STATE OF NEBRASKA, APPELLEE, V. MATTHEW C. SCHULLER, APPELLANT.

843 N.W.2d 626

Filed February 21, 2014. No. S-13-221.

1. **Constitutional Law: Search Warrants: Affidavits.** A claim that an affidavit is insufficient to justify issuance of a search warrant is a Fourth Amendment claim.
2. **Constitutional Law: Search and Seizure: Motions to Suppress: Appeal and Error.** In reviewing a trial court's ruling on a motion to suppress based on a claimed violation of the Fourth Amendment, an appellate court applies a two-part standard of review. Regarding historical facts, an appellate court reviews the trial court's findings for clear error. But whether those facts trigger or violate Fourth Amendment protections is a question of law that an appellate court reviews independently of the trial court's determination.
3. **Search Warrants: Affidavits: Probable Cause.** In *Franks v. Delaware*, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978), the U.S. Supreme Court held that a search warrant may be invalidated if a defendant proves that the affiant officer knowingly and intentionally, or with reckless disregard for the truth, included in his or her affidavit false or misleading statements which were necessary to establish probable cause. This rationale extends to omissions in warrant affidavits of material information.
4. **Trial: Convictions: Appeal and Error.** An appellate court will sustain a conviction in a bench trial of a criminal case if the properly admitted evidence, viewed and construed most favorably to the State, is sufficient to support that conviction.
5. **Convictions: Evidence: Appeal and Error.** When reviewing a criminal conviction for sufficiency of the evidence to sustain the conviction, an appellate court does not resolve conflicts in the evidence, pass on the credibility of witnesses, evaluate explanations, or reweigh the evidence presented, which are within a fact finder's province for disposition. Instead, the relevant question 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.
6. **Statutes.** Statutory language is to be given its plain and ordinary meaning.
7. **Statutes: Criminal Law.** The definition of an act forbidden by statute, but not defined by it, may be ascertained by reference to the common law.
8. **Evidence: Proof.** Actual possession is synonymous with physical possession. Constructive possession, however, may be proved by mere ownership, dominion, or control over contraband itself, coupled with the intent to exercise control over the same.
9. **Criminal Law: Evidence: Words and Phrases.** Under Neb. Rev. Stat. § 28-813.01 (Cum. Supp. 2012), "possess" includes constructive possession.
10. **Criminal Law: Evidence.** A defendant cannot intentionally procure and subsequently dispose of a depiction of child sexually abusive material without having either actual or constructive possession.

Appeal from the District Court for Lancaster County: KAREN B. FLOWERS, Judge. Affirmed.

Robert B. Creager, of Anderson, Creager & Wittstruck, P.C., L.L.O., for appellant.

Jon Bruning, Attorney General, and Melissa R. Vincent for appellee.

HEAVICAN, C.J., WRIGHT, CONNOLLY, STEPHAN, MCCORMACK, MILLER-LERMAN, and CASSEL, JJ.

CONNOLLY, J.

I. SUMMARY

Matthew C. Schuller admitted to periodically searching for, downloading, viewing, and then deleting child pornography computer files. Despite his efforts to delete the files, a forensic examination revealed remnants on his hard drive. Following a bench trial, the district court found Schuller guilty of knowingly possessing child pornography. The issues are (1) whether the investigator's failure to explain in his affidavit that dynamic Internet Protocol (IP) addresses can change tainted the probable cause determination and (2) whether the evidence was sufficient to find that Schuller "knowingly possess[ed]" child pornography as stated in Neb. Rev. Stat. § 28-813.01(1) (Cum. Supp. 2012). We conclude that the investigator's omission did not affect the probable cause determination and that the State adduced sufficient evidence to support Schuller's conviction. We affirm.

II. BACKGROUND

1. INVESTIGATION

In investigating child pornography crimes, law enforcement agencies use third-party databases to identify IP addresses associated with suspected child pornography files. An IP address is a unique number that an Internet service provider assigns to a computer or other device on the Internet.[1] These

[1] See, e.g., *Patco Const. Co., Inc. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012).

databases identify IP addresses which have (through peer-to-peer file-sharing software) made available for download known or suspected child pornography files. Essentially, peer-to-peer file-sharing software connects many different computers across the Internet and allows them to share their files with other connected computers.[2]

Law enforcement agencies then use specialized software to automatically browse for and download suspected child pornography files from those IP addresses. Once an IP address is confirmed to have child pornography files, law enforcement agencies subpoena the Internet service provider for the relevant subscriber information. That information generally includes a name and the subscriber's physical address, and then law enforcement agencies obtain a warrant, seize evidence, and make arrests.

Sgt. John Donahue, the lead investigator, followed that process. On July 16, 2011, Donahue used a program called E-Phex to browse IP addresses within his jurisdiction and connected to a computer with a specific IP address. E-Phex obtained a list of that computer's shared files (files available for download through the file-sharing software), which contained one suspected child pornography file. On July 22, Investigator Corey Weinmaster subpoenaed the Internet service provider and requested the subscriber information for that IP address for various times on July 17 and 19. On July 28, the Internet service provider sent the requested information, which identified an individual (presumably Schuller's father) as the account holder, with a specific physical address located on Blackstone Road in Lincoln, Nebraska. Further surveillance of that IP address revealed that an additional 13 suspected child pornography files were linked with that IP address between July 17 and September 21. Donahue downloaded four of those files and confirmed that they were child pornography.

On September 27, 2011, Donahue applied for and received a search warrant. In his affidavit in support of his request, Donahue set out the above facts. He also included other

---

[2] See, e.g., *U.S. v. Vadnais*, 667 F.3d 1206 (11th Cir. 2012).

significant information regarding his training, the typical investigation process in these kinds of cases, the type of evidence he hoped to find, and the types of items he wished to seize. A county judge granted his request for a warrant.

2. Police Execute Search Warrant

On September 30, 2011, Donahue executed the search warrant. During the search, officers located and seized three computers, including Schuller's laptop. Weinmaster seized the laptop, which at the time was running a disk-wiping program. A disk-wiping program overwrites data, which permanently removes it from the hard drive.[3] Weinmaster removed the battery from the laptop to stop the program from running. As the search continued, Donahue met with Schuller, who agreed to speak with Donahue.

Schuller, 20 years old, admitted that he had been using peer-to-peer file-sharing software to download child pornography since he was 14 years old. Schuller admitted that he would search for files using search terms like "pedo" and "boys" to find movies he wanted to watch. He would then download those movies, watch them, and then delete them. "Deleting" a computer file is a misnomer, because doing so does not actually remove it from the computer. Deleting a file only marks the location as available to be overwritten; the file is not actually removed until that happens.[4] Schuller admitted that he had downloaded hundreds of movies (though they apparently were all the same 10 to 15 movies, just repeatedly downloaded and deleted) and that he had downloaded movies just a few days before.

Schuller then accompanied Donahue to the Lincoln Police Department, where he again agreed to speak with Donahue.

---

[3] See, e.g., Brad Chacos, How to securely erase your hard drive, http://www.pcworld.com/article/261702/how_to_securely_erase_your_hard_drive.html (Sept. 3, 2012) (explaining that to permanently delete computer data requires software which overwrites that data) (last visited Feb. 10, 2014).

[4] 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 (2004).

In this interview, Schuller made the same admissions he had made earlier at his home. In addition, he admitted that when he deleted the files, he used a disk-wiping program (which would overwrite the files) to remove any traces of them from his computer. He also admitted that he knew that what he had been doing was illegal and that his inability to stop doing it was depressing. Eventually, he requested a lawyer and Donahue ended the interview.

3. Information and Motion to Suppress

The State filed an information against Schuller on December 9, 2011, for possession of child pornography.[5] Before trial, Schuller moved to suppress all evidence resulting from the earlier search and seizure. Schuller generally argued that the underlying basis for Donahue's conclusion that the files were child pornography, "SHA1 hash values," was not reliable. SHA1 hash values are digital signatures for files on a peer-to-peer network; all files have a SHA1 hash value, and if two files have the same one, they are the *exact* same file. Schuller also argued that, under *Franks v. Delaware*,[6] Donahue's affidavit in support of the search warrant was materially misleading because it did not include any information regarding the difference between dynamic and static IP addresses. Generally, the difference is that dynamic IP addresses can change, while static ones cannot.

The district court overruled Schuller's motion. The court found no need to address the reliability of SHA1 hash values, because Donahue "personally observe[d] images of child pornography associated with Schuller's IP address and told the County Judge so." Schuller did not appeal this ruling. Regarding Schuller's *Franks* challenge, the court noted that the file-sharing software assigned a functionally unique identifier to each computer on the network. This identifier, known

---

[5] See § 28-813.01.

[6] *Franks v. Delaware*, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978).

as the GUID, identified the specific computer making the child pornography files available to download. The court then emphasized that neither the GUID nor the IP address associated with it ever changed over the course of the investigation. As such, "[t]here was never a question that the pornography Donahue identified might have come from somewhere other than a single computer located at [the] Blackstone Road [address]." Thus, the court concluded that there was no reason for Donahue to discuss the difference between dynamic and static IP addresses.

4. Trial, Verdict, and Sentence

At the bench trial, Donahue was the only witness. Generally, Donahue testified regarding his investigation, the various computer programs and processes involved, his interviews with Schuller, and his forensic examination of Schuller's laptop. Regarding his examination of Schuller's laptop, Donahue explained that he used a program known as Forensic Toolkit. This program essentially copies the target hard drive and then looks for and retrieves all noteworthy images and files on the drive. This includes hidden files, deleted files, and sometimes encrypted files.

Going through the Forensic Toolkit report, Donahue explained that he had found 88 graphic files on the hard drive. These were still images of child pornography. Donahue explained that 10 of these files were not "carved" files, meaning that they were not deleted, in the sense that they were accessible to Schuller. Donahue explained that Schuller could have "copied, printed, e-mailed, [or] saved" these 10 files. He later clarified that Schuller apparently attempted to delete those files, but that some backup function saved them and moved them to another directory in the computer. So, although Schuller could have accessed and manipulated these files, he did not necessarily know they existed or where they were. The other 78 files were "carved," meaning that they had been deleted and that Schuller, an ordinary computer user, no longer had access to these files. Donahue also explained that although the wiping program had been running, the program

itself maintained a record of the names of files it had overwritten. These names were consistent with names for child pornography files.

Following the bench trial, the court found Schuller guilty. The court sentenced Schuller to 3 years' probation and ordered him to register as a sex offender.

III. ASSIGNMENTS OF ERROR

Schuller assigns, restated, that the court erred in (1) denying his motion to suppress and (2) finding sufficient evidence to find Schuller guilty of knowingly possessing child pornography.

IV. ANALYSIS

1. Motion to Suppress

Schuller argues that Donahue's failure to explain in his affidavit that dynamic IP addresses can change tainted the probable cause determination. As such, Schuller argues that under *Franks*,[7] the resulting warrant was invalid and the court should have suppressed the seized evidence. The State disagrees. It argues that because the IP address at issue was almost certainly assigned to Schuller's home throughout the investigation, the fact that dynamic IP addresses can change was immaterial. We agree with the State.

(a) Standard of Review

[1,2] A claim that an affidavit is insufficient to justify issuance of a search warrant is a Fourth Amendment claim.[8] In reviewing a trial court's ruling on a motion to suppress based on a claimed violation of the Fourth Amendment, we apply a two-part standard of review. Regarding historical facts, we review the trial court's findings for clear error. But whether those facts trigger or violate Fourth Amendment protections is a question of law that we review independently of the trial court's determination.[9]

---

[7] See *id*.

[8] See, e.g., *State v. Nuss*, 279 Neb. 648, 781 N.W.2d 60 (2010).

[9] See, e.g., *State v. Sprunger*, 283 Neb. 531, 811 N.W.2d 235 (2012).

(b) Analysis

[3] In *Franks*,[10] the U.S. Supreme Court held that a search warrant may be invalidated if a defendant proves that the affiant officer "knowingly and intentionally, or with reckless disregard for the truth," included in his or her affidavit false or misleading statements which were necessary to establish probable cause.[11] Courts have extended the *Franks* rationale to "omissions in warrant affidavits of material information."[12] In this "so-called reverse-*Franks* situation," if the defendant shows that the police knowingly and intentionally, or with reckless disregard for the truth, omitted information material to a probable cause finding, a reviewing court will reexamine the affidavit (with the omitted information) and determine whether it still establishes probable cause.[13] If it does not, then *Franks* requires that "the search warrant . . . be voided and the fruits of the search excluded."[14]

Schuller argues that such is the case here. Schuller argues that dynamic IP addresses (such as in this case) can change, while static IP addresses cannot. Schuller argues that Donahue knowingly and intentionally, or with reckless disregard for the truth, omitted that information from his affidavit and that doing so "tainted the probable cause determination."[15] Essentially, this is because, as a dynamic IP address, there was no guarantee that it remained assigned to Schuller's home throughout the investigation.

We conclude that Donahue's omission was immaterial to the probable cause determination and therefore did not run afoul of *Franks*. At the hearing, Donahue testified that he monitored the IP address' activity from July 16 to September 27, 2011.

---

[10] See *Franks, supra* note 6, 438 U.S. at 155.

[11] See, also, *U.S. v. Smith*, 715 F.3d 1110 (8th Cir. 2013).

[12] Annot., 72 A.L.R.6th 437, 449 (2012). See, also, *Smith, supra* note 11; *Sisson v. State*, 903 A.2d 288 (Del. 2006); *State v. Spidel*, 10 Neb. App. 605, 634 N.W.2d 825 (2001); *Smith v. Sheriff*, 506 Fed. Appx. 894 (11th Cir. 2013).

[13] See *Sisson, supra* note 12, 903 A.2d at 300.

[14] *Franks, supra* note 6 at 156.

[15] Brief for appellant at 14.

Donahue testified that throughout that period, the IP address, and its associated GUID, never changed. Recall that a GUID is a functionally unique identifier assigned by the file-sharing software to each computer on the network. Donahue testified that in other words, the same computer repeatedly shared child pornography using the same IP address. This suggests, as the State argues, that the IP address was assigned to only a single location—Schuller's home—throughout the investigation. This led the district court to conclude, correctly in our view, that "[t]here was never a question that the pornography Donahue identified might have come from somewhere other than a single computer located at [the] Blackstone Road [address]." We agree with the State and the court that, in this case, omitting the challenged information was immaterial to the probable cause determination.

We briefly note that Schuller emphasizes that the IP address was initially associated with child pornography files on July 16, 2011, but that police requested the subscriber information for the IP address for July 17 and 19. Schuller argues that "since law enforcement asked for information about the holder of that IP address on a different date, the failure to inform the magistrate that on a different date, that IP address could have been assigned to a different holder, would have undercut the entire theory of the investigation."[16]

We do not agree. Donahue testified that *from July 16* to September 27, 2011, neither the GUID nor the IP address ever changed. Considering the subscriber information, the most likely conclusion is that the IP address was also assigned to Schuller's home on July 16. But even were we to agree with Schuller about the alleged uncertainty of the IP address' assigned location on July 16, it would not "undercut the entire theory of the investigation." The fact remains that police observed that IP address sharing child pornography files on July 17 and 19, and further observed that IP address sharing child pornography files at various times up to September 21. As explained above, during those times, there was no real question that the IP address was assigned to Schuller's home,

---

[16] *Id.* at 15.

because neither the IP address nor the GUID ever changed during that time. This assigned error has no merit.

2. Sufficiency of Evidence

Schuller argues that the evidence was insufficient to conclude that he "knowingly possess[ed]" child pornography. He questions the applicability of the common-law principles of constructive possession to computer files downloaded from the Internet, and he argues that even if they do apply, the evidence was insufficient to show control or intent to control child pornography. We conclude that the principles of constructive possession apply here. And because Schuller repeatedly searched for, downloaded, viewed, and deleted child pornography, we conclude that the evidence was sufficient to support a finding that he knowingly possessed it.

(a) Standard of Review

[4,5] We will sustain a conviction in a bench trial of a criminal case if the properly admitted evidence, viewed and construed most favorably to the State, is sufficient to support that conviction.[17] In making this determination, we do not resolve conflicts in the evidence, pass on the credibility of witnesses, evaluate explanations, or reweigh the evidence presented, which are within a fact finder's province for disposition.[18] Instead, the relevant question 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.[19]

(b) Analysis

Section 28-813.01(1) explains that "[i]t shall be unlawful for a person to knowingly possess any visual depiction of sexually explicit conduct . . . which has a child . . . as one of its participants or portrayed observers." The parties do not dispute that this case involves "visual depiction[s] of

---

[17] See *State v. Lamb*, 280 Neb. 738, 789 N.W.2d 918 (2010).

[18] See *id.*

[19] See *id.*

sexually explicit conduct" involving a child (child pornography). Instead, the sole issue is whether the evidence was sufficient to convict Schuller of "knowingly possess[ing]" child pornography.

[6,7] Neb. Rev. Stat. § 28-1463.02 (Cum. Supp. 2012) defines several key words and phrases used in § 28-813.01, such as "child," "sexually explicit conduct," and "visual depiction." But it does not define "knowingly possess." Several doctrines, however, inform our interpretation of that phrase. It is an oft-stated rule that "'[s]tatutory language is to be given its plain and ordinary meaning . . . .'"[20] We have also explained that "[t]he definition of an act forbidden by statute, but not defined by it, may be ascertained by reference to the common law."[21]

[8] Black's Law Dictionary defines "possess" as "[t]o have in one's actual control; to have possession of."[22] It defines "possession" to include, among other things, both actual and constructive possession,[23] and our common law similarly recognizes both.[24] Actual possession is synonymous with physical possession.[25] Constructive possession, however, may be proved by mere ownership, dominion, or control over contraband itself, coupled with the intent to exercise control over the same.[26]

The initial question is whether "possess" in § 28-813.01 includes constructive possession. In other contexts, we have come to different conclusions. For example, in the narcotics context, we have long held that possession may be either actual or constructive.[27] In contrast, we have held that possession of

---

[20] *State v. Johnson*, 269 Neb. 507, 518, 695 N.W.2d 165, 174 (2005).

[21] *State v. Mattan*, 207 Neb. 679, 684, 300 N.W.2d 810, 813 (1981).

[22] Black's Law Dictionary 1281 (9th ed. 2009).

[23] See *id*.

[24] See *State v. Garza*, 256 Neb. 752, 592 N.W.2d 485 (1999).

[25] See *id*.

[26] See *id*.

[27] See, e.g., *id*.; *State v. Faircloth*, 181 Neb. 333, 148 N.W.2d 187 (1967).

a weapon during the commission of a felony does not include constructive possession.[28]

[9] We conclude that "possess" in § 28-813.01 must include constructive possession. Unlike our prior cases, here we are not discussing tangible objects such as narcotics or a physical weapon. Instead, we are discussing computer files, which are intangible objects. It is difficult to see how a person could actually possess, that is, physically possess, a computer file. As such, if "possess" in § 28-813.01 did not include constructive possession, it would seemingly be impossible to prosecute possession of computer files containing child pornography. This goes against the Legislature's clear intent, as derived from the statutory language. Section 28-1463.02 explains that "[v]isual depiction means live performance or photographic representation and includes any undeveloped film or videotape *or data stored on a computer disk or by other electronic means which is capable of conversion into a visual image, . . . whether made or produced by electronic, mechanical, computer, digital, or other means*."[29] We hold that, under § 28-813.01, "possess" includes constructive possession.[30]

Recall that constructive possession may be proved by mere ownership, dominion, or control over contraband itself, coupled with the intent to exercise control over the same.[31] With that in mind, the question is whether the evidence was sufficient for a rational trier of fact to have found beyond a reasonable doubt that Schuller "knowingly possess[ed]" child pornography. We conclude that it was.

It bears emphasizing that Schuller did not simply click on an innocuous banner advertisement and end up at a child pornography Web site; instead, he installed and used file-sharing software to search for and download child pornography. Donahue testified as to the various steps Schuller would have taken to use the software: "He would have to open up

---

[28] See *Garza, supra* note 24.

[29] § 28-1463.02(6) (emphasis supplied).

[30] Cf. *People v. Flick*, 487 Mich. 1, 790 N.W.2d 295 (2010).

[31] See *Garza, supra* note 24.

the LimeWire client. He would have to put in search terms that are associated with child pornography. He would view the title of the file, possibly the extension and double click on it to start the program downloading the file." Donahue testified that the forensic examination revealed that Schuller did in fact download the files, which were identifiable child pornography videos.

Once the downloads were complete, Schuller could have done any number of things with the file, such as change its name, relocate it, and, of course, view it, for as many times as he wished. The record shows that Schuller viewed the files and that, once done, he deleted them and used a wiping program to remove all traces of them from his computer, though he was ultimately unsuccessful in doing so. In an interview with Donahue, Schuller admitted essentially all of these facts. All of this shows both control and intent to control, which satisfies the elements of constructive possession. There is also no question that Schuller *knowingly* possessed those files. His use of the file-sharing software and his confession, among other things, confirm that he acted knowingly.

Also, the evidence was sufficient to satisfy the other elements of the crime. Schuller, in his reply brief, admits that "the uncontested evidence is that he searched the internet for images of child pornography by using file sharing software that allowed him to obtain such images from other computers and view those images on his computer."[32] Donahue averred in his affidavit that he downloaded and watched several of the videos available for download from Schuller's computer; based on Donahue's summaries of those videos, they constituted child pornography. Donahue also testified that several of the files available for download from Schuller's computer had SHA1 hash values identified as child pornography files. There was no question that this case involved images and videos of child pornography.

The evidence was also sufficient to conclude that Schuller's knowing possession occurred within the timeframe alleged in the information. Not only were his IP address and GUID

---

[32] Reply brief for appellant at 2.

associated with child pornography files during that time, but Schuller admitted to having searched for, downloaded, viewed, and deleted child pornography files a couple days before his arrest. The evidence was sufficient to support finding, beyond a reasonable doubt, that Schuller knowingly possessed child pornography[33] within the timeframe alleged in the information.

Obviously, Schuller disagrees, and he makes a variety of arguments as to why our conclusion is incorrect. He argues that Nebraska law, unlike federal law, does not criminalize the mere viewing of child pornography, but only its possession,[34] and he asserts that all he did was the former. He also argues that downloading alone could not be sufficient evidence of possession. Notably, too, he argues, for multiple reasons, that there was simply no evidence that he intended to exercise control over child pornography. Specifically, he emphasizes that there was no evidence he "copied, saved, emailed, put on a hard drive or disk" any child pornography,[35] and that his deleting and wiping of the child pornography files indicated an intent *not* to control them.

We find these arguments unpersuasive. First, this is not a case of "mere viewing." In the "cache" file context, one commentator[36] gives a helpful example of a "mere viewing" situation: An office worker intentionally seeks out child pornography on various Web sites, and views and manipulates those pictures (e.g., enlarges them). An innocent coworker happens to go into the office while the office worker does this and sees the images on the computer screen for several seconds. The innocent coworker had not affirmatively sought out the child pornography, nor did he have any ability to control or manipulate the images. He therefore did not knowingly possess those images. Unlike the innocent worker in that hypothetical,

---

[33] See, *U.S. v. Haymond*, 672 F.3d 948 (10th Cir. 2012); *U.S. v. McArthur*, 573 F.3d 608 (8th Cir. 2009); *U.S. v. Romm*, 455 F.3d 990 (9th Cir. 2006); *State v. McKinney*, 699 N.W.2d 460 (S.D. 2005).

[34] Compare § 28-813.01 with 18 U.S.C. § 2252(a)(4)(B) (2012).

[35] Reply brief for appellant at 6.

[36] Howard, *supra* note 4 at 1267.

however, Schuller did not "merely view" child pornography. Instead, he repeatedly searched for, downloaded, viewed, and then deleted child pornography. He did this intentionally and with the specific purpose to do so, and he used file-sharing software to achieve his ends. This constitutes knowing possession—not mere viewing.

Second, we agree that just because child pornography was downloaded onto a computer does not necessarily mean that there was knowing possession. Take, for example, a person who was legally browsing adult pornography online but mistakenly clicked on a link leading him to a child pornography Web site, which he immediately closed. The record shows that, in such a situation, child pornography would be downloaded to the computer's "cache" folder as temporary Internet files, through no further action by the user. In such a case, the person would not be guilty of knowingly possessing child pornography—he neither downloaded the files knowingly nor constructively possessed them, because there was no intent to control them. But again, as with Schuller's "mere viewing" argument, that is not what we have here. Schuller repeatedly searched for, downloaded, viewed, and then deleted child pornography files.

Third, as explained above, the record shows sufficient evidence to conclude that Schuller intended to control child pornography files. It is true that Donahue agreed that there was no evidence that Schuller "copied, saved, emailed, [or] put on a hard drive or disk" child pornography files. But we understand Donahue's testimony to be that, *outside of specifically downloading the child pornography files*, Schuller did not otherwise copy, save, e-mail, or put them on a hard drive or disk. To conclude otherwise, as Schuller implicitly suggests, would simply be wrong. By intentionally downloading the files through the file-sharing software, Schuller saved those files onto his hard drive; they were in fact located in the "Saved" folder. We understand that the file-sharing software, by default, designated that location for completed downloads (though an experienced user, as Schuller admittedly was, would likely know how to change that location). But regardless, Schuller knew that he was saving these files to his hard drive by downloading them

through the software. And he obviously knew where they were and how to access them, because he viewed them and later deleted them.

[10] We also do not agree that Schuller's deleting the files could indicate only "an intention to ***not*** take control over," and therefore not possess, the files.[37] In reviewing the sufficiency of the evidence, we give every reasonable inference to the State.[38] It seems reasonable to infer that Schuller deleted the files to hide evidence of his earlier knowing possession.[39] That being the case, a reasonable fact finder could infer a consciousness of guilt[40] and consider that as evidence that Schuller was in fact guilty of the crime charged, including the intent element.[41] As the Michigan Supreme Court observed, "a defendant cannot intentionally procure and subsequently dispose of a depiction of child sexually abusive material without having either actual or constructive possession."[42]

Finally, in his reply brief and at oral argument, Schuller argued that the partial dissent in *People v. Flick*[43] and the decision in *U.S. v. Flyer*[44] supported finding that Schuller did not "knowingly possess" child pornography. Because of Schuller's express and heavy reliance on these cases, we will address them explicitly. But we conclude that Schuller's reliance on these cases is misplaced.

In *Flick*, the partial dissent noted that for the defendants to have constructively possessed certain images, they had to have had not only the ability or power to exercise dominion or

---

[37] Brief for appellant at 17 (emphasis in original).

[38] See *Lamb, supra* note 17.

[39] See, *People v. Kent*, 79 A.D.3d 52, 910 N.Y.S.2d 78 (2010); *Crabtree v. Commonwealth*, No. 2011-CA-000452-MR, 2012 Ky. App. Unpub. LEXIS 1030 (Ky. App. Aug. 17, 2012) (unpublished opinion). See, also, *U.S. v. Upham*, 168 F.3d 532 (1st Cir. 1999).

[40] See *Kent, supra* note 39.

[41] See *State v. Draganescu*, 276 Neb. 448, 755 N.W.2d 57 (2008).

[42] *Flick, supra* note 30, 487 Mich. at 17, 790 N.W.2d at 304.

[43] *Flick, supra* note 30 (Cavanagh, J., concurring in part, and in part dissenting).

[44] *U.S. v. Flyer*, 633 F.3d 911 (9th Cir. 2011).

control, but also the intent to exercise that dominion or control. It argued that while the defendants could have "print[ed], resiz[ed], sav[ed], shar[ed], post[ed], e-mail[ed], or delet[ed]" the images, there was no evidence that they intended to do so and, therefore, there was no evidence of constructive possession.[45] Schuller emphasizes that, as with Michigan law, Nebraska requires both control and intent to exercise control to have constructive possession. And he argues that there was "no evidence, direct or circumstantial, to establish that [he] copied, saved, emailed, put on a hard drive or disk any of the files . . . or that he ever intend[ed] to do so."[46]

But as we explained above, that is not correct. The record shows that Schuller used file-sharing software to intentionally search for and download (and therefore save) child pornography files onto his hard drive. And the record also shows that he intentionally viewed and then deleted those files and that this was a repeated process. This is evidence of both his control and his intent to control. This is a far different situation from that in *Flick*. There, the partial dissent characterized the issue as whether the defendants had knowingly possessed child pornography by "intentionally accessing and viewing prohibited images on websites."[47] *Flick* did not involve, at least in the partial dissent's reading of the record, the intentional downloading of files; rather, the only downloaded files at issue were temporary Internet files that the defendants were apparently unaware of.[48] We find the partial dissent inapplicable here.

We conclude that Schuller's reliance on *Flyer* is also misplaced. There, the Ninth Circuit reversed a defendant's conviction for possession of child pornography. The particular files were located in the unallocated space of a computer; in other

---

[45] *Flick, supra* note 30, 487 Mich. at 33, 790 N.W.2d at 313 (Cavanagh, J., concurring in part, and in part dissenting).

[46] Reply brief for appellant at 6.

[47] *Flick, supra* note 30, 487 Mich. at 30, 790 N.W.2d at 312 (Cavanagh, J., concurring in part, and in part dissenting).

[48] See *Flick, supra* note 30.

words, they had been deleted. The Ninth Circuit noted that "[e]ven 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."[49] The court reasoned that because there was no evidence that the defendant knew of the files or that he could access them, there was no way that he could have exercised dominion or control over them. And in response to the government's argument that deletion equaled dominion and control, the Ninth Circuit reasoned:

> [D]eletion of an image alone does not support a conviction for knowing possession of child pornography on or about a certain date . . . . No evidence indicated that on or about April 13, 2004, [the defendant] could recover or view any of the charged images in unallocated space or that he even knew of their presence there.[50]

As such, the Ninth Circuit reversed the conviction.[51]

But as one federal district court noted,

> it is important to read with care the charge, the evidence, and the prosecution's concessions in *Flyer*. The case does not say that a defendant is not guilty of knowing possession of child pornography if the only identified images of child pornography are found in unallocated space or internet cache.[52]

It is important to note that the government charged the defendant in *Flyer* with possessing child pornography only "on or about April 13, 2004," the day that the government seized his desktop computer. The desktop computer (1) did not have file-sharing software (unlike his laptop) and (2) contained only deleted images. And, as explained above, the government

---

[49] *Flyer, supra* note 44, 633 F.3d at 918.

[50] *Id.* at 920.

[51] See *Flyer, supra* note 44.

[52] *United States v. Carpegna*, Nos. CR 07-13-H-DWM, CV 12-07-H-DWM, CR 08-14-M-DWM, CV 12-10-M-DWM, 2013 U.S. Dist. LEXIS 115002 at *10-11 (D. Mont. Aug. 14, 2013).

conceded there was no evidence that the defendant knew of those images, that he could access them, or that he had ever exercised dominion or control over them.[53]

In contrast, here the information does not focus on the day police seized the computer. As the State acknowledged at oral argument, had that been the case, it would have been exceedingly difficult (if not impossible) to prove knowing possession of the deleted files, because the evidence showed that Schuller could not access those files and likely did not even know they were there. But, it is important that the information alleges that Schuller knowingly possessed child pornography at various times from July 15 to September 30, 2011. Unlike *Flyer*, the allegations in this case did not rest solely on the knowing possession of the deleted images; rather, the deleted images were also evidence of Schuller's prior possession, i.e., when he searched for, downloaded, and viewed child pornography (and before he deleted it).[54] We also find *Flyer* inapplicable.

V. CONCLUSION

We conclude that the district court did not err in denying Schuller's motion to suppress. That dynamic IP addresses can change was immaterial to the probable cause determination in this case. We also conclude that the evidence was sufficient to support Schuller's conviction for knowingly possessing child pornography. We affirm.

AFFIRMED.

---

[53] See *Flyer, supra* note 44.

[54] See, *Haymond, supra* note 33; *McArthur, supra* note 33; *Romm, supra* note 33; *Upham, supra* note 39; *Kent, supra* note 39; *McKinney, supra* note 33; *Crabtree, supra* note 39.