ATTORNEY FOR APPELLANT

Victoria Bailey Casanova
Casanova Legal Services, LLC
Indianapolis, Indiana

ATTORNEYS FOR APPELLEE

Theodore E. Rokita
Attorney General of Indiana

Tyler Banks
Supervising Deputy Attorney General
Indianapolis, Indiana

IN THE COURT OF APPEALS OF INDIANA

William S. Sloan,
Appellant-Defendant,

v.

State of Indiana,
Appellee-Plaintiff.

December 29, 2023

Court of Appeals Case No.
22A-CR-2250

Appeal from the
Johnson Superior Court

The Honorable
Douglas B. Cummins, Judge

Trial Court Cause No.
41D03-1912-F1-22

Opinion by Senior Judge Robb
Chief Judge Altice and Judge Brown concur.

Robb, Senior Judge.

Case Summary and Issue

[1] William Sloan appeals his conviction of three counts of child molesting, challenging the admission of evidence seized from his home pursuant to a search warrant. Sloan contends the trial court erred by admitting the evidence because the probable cause affidavit supporting the warrant omitted a material fact and did not establish a sufficient nexus between him and the alleged criminal activity. We conclude the affidavit sufficiently established probable cause for the issuance of a search warrant for Sloan's residence, and we affirm.

Facts and Procedural History

[2] In 2019, Detective Brian Swisher of the Greenwood Police Department was assigned to the investigations division where he dealt with internet crimes against children. The detective used software on a computer in his office that allowed him to monitor downloads associated with child pornography. Through the use of this software, he discovered an IP address offering a file that appeared to contain child pornography. He downloaded and viewed the file to confirm his suspicion. The detective then determined that the IP address was registered to AT&T, that it was located in Greenwood, and that the account was in Sloan's name.

[3] Prior to Detective Swisher moving forward with his investigation, he was notified that another officer and a representative from the Department of Child Services were going to Sloan's residence to respond to an allegation of molestation against Sloan by his step-daughter. Concerned about the

destruction of evidence, the detective prepared and submitted a probable cause affidavit to obtain a search warrant for Sloan's residence. The warrant was issued, and the residence was searched. Evidence seized during the search included two videos of Sloan engaged in sexual activity with his step-daughter.

[4] The State charged Sloan with three counts of child molesting. At trial, the videos were admitted over Sloan's objection, and he now appeals the propriety of their admission.

Discussion and Decision

A. Technical Background

[5] Because cases involving technology often contain technical terms and because an understanding of the principles involved is vital to understanding the issue and arguments before the Court, we begin with an overview of such terms.

[6] The term "IP address" is short for Internet Protocol address, and it is a unique number assigned to every device that connects to the internet. *See* Internet Corporation for Assigned Names and Numbers, Beginner's Guide to Internet Protocol (IP) Addresses 4, 2 (2011) https://www.icann.org/resources/files/ip-addresses-beginners-guide-2011-03-04-en [https://perma.cc/FM65-D25M] (last visited December 15, 2023). When an individual purchases internet service from an internet service provider ("ISP"), the ISP assigns a unique IP address to the individual. Office of Legal Education, United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 65 (2009) https://www.justice.gov/criminal-

ccips/ccips-documents-and-reports [https://perma.cc/R7MD-N8UV] (last visited December 15, 2023); *see also* ICANN Guide at 4, 6, 11.

[7] This case also involves BitTorrent, a peer-to-peer ("P2P") file-sharing network. "P2P software is readily available on the internet and often free to download." Ex. Vol. p. 15, Defendant's Ex. F (PC Aff.). When P2P software is running on a device that is connected to the internet, the user can download digital files from and share files with other users on the same or compatible P2P networks. *Id.* On BitTorrent, users create a torrent file for the digital file they wish to share on the network. *Id.* Torrent files are small files that contain information about the available digital file and provide a method for downloading the digital file. *Id.* Each particular torrent file is associated with a unique identifier known as an "infohash." *Id.* The Supreme Court of Rhode Island explained these networks as:

> When a person uses these types of file-sharing services, it is akin to "leaving one's documents in a box marked 'free' on a busy city street." In order to use a peer-to-peer network, an individual must download software for the program. Peer-to-peer networks use hash values to verify the content of electronic files that are available for copying. Hash values—commonly referred to as "electronic fingerprints"—consist of "a string of numbers that, for all practical purposes, uniquely identifies a digital file" and will change any time a file is altered. Over time, law enforcement and other entities have identified and confirmed that certain hash values contain child pornography.

In re Austin B., 208 A.3d 1178, 1181 (R.I. 2019) (internal citations and footnote omitted).

B. Search Warrant Affidavit

[8] The probable cause affidavit in support of the search warrant alleged that:

- On July 1, 2019, Detective Swisher was conducting an investigation on the BitTorrent network looking for users sharing child pornography.
- The detective focused his investigation on a device using the IP address 99.9.229.7 because it was offering a torrent file that was identified by an infohash associated with child pornography.
- Using a computer that was running investigative BitTorrent software, the detective connected to the device at IP address 99.9.229.7 and downloaded directly from that device and IP address the file that was being offered and was named "boy girl sex 6yo.avi."
- Detective Swisher viewed the downloaded file and confirmed it contained child pornography.
- In October 2019, the detective used an online database that provides geolocation of IP addresses to determine that the IP address 99.9.229.7 was registered to ISP AT&T and was located in Greenwood.
- A subpoena was sent to AT&T for subscriber information for IP address 99.9.229.7 during the time period on July 1, 2019 in which the detective downloaded the file. AT&T responded that the IP address was at that time and date assigned to Sloan at an address in Greenwood. Through another online search, the detective confirmed Sloan's address.

C. Pre-Trial Motions

[9] Sloan requested a *Franks* hearing[1] for the purpose of determining the truthfulness of certain statements in Detective Swisher's affidavit, specifically

[1] In *Franks v. Delaware*, the United States Supreme Court held that a hearing is required when the defendant "makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit[.]" 438 U.S. 154, 155-56, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978). If the defendant proves the allegation by a preponderance of the evidence, the

the time of the download of the suspect file. *See* Appellant's App. Vol. II, pp. 197-99. Sloan also moved to suppress all the evidence seized from his home as a result of the search warrant. He listed five reasons the search was improper: (1) the application for the search warrant included false and misleading representations and/or omissions and stale information; (2) the warrant was overly broad; (3) the State failed to substantially comply with the statutory requirements to obtain a warrant electronically; (4) in executing the warrant, the officers exceeded its scope; and (5) in executing the warrant, the police unlawfully entered the home without properly knocking and announcing their presence. *See* Appellant's App. Vol. II, pp. 214-15. Following a hearing, the trial court denied Sloan's motions, and the evidence was admitted at trial over his objection.

D. Analysis

[10] Sloan argues that admission of the evidence was improper because the search warrant used to seize the evidence was not supported by probable cause. He asserts the warrant was invalid because it failed to inform the issuing court of the possibility that someone other than himself, on a device not belonging to him, could have used his Wi-Fi to connect to the internet and offer the file containing images of child pornography. Sloan further claims that, because of

---

search warrant must be voided where, "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause[.]" *Id.* at 156.

this possibility, any nexus between himself or a device at his residence and the criminal activity was insufficient to support a search warrant.

[11] We observe that Sloan framed the issues below differently from how he frames them on appeal. Consequently, whether he raised this issue to the trial court is subject to dispute.[2] Nevertheless, as the State does not raise a waiver argument, and because we prefer to resolve matters on their merits instead of on procedural grounds, *Littleton v. State*, 954 N.E.2d 1070, 1075 (Ind. Ct. App. 2011), we address the issue as presented.

[12] When a defendant challenges the propriety of a search following a completed trial, the issue is one of whether the trial court properly admitted the evidence. *Bulthuis v. State*, 17 N.E.3d 378, 382 (Ind. Ct. App. 2014), *trans. denied*. The trial court's ruling on the admission or exclusion of evidence is reviewed for abuse of discretion. *Cherry v. State*, 57 N.E.3d 867, 875 (Ind. Ct. App. 2016), *trans. denied*. An abuse of discretion occurs when a decision is clearly against the logic and effect of the facts and circumstances before the court. *Paul v. State*, 971 N.E.2d 172, 175 (Ind. Ct. App. 2012).

[13] Both the Fourth Amendment to the United States Constitution and article 1, section 11 of the Indiana Constitution require probable cause for a search warrant to issue. *Casady v. State*, 934 N.E.2d 1181, 1188 (Ind. Ct. App. 2010),

---

[2] In its order denying Sloan's motion for a *Franks* hearing and to suppress the evidence, the court refers to defense counsel's mention that an "unknown individual(s) may have 'piggy backed' off the IP address in question." Appellant's App. Vol. III, p. 5.

trans. denied. Probable cause is a fluid concept that is incapable of precise definition and that must be decided based on the facts of each case. *Id.* "In deciding whether to issue a search warrant, the issuing magistrate's task is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit, there is a fair probability that evidence of a crime will be found in a particular place." *Crabtree v. State*, 199 N.E.3d 410, 415 (Ind. Ct. App. 2022).

[14] In turn, the reviewing court's duty is to determine whether there was a substantial basis for the warrant-issuing judge to conclude that probable cause existed. *Casady*, 934 N.E.2d at 1189. Although the reviewing court applies a de novo standard of review, we give significant deference to the issuing judge's determination and focus on whether reasonable inferences drawn from the totality of the evidence support the finding of probable cause. *Crabtree*, 199 N.E.3d at 415. "In determining whether an affidavit provided probable cause for the issuance of a search warrant, doubtful cases are to be resolved in favor of upholding the warrant." *Id.* Likewise, we will not invalidate warrants by interpreting probable cause affidavits in a hypertechnical, rather than a commonsense, manner. *Rios v. State*, 762 N.E.2d 153, 161 (Ind. Ct. App. 2002).

1. Omission of Information

[15] On appeal, Sloan claims Detective Swisher erroneously omitted from his affidavit the material information that "he did not know whether the device from which the video was downloaded was inside [Sloan's] house, outside the house, or even on the property." Appellant's Br. p. 18. In other words, Sloan

asserts the detective should have informed the issuing court of the possibility that someone other than Sloan could have accessed his internet connection and made the child pornography file available for download. This appears to be the first occasion for this Court to address this specific issue.

[16] A probable cause affidavit must include all material facts, which includes facts that cast doubt on the existence of probable cause. *Ware v. State*, 859 N.E.2d 708, 718 (Ind. Ct. App. 2007), *trans. denied*. When the State has failed to include a material fact, we determine the validity of the warrant by considering collectively the omitted information and the information contained in the affidavit. *Id.*

[17] For a warrant to be invalid due to omission of information from an affidavit, the defendant must establish (1) that the affiant engaged in deliberate falsehood or reckless disregard for the truth in omitting the information and (2) that probable cause would no longer exist if the omitted information were considered by the issuing judge. *Darring v. State*, 101 N.E.3d 263, 268 (Ind. Ct. App. 2018). This rule "protects only against omissions that are 'designed to mislead, or that are made in reckless disregard of whether they would mislead,'" the issuing judge. *Keeylen v. State*, 14 N.E.3d 865, 877 (Ind. Ct. App. 2014) (citation and quotation marks omitted) (quoting *U.S. v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990)), *clarified on reh'g*, 21 N.E.3d 840, *trans. denied*.

[18] Here, Sloan makes no attempt to establish that Detective Swisher engaged in a deliberate falsehood or a reckless disregard for the truth when he failed to

include the information in his affidavit. Further, we cannot agree with Sloan's suggestion that the possibility that some unidentified individual was conceivably able to access his internet connection and offer the download is a "material fact" that is crucial to the determination of probable cause. This notion is sheer speculation that lacks any factual underpinning.

[19] We are not alone in our assessment of this theory; other courts have also considered and rejected this argument. Most notably, in *People v. Hayon*, 62 N.Y.S.3d 754, 760 (N.Y. Sup. Ct. 2017), the defendant was charged with 94 counts of possession of a sexual performance by a child. The authorities executed three search warrants and seized computers and other devices containing child pornography from both the defendant's home and office. He moved to suppress the evidence, claiming the warrant application was deficient "because it failed to explain to the court the 'realistic possibility' that someone other than defendant, such as a 'neighbor, a visitor or someone outside the premises' could have used defendant's *unsecured* IP address . . . ."[3] *Id.* (emphasis added). Classifying this argument as "extremely weak," the court stated:

> His argument rests on the idea that because anything is possible, the warrant court must exclude every alternative theory to a

[3] An internet subscriber's unsecured or non-password protected internet connection allows a person in the vicinity of the home—standing on the sidewalk in front of the house, for example—to access and use the subscriber's internet connection without a password and while under the disguise of the subscriber's IP address. *See Milan v. Bolin*, 795 F.3d 726, 727 (7th Cir. 2015) (explaining meaning of unsecured Wi-Fi network).

> certainty, a view that is inconsistent with the meaning of probable cause. In an often-quoted description of probable cause, the United States Supreme Court bluntly stated, "[i]n dealing with probable cause, however, as the very name implies, we deal with probabilities" (*Brinegar v. United States*, 338 U.S. 160, 175, 69 S. Ct. 1302, 93 L. Ed. 1879 [1949]). "The affidavit need not contain information providing certainty that the objects sought will be found in the search . . . but rather whether the facts and circumstances taken as whole gave the magistrate probable cause to believe that the desired items would be found in the search" (*United States v. Brinklow*, 560 F.2d 1003, 1006 [10th Cir. 1977], *cert. denied* 434 U.S. 1047, 98 S. Ct. 893, 54 L. Ed. 2d 798 [1978]).

Id.; *see also U.S. v. Featherly*, 846 F.3d 237 (7th Cir. 2017) (defendant challenged affidavit by claiming it contained deliberate falsehood that kept issuing judge from considering possibility that someone else in trailer park had connected to his modem without his knowledge and used his internet connection to share child pornography; court noted that while unknown user conceivably could connect to another's modem through unsecured wireless network, record did not reflect that defendant had such a network and held that connection between IP address and modem at internet subscriber's residence was sufficient to justify search).

[20] Likewise, the record here does not reflect whether Sloan's internet connection was unsecured but given the facts and determination in both *Hayon* and *Featherly*, it is of no moment. The affidavit did not need to exclude every hypothesis of Sloan's innocence to establish sufficient probable cause for the warrant; rather, it needed to demonstrate to the issuing judge that, given all the

circumstances, there was a fair probability that evidence of a crime would be found in a particular place. *Crabtree*, 199 N.E.3d at 415. Sloan has failed to establish the detective omitted any material fact that would have left probable cause in doubt.

2. Nexus

[21] Indiana Code section 35-33-5-2 incorporates the principles of protection against unreasonable searches and seizures and details the information to be included in a search warrant affidavit. The statute provides in relevant part:

> [N]o warrant for search or arrest shall be issued until there is filed with the judge an affidavit:
>
> (1) particularly describing:
>
> (A) the house or place to be searched and the things to be searched for; or
>
> (B) particularly describing the person to be arrested;
>
> (2) alleging substantially the offense in relation thereto and that the affiant believes and has good cause to believe that:
>
> (A) the things sought are concealed there; or
>
> (B) the person to be arrested committed the offense; and
>
> (3) setting forth the facts known to the affiant through personal knowledge or based on hearsay, constituting the probable cause.

Ind. Code § 35-33-5-2(a) (2014). Accordingly, "a probable cause affidavit is required to establish a logical connection, or nexus, between the suspect and the

location to be searched." *Rader v. State*, 932 N.E.2d 755, 759 (Ind. Ct. App. 2010), *trans. denied*.

[22] Sloan acknowledges that Detective Swisher's affidavit established a nexus between the downloaded file and his IP address and between his IP address and his residential address. Appellant's Br. p. 18. However, based on the chance that someone else accessed his internet connection to make the file available, he asserts the affidavit failed to establish a nexus between the file and any person or device at his address. *Id.* at 18-19. We thus restate the question posed here as whether identification of a specific IP address that is being used to make child pornography available and the physical address to which the IP address is linked creates a sufficient nexus to support a search warrant for that physical address, despite the possibility that an individual other than the subscriber may have been using the IP address. As with Sloan's related first argument, this Court has not yet addressed this precise question. However, several federal and state courts have had occasion to do so and have rejected it.

[23] In *United States v. Perez*, 484 F.3d 735 (5th Cir. 2007), the defendant was convicted of transmitting child pornography by means of a particular IP address that was assigned to him at his home address. On appeal, the defendant contended that the association of an IP address with a physical address does not give rise to probable cause to search that address. He argued that if he used an unsecured wireless connection, neighbors would have been able to easily use his internet access to make the transmissions of child pornography. The affidavit supporting the search warrant included the IP address, the fact that the IP

address was assigned to Perez, and Perez's specific physical address. The court determined that it was clear there was a substantial basis to conclude that evidence of criminal activity would be found at Perez's physical address and reasoned that, while "it was *possible* that the transmissions originated outside of the residence to which the IP address was assigned, it remained *likely* that the source of the transmissions was inside that residence." *Id.* at 740 (emphasis added). *See also U.S. v. Vosburgh*, 602 F.3d 512 (3rd Cir. 2010) (agreeing with reasoning in *Perez* and holding that evidence that computer with particular IP address possessed or transmitted child pornography can support search warrant for physical premises linked to that IP address).

[24] More recently, in *Commonwealth v. Martinez*, 71 N.E.3d 105 (Mass. 2017), the defendant appealed from his conviction of possessing child pornography. Martinez challenged the affidavit supporting a search warrant, claiming the police needed to do more to link him to the place to be searched and the items to be seized before a valid warrant could issue. He argued the authorities did not determine whether the internet connection at the apartment used a wireless router, and, if so, whether the wireless network required a password. As a result, it was possible that "someone other than the subscriber, located at a different physical address, was 'joyriding' on an unsecured wireless network based out of the apartment." *Id.* at 113.

[25] In its decision, the court included a helpful explanation of the evolution of the internet as it relates to the ability to link an individual to internet activity:

> In the early days of the Internet, when a residential Internet subscriber went online using only a home computer connected to a hard-wired Internet connection, there was a very strong correlation between an IP address assigned to a subscriber and a particular computer. Now, however, many subscribers use a wireless Internet router, which allows multiple devices within the range of the router to connect to the Internet simultaneously. To the outside world, all of these devices will share a single public IP address—the one that the ISP has assigned to its subscriber. . . . As a result, the correlation between an Internet subscriber's assigned IP address and any one particular Internet-enabled device may often be weaker than it once was. However, the correlation between an IP address and a physical address can still be strong, at least when the ISP has verified its assignment of a particular IP address to a subscriber at a specific physical address at a specific point in time.

Id. at 107-08 (internal citations omitted).

[26] The court acknowledged that, from a "technological standpoint," if an internet subscriber sets up an unsecured wireless internet network, a computer outside of the physical address could access the internet and share child pornography using the subscriber's IP address. *Id.* at 114. Nevertheless, the court found Martinez's argument missed the mark, explaining:

> A showing of probable cause to search a place (as opposed to arrest a person) need not identify a specific criminal suspect—although frequently it does. Indeed, the critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific things to be searched for and seized are located on the property to which entry is sought. In other words, police need only demonstrate a sufficient nexus between the criminal activity under investigation, the items sought, and a place to be

> searched where the items may reasonably be expected to be located—independent of whether they have identified a specific criminal suspect. Certainly police may have an easier time demonstrating a sufficient nexus if they can link a specific suspect (e.g., the named Internet account holder) to the criminal activity. However, such a link is not always required.

Id. at 113-14 (internal citations and quotation marks omitted). The court also clarified that probable cause does not require a showing of certainty that evidence of criminal activity will be found at a particular location nor does it require a showing that any and all possibilities of finding the evidence elsewhere have been excluded. *Id.* at 115 (quoting *Commonwealth v. Anthony*, 883 N.E.2d 918, 926 (Mass. 2008)).

[27] The affidavit in *Martinez* included an IP address that was used to share child pornography and the subscriber's name and residential address to which the IP address was assigned at the time in question. The court thus concluded that "[t]he temporal and geographical links between the target IP address and the physical address to be searched provided a substantial basis" for concluding that evidence connected to the suspected crime "likely would be found at the specified premises" and "therefore gave rise to a sufficient nexus between the suspected criminal activity and the residence." *Id.* at 111. *See also In re Austin B.*, 208 A.3d 1178 (finding search warrant valid where warrant application contained IP address that was being used to share images of child pornography, physical address linked to IP address, and subscriber's name, even though it was later learned subscriber no longer lived there); *Commonwealth v. Green*, 204

A.3d 469, 475 (Pa. Super. Ct. 2019) (rejecting defendant's argument that possibility that another person could have used his IP address precluded finding of probable cause for search warrant and finding sufficient affidavit containing information that child pornography had been downloaded by device using IP address associated with defendant's residence), *aff'd by* 265 A.3d 541 (Pa. 2021).

[28] Similar rulings have been reached in *State v. Aston*, 125 So. 3d 1148 (La. Ct. App. 2013) (concluding search warrant was based on probable cause where supporting affidavit contained IP address of device that had shared images of child pornography, as well as name and physical address to which IP address was assigned), *writ denied by* 135 So. 3d 618 (La. 2014); *State v. Aguilar*, 437 S.W.3d 889 (Tenn. Crim. App. 2013) (rejecting defendant's claim that supporting affidavit failed to establish nexus between child pornography files on computer and his residence and concluding that affidavit containing IP address of computer and subscriber name and address linked to IP address was sufficient to establish probable cause for warrant to search defendant's residence); *Barrett v. State*, 367 S.W.3d 919 (Tex. Ct. App. 2012) (holding affidavit sufficient to support probable cause for search warrant for evidence of child pornography at particular address where affidavit provided IP address and subscriber's name and address associated with specific IP address).

[29] Here, the probable cause affidavit in support of the search warrant submitted to the court was thoroughly detailed and provided ample evidence to conclude that probable cause existed for the issuance of the warrant to search Sloan's residence. In his affidavit, Detective Swisher explained peer-to-peer sharing

networks generally and BitTorrent specifically, including the process for searching and downloading files on the network. He conveyed his knowledge, acquired through training and experience, of the dissemination, collection, and storage of child pornography and the behaviors of individuals involved in such acts. He further expressed his understanding of the role of forensic experts to sort and obtain information from a computer system, including concealed information. The detective provided background information on mobile devices and related terminology, as well as information on the process of acquiring data from these devices.

[30] In addition, Detective Swisher specifically averred that a device using the IP address 99.9.229.7 was on the BitTorrent network offering a file that was identified by an infohash associated with child pornography. The detective connected to the device at IP address 99.9.229.7 and downloaded directly from that device and IP address the file that was being offered and was named "boy girl sex 6yo.avi." He then viewed the downloaded file and confirmed it contained child pornography. The detective used an online database to determine that the IP address 99.9.229.7 was registered to ISP AT&T and was located in Greenwood. Information obtained from AT&T showed that the IP address was, at the time and date in question, assigned to Sloan at his address in Greenwood. The detective confirmed Sloan's address through another online search.

[31] The fundamental question is whether there was a substantial basis from which the warrant-issuing judge could conclude there was a fair probability that

evidence of the crime of child pornography would be found in Sloan's residence. We emphasize here that probable cause deals with probabilities, not certainties. *See Keeylen*, 14 N.E.3d at 871 ("'Probable cause is only a probability or substantial chance of criminal activity, not a certainty that a crime was committed.'") (quoting *Suarez v. Town of Ogden Dunes, Ind.*, 581 F.3d 591, 596 (7th Cir. 2009)). Despite the possibility that an individual other than Sloan may have used the account, the circumstances here establish a fair probability that Sloan, the subscriber, committed this act and that evidence of the illegal activity would be found in his home. We therefore hold that facts establishing illegal internet activity associated with a particular IP address and assignment of the IP address at the time in question to a particular internet subscriber at a specific physical address provide a nexus between the illegal activity and the physical address sufficient to establish probable cause for a warrant to search the residence at the physical address.

Conclusion

[32] The trial court did not err by admitting the evidence seized from Sloan's residence pursuant to the search warrant because the affidavit supporting the warrant sufficiently established probable cause for its issuance.

[33] Affirmed.

Altice, C.J., and Brown, J., concur.