child erotica. "Lolidus" is a spelling variation of "lolita."

¶6 On October 8, 2007, the State charged Mercer with fourteen counts of possession of child pornography in violation of WIS. STAT. § 948.12(1m).⁴ These charges stemmed from the use of his work computer on May 28, 2004. The case was tried to a jury. The State's case was, to a large extent, based on the testimony of the software's cofounder. In order to explain the significance of his testimony, we will describe his commentary regarding the day's log in some detail. We will also draw from logs and website printouts⁵ shown to the jury.

¶7 From this evidence, we relate the facts as follows: The computer user⁶ (Mercer) started at Yahoo!, then navigated to Perverts-R-Us (which, like Yahoo!, is a web portal to help a person navigate to and find other websites). Then the user clicked to enter "LOLITA NEWS: The Best Lolitas Here!" Lolita News contained a series of Internet magazines that people could click on and view. From there the user clicked to enter the magazine "Lolita LS-Flash," which showed up on the log as "Lolita-news.info/ls-flash.html." Then there was a click somewhere on LS-Flash that led the user to "Flash-005b.jpg," one of the charged images, and once the image was displayed the user clicked two more times within "Flash-005b.jpg." The next entry was back to LS-Flash, and then back to Lolita News. Next the user clicked to enter "LS-BARBIE" and clicked again to view

⁴ The State also charged Mercer with additional counts of possessing child pornography. These counts were based on other evidence not derived from the software program logs. The jury found him not guilty on these counts, and the State does not appeal those verdicts. They are irrelevant to this appeal.

⁵ As the officer reviewed the websites listed in the log, the officer saved and printed out copies of the websites to preserve the website so no one could alter or edit it.

⁶ Mercer testified at trial that he had never seen anyone else using his computer who may have searched for and viewed the charged images.

“lsbar-007b-044.jpg,” went back to “LS-BARBIE” to view another image, “Barbie-008a.jpg,” and then to another one of the charged images. The user clicked four times while on the “Barbie-008a.jpg” image.

¶8 We will not repeat the entire log because the subsequent entries are similar. The software’s cofounder testified that the clicks recorded in the log “indicate that the person is at each one of [the] particular magazines [linked to the Lolita-News website]; [the person is] going into the magazine and backing out; going in and backing out.” They show the user going back to Lolita News and then clicking on one of the magazines and, once at the magazine, clicking back and forth to view images within each magazine before returning to Lolita News to choose a different magazine, like “LS-FANTASY,” “LITTLE GUESTS” and “LS-LAND.” Over the course of Mercer’s web browsing that day, he returned to Yahoo! three times before returning to “LOLITA NEWS” and again clicking through the various magazines. The record also shows that Mercer navigated from Yahoo! to other nonpornographic websites, to other pornographic websites with lolita in the title, such as http://www.pornololita.info/cgi-bin/scj/out.cgi?link=lolita_bbs_pics, and to “Alt.Sex.Stories Text Repository.”

¶9 The printout of the Lolita News homepage shows that the website states “The Best Lolita Portal” at the top, talks about how it has “24 Lolita Sites” with girls aged fourteen or younger, and then lists the lolita sites. The sites are the magazines Mercer visited (LS Dream, LS-Land, Touch-It, and so on), and Lolita News lists the sites on its homepage with a title, textual description, and a picture of young girls in various states of undress.

¶10 The jury also heard from a forensic expert that Mercer took steps to delete the place on his computer hard drive where the computer would

automatically download any viewed images to (the “cache,” a term we explain below). He had searched for the programs Evidence Eliminator and Window Washer, both of which are designed to delete Internet history (including the cache) and privacy information. And he searched the Windows Help Center for how to delete files associated with one’s Internet browsing.

¶11 After the State had rested its case, Mercer testified in his own defense. The jury heard him deny looking at the images or searching for child pornography, but admit that he “may have” searched with terms like “lolita” that are associated with child pornography. Mercer also explained how one would print an image from the Internet and said he had done so in the past. Finally he admitted that he deleted his cache on a daily or weekly basis.

¶12 The jury found Mercer guilty on all fourteen counts. Mercer then filed this appeal, challenging the sufficiency of the evidence, the trial court’s instruction on the meaning of “possession,” and additional discretionary decisions made by the trial court. We will provide additional facts as needed.

DISCUSSION

Sufficiency of the Evidence of Knowing Possession

¶13 Mercer first challenges the sufficiency of the evidence that he knowingly possessed the charged images. Normally, we review a sufficiency of the evidence challenge by deciding whether the trier of fact could, acting reasonably, be convinced by the evidence that the defendant is guilty beyond a reasonable doubt of every essential element of the crime charged. *State v. Poellinger*, 153 Wis. 2d 493, 501, 503-04, 451 N.W.2d 752 (1990). And in these situations, we will view the evidence in the light most favorable to the trier of

fact’s finding. *Id.* at 504. Under that standard, we may overturn a verdict on grounds of insufficiency of the evidence only if the trier of fact could not possibly have drawn the appropriate inferences from the evidence adduced at trial. *State v. Watkins*, 2002 WI 101, ¶68, 255 Wis. 2d 265, 647 N.W.2d 244. So, to the extent that Mercer denied viewing pornographic evidence or claimed that, if he did, a virus or pop-up or a pop-under caused him to do so, this standard of review is appropriate.

¶14 But the main theory driving Mercer’s sufficiency of the evidence challenge does not depend on whether the historical facts supporting the verdict lacked the probative value and force sufficient to meet every essential element of the charged crime. Rather, the issue he raises is one of law—the application of a statute to a particular set of facts. *See, e.g., State v. Piddington*, 2001 WI 24, ¶13, 241 Wis. 2d 754, 623 N.W.2d 528. We will discuss the sufficiency of the evidence issue in this context first and then discuss the issues of fact after.

¶15 We start by examining the definition of the essential element at issue, knowing possession. *See* WIS. STAT. § 948.12(1m)(a); WIS JI—CRIMINAL 2146A (May 2007). The statute states that: “Whoever possesses any undeveloped film, photographic negative, photograph, motion picture, videotape, or other recording of a child engaged in sexually explicit conduct under all of the following circumstances [is guilty of a class D felony]: (a) The person knows that he or she possesses the material.” Sec. 948.12(1m)(a). And the pattern jury instruction explains “possessed” as when “the defendant knowingly had actual physical control of the recording.” WIS JI—CRIMINAL 2146A (footnotes omitted).

¶16 The pattern jury instruction also provides optional paragraphs for cases in which the child pornography is under the defendant’s control but not directly in his or her physical possession:

[A recording is (also) in a person’s possession if it is in an area over which the person has control and the person intends to exercise control over the recording.]

[It is not required that a person own a recording in order to possess it. What is required is that the person exercise control over the recording.]

[Possession may be shared with another person. If a person exercises control over a recording, the recording is in that person’s possession, even though another person may also have similar control.]

Id. & n.4; *see also* WIS JI—CRIMINAL 920 & n.2 (supplying the definition of possession). Cases sometimes refer to this concept as “constructive possession,” which describes “circumstances that are sufficient to support an inference that the person exercised control over, or intended to possess, the item in question.” WIS JI—CRIMINAL 920 n.2; *see also* **Schmidt v. State**, 77 Wis. 2d 370, 379, 253 N.W.2d 204 (1977) (holding that constructive possession exists when “the contraband is found in a place immediately accessible to the accused and subject to his [or her] exclusive or joint dominion and control, provided that the accused has knowledge of the presence of” the contraband).

¶17 We previously addressed the meaning of knowing possession under WIS. STAT. § 948.12(1m) in **State v. Lindgren**, 2004 WI App 159, 275 Wis. 2d 851, 687 N.W.2d 60. Numerous other courts have also confronted this question in recent years. But in **Lindgren** and *all* of the other cases that we have found, the digital images were recovered from the defendant’s hard drive. There is no forensic evidence in this case that the images were in Mercer’s hard drive. And Mercer asserts, as we interpret his arguments, that the lack of hard drive evidence

makes all the difference because one cannot possess a digital image that is not in the hard drive. Mercer even has a name for the issue at hand. He characterizes this case as a “pure view” case. The main issue, therefore, is whether a person can knowingly possess images of child pornography he or she views while browsing the Internet if there is no evidence that the images viewed were in the computer hard drive.⁷

¶18 We disagree with Mercer 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 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

⁷ This issue was certified to the Wisconsin Supreme Court on July 1, 2009. Certification was refused.

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.

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, 1267-68 (2004). We do not consider Mercer to be in the same shoes as the fictional Ian. This is not a “pure view” case.

¶19 We also disagree with Mercer's assertion that, if the images were not found in his hard drive, he could not have possessed it as a matter of law. Mercer looks to past cases where the images *were* found in the computer hard drive and posits that in order to “possess” child pornography, the evidence *must* show that the image or images were found in the hard drive.

¶20 First, none of the cases have explicitly held that hard drive evidence is the sine qua non of a knowing possession case. Rather, some of the cases discuss possession in terms of what a user can do to control images in the hard drive, *see, e.g., United States v. Tucker*, 305 F.3d 1193, 1204-05 (10th Cir. 2002) (images in a cache can be attached to an e-mail, posted to a newsgroup, placed on a website, or printed to a hard copy), and some of the cases refer to what a user can do with images displayed on a computer screen from the Internet, *see, e.g., Commonwealth v. Diodoro*, 970 A.2d 1100, 1107 (Pa. 2009), *cert. denied*, 130 S. Ct. 200 (2009) (images displayed on a computer screen from the Internet can be downloaded, printed, copied, or e-mailed). To fully understand what these cases stand for, we must examine how these courts have used hard drive evidence.

Since the particular hard drive evidence used in past cases (the “cache”) requires some technical knowledge, we will explain what a “cache” is first.

¶21 Again, we refer to the commentator who helped us with the question of when a case is a “pure view” situation and when it is not. The commentator explains the meaning of a “cache” (also known as a temporary Internet file) in the context of knowing possession of child pornography as follows:

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 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.

Howard, 19 BERKELEY TECH. L.J. at 1229-30 (footnotes omitted).

¶22 Legal commentators have also commented on the dangers of relying on cache evidence because of the automation of caching and the variation of knowledge among computer users about caching:

This process occurs automatically, without any prompting by the user, any time an Internet user visits any [webpage] Although it is possible to deactivate the cache function of a computer, the average computer user does not know how or why the process works. Even users that have a general idea of the process’s function and operation might not know how to prevent it. A user needs advanced computer skills to directly access files in the cache while the computer is offline.... Finally, the cache can be easily deleted through the web browser without any

special knowledge,^[8] or it can be deleted as part of routine computer maintenance.

Giannina Marin, *Possession of Child Pornography: Should You Be Convicted When the Computer Cache Does the Saving for You?*, 60 FLA. L. REV. 1205, 1213-14 (2008) (footnotes omitted). But computer forensic examiners, who specialize in the use of computer-related media for evidence, generally can recover the contents of a computer's cache and, with it, information about the user's browsing history. Howard, 19 BERKELEY TECH. L.J. at 1235-36. This browsing history includes the particular websites visited, the number of times visited, the degree of manipulation (such as enlarging, cutting, or pasting an image), and any downloading activity. *Id.* at 1236.

¶23 It seems to us that the facts and inferences derived from cache evidence is not all that different than that derived from the monitoring software employed by the city of Fond du Lac in this case. Both show which websites were visited and how often. Both show what the user searched for and how the user got to the website. Both record the computer user's web browsing activity. The only difference is that the evidence from the monitoring software device was instantly

⁸ The same legal commentator explained how one would delete the cache:

Web browsers offer an option to clean that cache with a few simple clicks. In Internet Explorer, for example, it is located in the "General" tab of the "Internet Options" menu which is in turn located under the "Tools" menu. In Firefox, the user can click "Tools" and then "Clear Private Data" in order to clear the cache.

Giannina Marin, *Possession of Child Pornography: Should You be Convicted When the Computer Cache Does the Saving for You?*, 60 FLA. L. REV. 1205, 1214 n.74 (2008).

reviewable by system administrators without having to physically possess the computer.

¶24 With that in mind, we turn to the case law. In particular, we go back to *Lindgren*, which we earlier cited. In *Lindgren*, five thumbnail images and six other enlarged images of child pornography were found in Lindgren’s computer hard drive.⁹ *Lindgren*, 275 Wis. 2d 851, ¶¶11, 21. The State charged Lindgren with six counts of possession of child pornography. *Id.*, ¶11. At trial, one of the State’s computer experts testified that “for the photographs found on Lindgren’s hard drive to be stored as they were, the [user] would have had to go to the [website] and click on the small thumbnail pictures to enlarge the images. Upon clicking to enlarge the image, it would be stored on the hard drive.” *Id.*, ¶21. Lindgren argued that this did not prove possession because his expert opined that Lindgren did not save the images to his computer. *Id.*, ¶23. But the court disagreed and held that the State presented sufficient evidence of possession because Lindgren repeatedly visited child pornography websites, clicked on thumbnail images to create larger pictures for viewing, accessed five images twice, and saved at least one image to his personal file. *Id.*, ¶27.

¶25 In *Lindgren*, we adopted the reasoning of *Tucker*, which had reasonably analogous facts. In *Tucker*, the defendant viewed child pornography images on the Internet, which he knew the computer would automatically save to

⁹ It is unclear from the facts set forth in *State v. Lindgren*, 2004 WI App 159, 275 Wis. 2d 851, 687 N.W.2d 60, if the images were found in the cache or some other part of the hard drive.

the cache. See *Lindgren*, 275 Wis. 2d 851, ¶¶25, 27. We quoted *Tucker*'s holding that

Tucker ... intentionally sought out and viewed child pornography knowing that the images would be saved on his computer. Tucker may have wished that his Web browser did not automatically cache viewed images on his computer's hard drive, but he concedes he knew the Web browser was doing so. Tucker continued to view child pornography knowing that the pornography was being saved, if only temporarily, on his computer. In such circumstances, his possession was voluntary. Since he knew his browser cached the image files, each time he intentionally sought out and viewed child pornography with his Web browser he knowingly acquired and possessed the images.

Lindgren, 275 Wis. 2d 851, ¶26 (quoting *Tucker*, 305 F.3d at 1205). *Tucker* also held that the defendant had control over the images because there was unrebutted expert testimony that images in a cache can be attached to an e-mail, posted to a newsgroup, placed on a website, or printed to a hard copy. *Tucker*, 305 F.3d at 1204-05. Finally, *Tucker* described, in its discussion of the facts, a litany of other evidence that the jury heard—testimony that the computer user deleted a large number of files a few days before the police searched it, had tens of thousands of images of child pornography on his computer, repeatedly visited the same websites, and clicked thumbnails to enlarge them. *Id.* at 1197-98.

¶26 Both *Lindgren* and *Tucker* focused on web browsing activity. The evidence in *Lindgren* included repeated actions to seek and obtain child pornography over the Internet and manipulation and control of the images by clicking on them; whereas, in *Tucker*, the evidence also included deletion of images, knowledge of the cache, and a high number of images. And both courts described the facts of the case in terms of the defendants' affirmative actions to reach out for and obtain child pornography and the ability or actions taken to

control the images. See *Lindgren*, 275 Wis. 2d 851; ¶27; *Tucker*, 305 F.3d at 1204-05. The focus on these two types of behavior is seen in other cases as well. We will discuss only one, but we cite others in a footnote.¹⁰

¶27 The case with the facts that are the most similar to this case is *Diodoro*. That case addressed the question of “whether accessing and viewing child pornography over the [I]nternet constitutes ‘control’ of such pornography.” *Diodoro*, 970 A.2d at 1100. In *Diodoro*, 340 images of suspected child pornography and thirty additional images of known child pornography were found on Diodoro’s computer. *Id.* at 1100. The statute in that case criminalized the knowing possession or control of child pornography. See *id.* at 1100 n.1. The forensic examiner explained that “he searched the images and web history on [Diodoro’s] hard drive using forensic software, which revealed, *inter alia*, web pages pertaining to child pornography websites, and 370 images relating to child pornography that were stored in the cache files or unallocated space of the hard drive.” *Id.* at 1101. The examiner further testified that the images stored in the cache “indicated that someone accessed the child pornography websites and by

¹⁰ See, e.g., *State v. Mobley*, 118 P.3d 413, 416 (Wash. Ct. App. 2005) (holding that the question is “whether the totality of the circumstances establish[] that [the] defendant reached out for and exercised dominion and control over the images at issue;” “evidence of ‘reaching out for’ and ‘controlling’ child pornographic images is incriminating, while inadvertent viewing questions are left to the fact finder”); *Ward v. State*, 994 So.2d 293, 301 (Ala. Crim. App. 2007) (holding that the question is: “Did the defendant specifically seek out the prohibited images and did he [or she] have the ability to exercise dominion and control over those images?”); *United States v. Romm*, 455 F.3d 990, 998 (9th Cir. 2006) (“In the electronic context, a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it.”); *Commonwealth v. Simone*, 63 Va. Cir. 216, 2003 WL 22994238, *32 (Va. Cir. Ct. 2003) (holding that the question is: “Did the defendant reach out for and control the images at issue”).

clicking the ‘next’ button or a specific image, accessed and viewed the various images.” *Id.*

¶28 *Diodoro* summarized this behavior by determining whether it showed that Diodoro “purposefully search[ed] child pornography] out on the [I]nternet,” “intentionally view[ed] it,” and could control it. *See id.* at 1107. As to reaching out for the images, the court stated: “[T]he viewer has affirmatively clicked on images of child pornography from different websites and the images are therefore purposefully on the computer screen before the viewer.” *Id.* And as to control, the court explained that the conduct of *purposefully* viewing child pornography is control “because the viewer may, *inter alia*, manipulate, download copy, print, save or e-mail the images.” *Id.* The court considered it unimportant “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.” *Id.* Instead of focusing on the cache, which is a computer technology not necessarily known to the average computer user, the court focused on the control users have over their web browsing and concluded: “The use and operation of computers are not the novelty they once were. Control via a computer is little different from the control one exercises by viewing a book or a magazine—whether one purchases the tangible image or not.” *Id.*¹¹

¹¹ While the statute in *Commonwealth v. Diodoro*, 970 A.2d 1100, 1101 n.1 (Pa. 2009), states control or possession and Wisconsin’s statute states only possession, we conclude this is a distinction without a difference because Wisconsin’s pattern jury instructions say “actual physical control,” WIS JI—CRIMINAL 2146A, and the definition of constructive possession includes control, *see Schmidt v. State*, 77 Wis. 2d 370, 379, 253 N.W.2d 204 (1977).

¶29 Our impression of these cases is that courts are more concerned with how the defendants got to the website showing child pornography, than what the defendants actually did with the images. In all of the cases, the defendant *reached out* for the images. This fits with the definition of constructive possession: the user could save, print or take some other action to control the images, and the user affirmatively reached out for and obtained the images knowing that the images would be child pornography as shown by the pattern of web browsing. This may occur whether there is cache evidence or not. And that is the main point to be made here.

¶30 At oral argument, the State provided the following explanation of how viewing images and web browsing can constitute reaching out for images by describing the difference between “push technology” and “pull technology.” In push technology, the receiver does not request the materials. The cyber equivalent is spam. The real world equivalent would be like walking on a route, which you cannot change, that has a newsstand displaying risqué magazines for passersby. As the State explained, people confronted with push technology “are not asking to see it, but it’s there to view.” In contrast, pull technology is where the receiver is asking for the materials. The cyber equivalent is clicking on a button and asking something to come to you. Similarly, the real world equivalent would be like writing to a company and asking it to send you its marketing literature.

¶31 This distinction makes sense to us, because in pull technology the user knows what he or she is looking for and is making a request to obtain that material. So we conclude that an individual knowingly possesses child pornography when he or she affirmatively pulls up images of child pornography on the Internet and views those images knowing that they contain child pornography. Whether the proof is hard drive evidence or something else, such as

the monitoring software here, should not matter because both capture a “videotape” of the same behavior. And images in either place can be controlled by taking actions like printing or copying the images.

¶32 *Commonwealth v. Simone*, 63 Va. Cir. 216, 2003 WL 22994238, *32 (Va. Cir. Ct. 2003), which we cited in a footnote earlier, framed the question as being “whether a defendant has reached out for and controlled the images.” The court reasoned that such is the appropriate question to ask because it recognizes and promotes the purpose behind such statutes as delineated by the United States Supreme Court: the protection of the physical and psychological well being of juveniles, *New York v. Ferber*, 458 U.S. 747, 756-57 (1982), and destruction of the market for the exploitative use of children, *Osborne v. Ohio*, 495 U.S. 103, 109 (1990). *Simone*, 2003 WL 22994238, *32. As the *Simone* court explained, “If there is no reaching out for and controlling of such images, then presumably juveniles will be in less demand for such exploitation, with a resulting reduction in physical and psychological harm.” *Id.*

¶33 Here, the evidence supporting the verdict tended to show, and the jury could find from it, that Mercer had a habit of surfing the Internet for pornography. He searched with terms associated with child pornography and looked at images and text stories. And his searches were not an isolated instance. He had searched using those terms on at least fifty different days. He was able to navigate directly to a web portal specific to sex. Moreover, on the day in question, he did not click on a website, see a child pornography image, and exit the website (indicating a mistake)—he clicked to look at a magazine and its images, had the image on his screen until he clicked back, at which point he looked at another magazine and its images and another and another and another. Then he left, did something else, and returned to look at still more magazines and images. And

each time he pulled an image from the Internet onto his screen he controlled how long it was displayed on his screen and he had the ability to and knew how to print, save, or copy it.¹² Moreover, the jury heard evidence from which it could infer that Mercer deleted the files where the forensic examiners would have found the child pornography stored in his hard drive.¹³ We conclude that there was sufficient evidence of knowing possession as a matter of law.

¶34 In so holding, we reject Mercer’s corollary argument that the jury instruction¹⁴ on the meaning of possession should have stated that “the image must

¹² Mercer’s computer forensic expert testified that nothing on the Lolita News website limited access to images that would prevent the viewers from clicking on images to save or print them.

¹³ We note that the evidence at trial suggested that the reason the images were not in the cache was that Mercer regularly deleted those files. Mercer testified at trial that he was instructed by a Fond du Lac computer information systems employee to frequently delete these files to maintain the efficiency of his computer. And he stated that he did delete the files when he remembered, which varied from deleting the files daily to weekly, though he could not remember if he deleted the files on the day in question. As we mentioned earlier, there was evidence that Mercer searched for software programs which also would delete his Internet history.

¹⁴ The trial court instructed the jury that

[p]ossessed means that the defendant knowingly had actual physical control of the recording, or that the recording is in an area over which the person has control and the person intends to exercise control over the recording.

In cases involving digital images, if you are satisfied that the defendant intentionally visited child pornography websites when [sic] contained child pornography images; and (a) acted on or manipulated the child pornography image; or (b) viewed the child pornography image knowing that his web browser automatically saved the image in the temporary Internet cache file; you may find knowing possession of such images.

(continued)

be able to be accessed later and that the accused has to know not only that it goes to a ‘location’ on his computer, but that it can be accessed and that he has acted on or manipulated the images to allow for more ready access.” As the State aptly notes and as we have already decided, all the statute requires is that the defendant knowingly had actual physical control of the item. The conduct described by Mercer is not necessary proof but is rather a typical evidentiary indication.

¶35 Here, the trial court instructed the jury that possessed means “actual physical control” and then it went on to give examples of what could constitute possession. In doing so, it described cache evidence as an example of possession. As we explained above, cache evidence is not required to prove possession because people can control an image they view from the Internet just as they can from the cache. The jury instruction therefore actually inured to Mercer’s benefit because it gave an example fitting his theory of defense, a defense to which he was not entitled. We conclude that there was no harm to Mercer and reject his objection to the jury instructions. *See State v. Courtney*, 74 Wis. 2d 705, 716, 247 N.W.2d 714 (1976).

¶36 Having dealt with the issue of law as to whether the facts support the applicable statute, we now review Mercer’s “question of fact” arguments that there was no credible evidence to support the jury verdict. First, he asserts that any possession was involuntary and unintentional. Like he testified at trial, he argues

It is not required that a person own a recording in order to possess it. What is required is that the person exercise control over the recording. Recording means a reproduction of an image or a sound or the storage of data representing an image or a sound, including a digital image.

that the images were displayed on his screen because of a pop-up, pop-under, virus, or some similar problem that would create a loop of unwanted images or a redirect to an undesired website that displayed child pornography.

¶37 At trial, however, the jury heard testimony from the software's cofounder that, based on the log, the images could not have been a pop-up or pop-under. As to pop-ups, the jury heard that there would be no reason to click on the same image three or four times, like he did with some of the images, and no reason for a click before each image was displayed. The jury also saw a live demonstration of how the software works and, during that demonstration, a pop-up appeared which did not show up on the log. And as to pop-under, the jury heard that pop-under displays beneath the current application on a computer. So for the software to record a pop-under, Mercer would have had to click on it. But, there was not enough time between log entries for Mercer to have seen the window displayed beneath the current application and to have clicked on the pop-under.

¶38 And though Mercer testified that "this was one of those endless loops that you got into when you start to exit out by hitting that small X button in the upper right-hand corner [then] more and more things would begin to pop up" and you can only get out of the loop by restarting the computer, he never reported the problem and the log shows that he never turned off or restarted his computer after either of the times the images of child pornography were displayed on his computer.

¶39 Second, Mercer claims that a virus caused the images to be displayed on his computer. But, the jury heard from a computer forensics expert who testified at trial. The expert testified that he investigated the viruses on

Mercer's computer and found nothing to suggest that the viruses were related to child pornography or even fully operational.

¶40 Third, Mercer argues that six of the fourteen charged images do not show “sexually explicit conduct.” WISCONSIN STAT. § 948.01(7)(e) defines “sexually explicit conduct” as “actual or simulated” “[l]ewd exhibition of intimate parts.” The term “lewd” contemplates that the jury should use common sense to determine whether the pictures show nudity and are sexually suggestive. *See State v. Petrone*, 161 Wis. 2d 530, 561-62, 468 N.W.2d 676 (1991). We have viewed the images Mercer challenges. They all show young girls that are nude or partially nude and in posed positions that are sexually suggestive. And the young girls who are partially nude are also dressed in outfits that the jury could conclude adds to the sexual suggestiveness. We reject this challenge. We conclude that all of Mercer's claims regarding “questions of fact” must fail.

¶41 At the end of the day, the common thread underlying Mercer's arguments is the hypothesis that computers are only knowable to the technically savvy and he—not being of that ilk—could not have had the technical know-how necessary to “possess” pornography. For example, he contends that he has no real expertise in the caching process. But, while it is true that some computer-related issues may require expertise, that simply is not the case in many situations. People do not cower and sit in a corner every time the word “computer” is mentioned. Computers are becoming more and more a fact of everyday life. Technology issues aside, the facts before the jury were very clear and easy to understand. The jury could infer that an individual, who searches for a term associated with child pornography on *repeated* occasions, should be aware that he or she is controlling the request that child pornography be sent to him or her. And when that individual sees that the selected website shows images of child pornography and continues

browsing through that website with the ability to control those images, a jury could conclude that the individual knowingly possessed the material. In this case, Mercer'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. The evidence is sufficient to show knowing possession.

Motion to Suppress

¶42 Three issues remain which are separate from his claim that he did not possess pornography. The first of these is Mercer's argument that the trial court erred in not granting his motion to suppress the statements he made during an interrogation at the time the search warrant was executed for the computer in his home. He argues that the facts show that his statements were made during a custodial interview. But the trial court concluded otherwise; it held that Mercer's testimony was not credible and did not make any sense in light of the record. "[T]he credibility of witnesses testifying at a hearing outside of the presence of the jury, such as a suppression hearing, is a question to be resolved by the trial judge." *Sanders v. State*, 69 Wis. 2d 242, 253, 230 N.W.2d 845 (1975). We resolve any conflicting testimony in favor of the trial court's finding. *State v. Flynn*, 92 Wis. 2d 427, 437, 285 N.W.2d 710 (1979). We have reviewed the record, and the trial court's finding is not clearly erroneous. See *State v. Turner*, 136 Wis. 2d 333, 343-44, 401 N.W.2d 827 (1987).

Other Acts Evidence

¶43 Mercer also objects to the trial court allowing the State to present other acts evidence. The other acts evidence Mercer objects to is evidence (1) of other Internet searches for child pornography, (2) that Mercer accessed image files

from a website which “depicted children in sexually suggestive or sexually explicit manners,” (3) that Mercer accessed sexually explicit text websites which included sex with minors, and (4) of nineteen other images on the hard drive that were not charged. Mercer argues that the cumulative effect of this evidence was too prejudicial to his character, so prejudicial that the jury must have improperly considered the evidence. But this was a discretionary decision of the trial court. We will uphold the trial court’s evidentiary rulings if it “examined the relevant facts, applied a proper standard of law, used a demonstrated rational process, and reached a conclusion that a reasonable judge could reach.” *State v. Walters*, 2004 WI 18, ¶14, 269 Wis. 2d 142, 675 N.W.2d 778. The trial court examined the facts the State wanted to present, examined the relevant law, and concluded that while the evidence was relevant, some of it should be excluded because of the remoteness in time. The court limited, for example, evidence of the variations on the words “lolita” and “preteens” because “[o]therwise there could be a whole slew or panoply of words.” Though there was still a significant amount of other acts evidence presented at trial, we hold that the trial court did not erroneously exercise its discretion in finding that “the probative value far outweighs any prejudicial effect.” We uphold the trial court’s reasoned determination that the evidence went directly to Mercer’s defense that he was not searching for child pornography and that the other acts evidence was “extremely similar” to Mercer’s conduct on the day he reached out for and viewed the charged images.

Motion in Limine

¶44 Finally, Mercer challenges the trial court’s denial of his motion in limine to exclude evidence that he destroyed the hard drive on his home computer in late March 2005. This again, was a discretionary decision of the trial court. The trial court concluded that it would admit the evidence because it was relevant

to consciousness of guilt. That decision was also a reasoned one based on the facts of record and the applicable law.

By the Court.—Judgment affirmed.

