IN THE

ARIZONA COURT OF APPEALS

DIVISION TWO

THE STATE OF ARIZONA,
Appellee,

v.

SHANNON PAUL ZUCK,
Appellant.

No. 2 CA-CR 2019-0130
Filed May 25, 2021

THIS DECISION DOES NOT CREATE LEGAL PRECEDENT AND
MAY NOT BE CITED EXCEPT AS AUTHORIZED BY APPLICABLE RULES.
NOT FOR PUBLICATION
See Ariz. R. Sup. Ct. 111(c)(1); Ariz. R. Crim. P. 31.19(e).

Appeal from the Superior Court in Pima County
No. CR20135415001
The Honorable Javier Chon-Lopez, Judge
The Honorable Michael Butler, Judge

AFFIRMED

COUNSEL

Mark Brnovich, Arizona Attorney General
By Linley Wilson, Deputy Solicitor General/Section Chief of Criminal Appeals, Phoenix
Counsel for Appellee

James Fullin, Pima County Legal Defender
By Robb P. Holmes, Assistant Legal Defender, Tucson
Counsel for Appellant

MEMORANDUM DECISION

Vice Chief Judge Staring authored the decision of the Court, in which Presiding Judge Espinosa and Judge Eckerstrom concurred.

S T A R I N G, Vice Chief Judge:

¶1 Shannon Zuck appeals from his convictions and sentences for sexual exploitation of a minor under fifteen, challenging the trial court's denial of his motions to suppress evidence gained through disclosure of identifying information by an internet service provider and an ensuing search warrant, and a jury instruction permitting the jury to infer the minority of the exploited children. For the following reasons, we affirm.

Factual and Procedural Background

¶2 We view the facts in the light most favorable to sustaining the jury's verdicts and resolve all reasonable inferences against Zuck. *See State v. Felix*, 237 Ariz. 280, ¶ 30 (App. 2015). In September 2013, a Tucson police detective was monitoring a law-enforcement computer application named Roundup,[1] and found that a child pornography file "had been downloaded from a specific IP address" over a peer-to-peer network. Having verified that the file portrayed child pornography, police officers obtained subpoenas for Cox Communications, seeking the subscriber information related to the IP address, which included the subscriber's home address.[2] Cox complied, informing police that the IP address was assigned to J.P., who was Zuck's mother.

¶3 The officers surveilled the subscriber's home to ensure any wireless network was secured, that is that the computer associated with the

[1] Testimony at trial established the Roundup software, in simple terms, functions by "quer[ying] all of the computers" on a peer-to-peer network, that is, computers in direct communication with each other over the internet, for child pornography, flagging suspect IP addresses, and then "go[ing] to those computers with those IP addresses . . . [and] tr[ying] to make a connection" in order to download the illicit media.

[2] The subpoena specifically requested "subscriber information to include name, address and phone numbers related to the user of the[]" obtained IP address.

illicit file was at that address. Once they had concluded there was no unsecured network, the officers applied for and were granted a warrant to search the residence for devices able to store child pornography, other related devices, and evidence of who resided at the home.

¶4 At the residence, the officers found a laptop and a thumb drive. Zuck admitted he had used the laptop and provided storage locations of the illicit files, along with passwords necessary to access them. Zuck also admitted he had been "downloading child pornography for . . . two years." Police ultimately confirmed child pornography was stored on the thumb drive, and had been stored and viewed on the laptop.

¶5 Zuck was initially charged with ten counts of sexual exploitation of a minor under fifteen, but was convicted of six. For each count, he was sentenced to a consecutive term of twenty-five years of imprisonment, totaling 150 years. This appeal followed. We have jurisdiction pursuant to article VI, § 9 of the Arizona Constitution and A.R.S. §§ 12-120.21(A)(1), 13-4031, and 13-4033(A)(1).

Discussion

¶6 Zuck claims the trial court erred in denying his motions to suppress because the search warrant for his residence was "based on an affidavit . . . containing misleading, inaccurate[, stale,] and illegally-obtained information" and was not supported by probable cause, and a grand jury subpoena was unlawfully used to obtain the internet subscriber information related to his residence. He also argues the court erred by denying a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), "fail[ing] to find that a person in Arizona has a constitutionally-protected reasonable expectation of privacy-by-anonymity to connect to the internet in the home through an anonymous public IP address," and instructing the jury that it was entitled to infer that the illicit images and videos at issue depicted actual minors. We address Zuck's arguments in the order he presents them.

Jury Instructions

¶7 Zuck first argues the trial court erred in instructing the jury it was entitled to "draw the inference that a participant was a minor if the visual depiction or live act through its title, text or visual representation depicted the participant as a minor," pursuant to A.R.S. § 13-3556. We conclude that, even assuming the court erred in giving the instruction, any such error would have been harmless.

¶8 Section 13-3556 provides that "[i]n a prosecution relating to the sexual exploitation of children, the trier of fact may draw the inference that a participant is a minor if the visual depiction or live act through its title, text or visual representation depicts the participant as a minor." In *State v. Hazlett*, 205 Ariz. 523, n.10 (App. 2003), another department of this court concluded § 13-3556 "permit[s] a prosecution and conviction where no actual child was involved in the material or live act." And, in the same footnote, *Hazlett* "holds" that § 13-3556 "falls afoul" of the Supreme Court's decision in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 257-58 (2002), which concluded a similar federal statute was an overbroad regulation of speech violating the First Amendment. 205 Ariz. 523, ¶ 6 & n.10.

¶9 At trial, citing *Hazlett*, Zuck requested the jury be instructed that it was not permitted to merely infer that the images and videos at issue portrayed actual minors. The trial court ultimately denied this request, and instructed the jury, nearly verbatim, with the language of § 13-3556. It reasoned that, despite *Hazlett*, the legislature had not repealed that section, and whether it should be the basis for a jury instruction "is for people other than me to determine."[3]

¶10 On appeal, Zuck contends § 13-3556 is unconstitutional and the trial court erred in giving an instruction based on it. He further claims that because of the instruction, the jury was allowed "to find the 'victim' element [of sexual exploitation of a minor] without evidence," meriting reversal. The state responds that any error resulting from the instruction was harmless. Specifically, it points to other instructions, a juror's question, and statements made in closing arguments to support its claim that the jurors understood the images and videos at issue portrayed actual minors. In short, the state contends the evidence presented clearly proved the images and videos depicted actual minors.

¶11 We review a statute's constitutionality de novo. *See State v. Arevalo*, 249 Ariz. 370, ¶ 9 (2020). "An act of the legislature is presumed constitutional, and where there is a reasonable, even though debatable, basis for enactment of the statute, the act will be upheld unless it is clearly unconstitutional." *Id.* ¶ 9 (quoting *State v. Ramos*, 133 Ariz. 4, 6 (1982)). Thus, if possible, we interpret a statute in favor of its constitutionality. *See*

[3]We disagree with the trial court to the extent it based its reasoning on whether the legislature had repealed § 13-3556. If the court concluded *Hazlett* was precedent, it was not free to disregard it. *See State v. Patterson*, 222 Ariz. 574, ¶ 20 (App. 2009).

id. And, a party asserting that a statute is unconstitutional must overcome "a strong presumption in favor of a statute's constitutionality." *Id.*

¶12 In this instance, however, we need not address the constitutionality of § 13-3556.[4] Even assuming the trial court erred by giving the instruction, the error was harmless in light of the strength of the evidence that each image depicted an actual minor.[5] Notably, while testifying about the software and procedures used to track the initial illicit image to Zuck's computer, one of the detectives—who had been involved in "upwards of 500" child pornography investigations—explained he had been "told to review the image[s] to make sure that [they] . . . depict[ed] a minor that is illegal" in the given jurisdiction. Another detective—the lead detective on the case—testified he had reviewed "the file to confirm that it actually was child pornography that had been downloaded." Further, after being instructed on the state's burden of proving that each image and video portrayed an "actual child under the age of fifteen years," the jury was presented with and able to inspect each illicit image and video for itself. And, in response to viewing one of the videos, a jury question was submitted asking one of the investigating officers, a digital forensic examiner assigned to the crime laboratory, with extensive experience in child pornography investigations, to "explain how [he] knew the female was less than fifteen years old." The officer explained the criteria detectives employ in determining whether an image shows a girl younger than fifteen, including analysis of hip development, vaginal-area development, pubic hair and breast development.

¶13 Additionally, Zuck plainly admitted to police that he had been downloading child pornography for two years, focusing on material involving girls between eight and twelve years old. Given Zuck's experience and specified preference, reasonable jurors could consider his statements to be relevant in determining whether actual minors were depicted. *See* Ariz. R. Evid. 401(a) (evidence relevant if "it has any tendency

---

[4]Neither need we address whether *Hazlett* is precedent concerning the constitutionality of § 13-3556.

[5]Because Zuck objected to the instruction below, we review for harmless error. *See State v. Henderson*, 210 Ariz. 561, ¶ 18 (2005); *State v. Dann*, 205 Ariz. 557, ¶ 18 (2003). "Harmless error review places the burden on the state to prove beyond a reasonable doubt that the error did not contribute to or affect the verdict or sentence." *Henderson*, 210 Ariz. 561, ¶ 18.

to make a fact more or less probable than it would be without the evidence").

¶14 Thus, even assuming the jury was improperly allowed to infer that the images portrayed actual minors, no reasonable jury would have been able to conclude the media at issue did not portray actual minors. *Cf. Dann*, 205 Ariz. 557, ¶ 18 (when jury instructions omit element of crime, error is harmless if no rational jury could find that omitted element was not proven). Therefore, the state has met its burden and demonstrated that any error would not have contributed to the verdict.

First Motion to Suppress

¶15 Zuck also argues the trial court erred in denying his first motion to suppress evidence, claiming the state unlawfully used grand jury subpoenas to obtain information from the internet service provider. He further claims the court erred by not recognizing constitutional privacy interests in the internet subscriber information, requiring a warrant for its retrieval. We review a denial of a motion to suppress for an abuse of discretion, but review accompanying constitutional and purely legal issues de novo. *See State v. Blakely*, 226 Ariz. 25, ¶ 5 (App. 2010). To that end, "we consider only the evidence presented at the suppression hearing and view it in the light most favorable to upholding the court's ruling." *Id.* (citation omitted). However, in this instance, the parties presented only oral arguments at the hearing. Nonetheless, the material facts appear to be undisputed, and we view them in the light most favorable to upholding the ruling. *Cf. State v. Navarro*, 241 Ariz. 19, n.1 (App. 2016) (considering undisputed facts to decide suppression motion where no hearing held).

Grand Jury Subpoena Procedure

¶16 Below, Zuck argued the internet subscriber information in this case had been secured through an "*ultra vires* simulated legal process," *see generally* A.R.S. § 13-2814(A) ("A person commits simulating legal process if such person knowingly sends or delivers to another any document falsely purporting to be an order or other document that simulates civil or criminal process."), violating his due process rights, GA. CODE ANN. 16-9-109(b) (2018), A.R.S. § 13-4071, "Title 13, Article 23 [of the] Uniform Act to Secure the Attendance of Witnesses, A.R.S. §§ 13-4091 through 4096 . . . [and] 18 U.S. Code § 2703." Zuck's argument centered on his contention that police officers had "used [an] illegal simulated 'grand jury' process in secret and without judicial or grand jury oversight." Given

this, Zuck urged the trial court to suppress his subscriber information "as well as all 'fruits' of such unlawfully acquired evidence."[6]

¶17 The trial court consolidated Zuck's case with several others involving motions to suppress "based on the alleged illegality of grand jury subpoenas duces tecum used to obtain evidence . . . ." Although the court concluded the state had violated § 13-4071(C)'s requirement that it notify the grand jury foreperson or presiding judge of the subpoena's issuance, it nonetheless determined that, in the absence of the statute expressly providing for suppression as a remedy for violation, suppression was a discretionary remedy that may "be chosen by a trial court as a sanction in a given case." The court also ruled that, to the extent Zuck and the other defendants argued that the grand jury subpoenas were otherwise problematic, they nonetheless lacked standing because the "subpoenas did not seek any evidence from Defendants or any evidence in which Defendants had a right to privacy that society recognizes." Ultimately, the court denied Zuck's motion to suppress.[7]

¶18 On appeal, Zuck renews his argument that the state's use of the grand jury subpoenas in this case exceeded the authority prescribed by § 13-4071(C). Thus, he claims he "was deprived of the opportunity to seek timely judicial intervention by motion to quash the subpoena as an unlawful de facto police subpoena." And, Zuck again argues the state's use of the subpoenas on out-of-state witnesses "d[id] not comply with Arizona's out-of-state witness statute." He further emphasizes the state failed to "keep a log of 'returns' of evidence" associated with the subpoenas.

¶19 Zuck also argues his subscriber information was protected under 18 U.S.C. §§ 2701–2712 and 47 U.S.C. § 551, claiming these "statutes preempt any state statutes and set forth minimum procedural [and constitutional] requirements for state and federal orders authorizing compelled discovery of the communications." Thus, he claims police obtained "legally-protected personal information under false pretenses," violating several federal and state statutes and requiring preclusion under

---

[6]Zuck brought attention to 47 U.S.C. § 551 in his reply to the state's response to his motion to suppress, and argued for application of A.R.S. § 44-1376.01(C) at the suppression hearing.

[7] Zuck also sought special-action review of this ruling, but we declined jurisdiction, and our supreme court denied Zuck's petition for review of that decision.

A.R.S. § 44-1376.01(C). Finally, Zuck urges that "the court erred by finding that the county attorney merely made a mistake and that making a mistake does not make the 'grand jury subpoenas' in question ultra vires and void."

¶20 The state primarily responds that "Zuck lacks standing to challenge the obtaining of his mother's subscriber information" on any ground because the information at issue belonged solely to J.P. And, in any event, the state asserts that "Arizona law does not support suppression of evidence for purely statutory violations, which is what occurred in this case." The state also argues any violations of the statute that occurred in the process of obtaining the grand jury subpoena were "technical violation[s]," allowing the good-faith exception under A.R.S. § 13-3925 to apply. Lastly, the state asserts that it complied with the plain language of § 13-4071(C), and that Zuck and J.P. lack standing to assert it failed to comply with the out-of-state witness statutes.

¶21 We conclude the trial court did not err in denying Zuck's motion to suppress based on the state's noncompliance with § 13-4071(C) or the Uniform Act to Secure the Attendance of Witnesses from Without a State in Criminal Proceedings, A.R.S. §§ 13-4091 through 4096. None of these provisions includes suppression or exclusion of evidence as a remedy. *See United States v. Forrester*, 512 F.3d 500, 512 (9th Cir. 2008) (suppression is a "disfavored remedy" only imposed outside the constitutional context "where it is clearly contemplated by the relevant statute"). And, to the extent Zuck relies on § 44-1376.01(C), subsection (A) nonetheless exempts "any action by a law enforcement agency or any officer, employee or agent of a law enforcement agency . . . in connection with the performance of the official duties of the agency."

¶22 Further, Zuck has not persuaded us the trial court erred in connection with his arguments related to 18 U.S.C. §§ 2701–2712, also known as the Stored Communications Act (SCA), 47 U.S.C. § 551, and the other federal laws Zuck briefly refers to on appeal. Essentially, he contends that the subscriber information at issue was "protected" under these statutes, and, without explanation, that the state violated the SCA's provisions, which, along with the other federal statutes he refers to, serve as a "floor, not a ceiling, to what States must do." He also asserts the state illegally obtained "protected personal information under false pretenses," citing 15 U.S.C. § 6821(a) and 18 U.S.C. § 1039(a), (g) without further elaboration.

¶23 Notably, however, Zuck does not explain how the trial court erred in declining to suppress his subscriber information based on these statutes, or why the statutes required suppression in this case. Rather,

without referring to these federal laws, he points to inapposite cases involving disclosure of witnesses and testimony, and violation of a court order. *See State v. Naranjo*, 234 Ariz. 233, ¶¶ 31–34 (2014); *State v. Fredrick*, 129 Ariz. 269, 272 (App. 1981). On these grounds, too, we find no error in the court's denial of Zuck's first motion to suppress.

Constitutional Protection of Subscriber Information

¶24 The Fourth Amendment of the United States Constitution and the Arizona Constitution's Private Affairs Clause "protect against unlawful searches and seizures," and absent an exception, require a warrant for such state action. *State v. Peoples*, 240 Ariz. 244, ¶¶ 8-9 (2016); *see* Ariz. Const. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."). These provisions confer personal rights reserved for those with a "legitimate expectation of privacy in the invaded place." *Peoples*, 240 Ariz. 244, ¶¶ 8-9 (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)).

¶25 Zuck argued in the trial court that "[t]here is a reasonable expectation of privacy in 'personal identifying information' . . . held in trust by Cox Communications." He urged that this expectation arose from his "private constitutionally protected internet activ[ity] in [his] home," which was "protected by the anonymity of the anonymous Public IP Address." Thus, he asserted, the grand jury subpoena had effected "an unconstitutional search and compelled seizure that triggered the protection of the Fourth Amendment and the privacy rights under the Arizona and Georgia constitutions," requiring suppression. Relying on the fact that Zuck and the other defendants had "voluntarily turned over their subscriber information to a third party," the trial court concluded that any expectation of privacy in the subscriber information was unreasonable.

¶26 On appeal, Zuck claims that, under the Fourth Amendment and, specifically, *Carpenter v. United States*, ___ U.S. ___, 138 S. Ct. 2206 (2018), he had a reasonable expectation of privacy in the internet subscriber information used to obtain his home address. He also urges us to follow our previous opinion, in which a majority of this court concluded that similar subscriber information was protected under the Private Affairs Clause. *See State v. Mixton*, 247 Ariz. 212, ¶¶ 3, 27 (App. 2019). Zuck further claims he was "entitled to rely on the ISP's contractual obligation to guarantee confidentiality of their customer subscriber information . . . [and] statutory and criminal laws . . . that protect . . . private and confidential communication services records," as well as "Arizona Supreme Court rulings that guarantee First Amendment and privacy rights to anonymously access information." He also contends that warrantless

access to subscriber information "would destroy First Amendment rights to anonymity." Lastly, Zuck argues that unlike in *Mixton*, the good-faith exception should not apply here. *Id.* ¶ 39.

¶27 While this appeal was pending, our supreme court vacated this court's decision in *Mixton*. *See State v. Mixton*, 250 Ariz. 282, ¶ 77 (2021). The court concluded the internet subscriber information at issue was subject to the third-party doctrine and was thus unprotected under the Fourth Amendment, and was not a "private affair" protected by the Private Affairs Clause. *See id.* ¶¶ 20-21, 49. Here, as in *Mixton*, law enforcement obtained a suspect's IP address and using this information, obtained the location of the suspect's computer, which led to a search warrant and discovery of illicit material. *See id.* ¶¶ 5-6. In light of our supreme court's decision in *Mixton*, Zuck's arguments fail.[8]

¶28 Our supreme court made clear that the subscriber information at issue enjoys no Fourth Amendment protection, even in light of *Carpenter*.[9] *Id.* ¶ 26. And, although Zuck claims case law protecting anonymous speech and laws protecting communication service records fostered a reasonable expectation of privacy in the subscriber information, the supreme court determined in *Mixton* that, for Fourth Amendment purposes, any such expectation is unreasonable in light of the fact that the information was being transferred to third parties, that is, the internet service providers. *See id.* ¶¶ 14, 20-21. Similarly, this argument fails on state constitutional grounds, given the court's conclusion that the subscriber information is not a "private affair." *See id.* ¶ 51 ("IP address and subscriber information are not 'private affairs' . . . because the nature of th[is] information is inconsistent with privacy").

¶29 Zuck's argument regarding his expectation of privacy based on his ISP's "contractual obligations" is similarly unpersuasive. Supporting this contention, Zuck quotes Cox's "Notice to Cox Customers," which appears to ensure that his "personal information" would only be used to provide services offered by Cox or its partners, and would not be

[8] Given that the subscriber information is not constitutionally protected, we need not address whether Zuck had standing to assert such protection. Likewise, we need not address the application of any good-faith exception to the exclusionary rule.

[9] The state asserts that Zuck failed to develop his Fourth Amendment argument and thereby waived it. *See generally* Ariz. R. Crim. P. 31.10(a)(7)(A); *State v. Bolton*, 182 Ariz. 290, 298 (1995). Because Zuck elaborated on *Carpenter* and how it should apply to this case, we disagree.

disclosed "to others outside of Cox, [its] affiliates, vendors and business partners" without the customer's consent. This argument does not survive in light of our supreme court's treatment of the federal and state constitutional issues in *Mixton*. *See id.* ¶¶ 17-18, 51 (subscriber information is unprotected non-content information). Moreover, Zuck fails to offer authority to support the proposition that a private company may implicitly contract to resist lawful requests for information from law enforcement.[10]

¶30 Finally, in *Mixton*, our supreme court directly addressed the contention that leaving internet subscriber information unprotected would imperil rights to participate in anonymous speech. *See id.* ¶ 67. The court concluded that because Mixton had "conveyed data files to others using his actual IP address" through a messaging application, his actions were "analogous to his mailing a letter under a pseudonym but scrawling his actual return address on the outside of the envelope," and therefore did not implicate anonymous speech. *Id.* ¶¶ 4, 69. As we previously stated, police officers obtained Zuck's IP address from an illicit image that was downloaded from his computer through a file-sharing network. Thus, we also conclude anonymous speech is not implicated in this case. For these and the foregoing reasons, the trial court did not err in denying Zuck's first motion to suppress.

Second Motion to Suppress

¶31 Zuck also challenges the trial court's denial of his second motion to suppress evidence, which focused on the search warrant for his home and the affidavit provided in support of the warrant. Among the arguments Zuck made in his motion was that the affidavit supporting the warrant: (1) "lacked the requisite information necessary for the judge to make an informed determination of probable cause" and was based on stale information; (2) "contained deliberate falsehoods, material omissions, and reckless disregard for the truth"; (3) included evidence "from an unlawful, unconstitutional continuous 'mechanical' 'intercept' of 'electronic communications'"; and (4) "contained information from unconstitutional . . . 'tracking' of online searches and online behaviors." Zuck also contended he was entitled to a *Franks* hearing.

¶32 Denying the motion to suppress, the trial court found Zuck's "objections to allegedly untrue statements in the affidavit relate to general statements that the Court finds are accurate." The court concluded

[10]Further, Zuck fails to point to the "Notice to Cox Customers" in the record, providing only a broken hyperlink.

probable cause supported the search warrant, police had "not violate[d] any wiretap laws," and "[t]he law enforcement software monitored public peer-to-peer networks, and users therefore had no reasonable expectation of privacy on those networks." Zuck reasserts his arguments on appeal.

Legality of the Roundup Software

¶33 We first address Zuck's claim that "continuous electronic monitoring of . . . communications in a peer-to-peer network . . . was unlawful and unconstitutional under the state and federal constitutions" and thus could not provide evidence to support the search warrant. As we stated above, the Fourth Amendment and Private Affairs Clause[11] "protect[] people . . . 'seek[ing] to preserve something as private' [when] that expectation is 'one that society is prepared to recognize as reasonable.'" *Mixton*, 250 Ariz. 282, ¶¶ 13, 41 (quoting *Carpenter*, 138 S. Ct. at 2213). Evidence obtained in violation of these provisions cannot support the issuance of a search warrant. *See State v. Hackman*, 189 Ariz. 505, 508 & n.3 (App. 1997); *State v. Gulbrandson*, 184 Ariz. 46, 58 (1995).

¶34 Below, Zuck asserted that "police need judicial authorization to place a mechanical recording device in a p2p network to eavesdrop 24/7, [and] record and analyze non-public anonymous 'electronic communications.'" He also emphasized that "trusted members of p2p networks" attempt to block untrusted members. Given this, Zuck asserted that police's use of the Roundup software in this case was analogous to a detective secretly entering a conference call without any authorization and intercepting communications.

¶35 On appeal, Zuck first relies on *State v. Jean*, 243 Ariz. 331, ¶ 32 (2018), a case in which our supreme court concluded "passengers traveling with the owner in a private vehicle generally have a reasonable expectation of privacy that is invaded" by GPS tracking, alluding that the Roundup software also "allows the government to continually gather, store, and mine vast amounts of information at relatively little cost." He also points to *Riley v. California*, 573 U.S. 373 (2014), and *Kyllo v. United States*, 533 U.S. 27 (2001), asserting that "[c]ourts in other contexts have recognized the need to

[11]The state argues Zuck's state constitutional argument is waived on appeal. However, Zuck mentions our state constitution in his argument heading, cites the Private Affairs Clause in his argument that the use of the Roundup software was unconstitutional, and cites two cases analyzing that clause—*Mixton*, 247 Ariz. 212, ¶ 14, and *State v. Jean*, 243 Ariz. 331, ¶ 32 (2018). We decline to deem this argument waived.

consider the impact of evolving technology when applying the Fourth Amendment."

¶36 In light of these concerns, Zuck reasserts his argument that "allowing law enforcement to run programs that intrude on the privacy of users who have a reason for anonymity and make efforts to protect their privacy without probable cause and judicial authorization" is unconstitutional.[12] In response, the state argues, "because he ha[s] no reasonable expectation of privacy in the information he shared publicly over the peer-to-peer network," Zuck's claim fails. The crux of the state's argument is that "Zuck placed his personally selected computer files in a location . . . that was readily accessible to a large number of people not within Zuck's control, including the police."

¶37 We agree. At the suppression hearing, the state established that although files downloaded through the peer-to-peer software used by Zuck can be moved to any folder on a computer, they are automatically saved to a default folder where they "are available to be shared on the network with others." Thus, law enforcement is able to access those shared files by using "the same tools that any other common user on the" peer-to-peer network could use.

¶38 This is not a situation similar to the government surreptitiously tracking a passenger in a private vehicle via GPS, *see Jean*, 243 Ariz. 331, ¶ 32, searching the contents of one's cell phone incident to an arrest, *see Riley*, 573 U.S. at 403, or using a device "to explore details of the home that would previously have been unknowable without physical intrusion," *Kyllo*, 533 U.S. at 40. Rather, as the state points out, Zuck's use of the peer-to-peer software was akin to him leaving illicit files in "one of the 'Little Free Libraries' currently proliferating in neighborhoods, where people place cabinets of books outside their homes for any passers-by to take and read." Any expectation of privacy Zuck had in material shared as such was not reasonable, therefore, no constitutional violation occurred in its gathering and it properly supported the issuance of the search warrant.

[12] Zuck also claims this alleged action "violates the . . . 5th . . . amendment[] of the U.S. Constitution; Ariz. Const. art. 2 §§ 6 . . . and 24, and 18 U.S.C. 2510 *et seq.*, and A.R.S. § 13-3010." These arguments are waived for lack of development. *See* Ariz. R. Crim. P. 31.10(a)(7)(A); *Bolton*, 182 Ariz. at 298.

Misleading and Inaccurate Information

¶39 Zuck further contends that the search warrant affidavit contains "false information" and that he was thus entitled to a *Franks* hearing. "[A] defendant is entitled to a hearing to challenge a search warrant affidavit when he shows (1) that the affiant knowingly, intentionally, or with reckless disregard for the truth included a false statement in the affidavit, and (2) the false statement was necessary to the finding of probable cause." *State v. Buccini*, 167 Ariz. 550, 554 (1991) (citing *Franks*, 438 U.S. at 155-56). A trial court's determination of whether the affiant included a false statement is a factual determination that we will uphold unless it is clearly erroneous. *See id.*; *see generally In re Martinez*, 248 Ariz. 458, ¶ 6 (2020) ("Findings are clearly erroneous if they are not supported by reasonable evidence." (quoting *In re Alexander*, 232 Ariz. 1, ¶ 11 (2013))).

¶40 Zuck argued below that "[i]n his Affidavit for Search Warrant, Det[ective] Holewinski falsely claims that he identified a . . . singular computer . . . by an IP address that a computer used to access the internet . . . ." He asserted that "[i]t was impossible for [the detective] to identify that there was one, and only one, computer device accessing the internet through the . . . IP address under investigation," given that multiple devices can associate with the same IP address. Thus, he concluded the detective improperly referred to a "known computer."[13] The trial court ruled:

> [T]hings such as the Judge needed to know that it wasn't a computer or that a computer hadn't been identified, the fact that some computer within that home on that date downloaded it is sufficient so . . . I don't find that there were any false statements knowingly or intentionally made or with reckless disregard . . . .

¶41 On appeal, Zuck again claims the identification of a "specific computer address" is "false information." The state, however, urges it established at the suppression hearing that "when law enforcement

[13] The affidavit states: "On 9/19/13, I was conducting an investigation into the sharing of child sexual abuse files . . . on a file sharing network. At that time, I identified a computer with the IP address . . . as a potential download candidate . . . for multiple file(s) of investigative interest."

downloads a file over a peer-to-peer network, they 'connect[] only to one computer at [a] time.'" (Alterations in original.) Therefore, the state asserts the affidavit correctly references an individual computer.[14]

¶42 The trial court's finding was supported by reasonable evidence and, therefore, not clearly erroneous. As the state points out, testimony at the suppression hearing established that when law enforcement gathers illicit images through Roundup, it performs a "single source connection" from "the other computer." Thus, the affidavit accurately references a single computer and that the officer identified it as a potential "download candidate" for illicit material. We find no error.

Probable Cause

Depiction of Actual Minors

¶43 Zuck argues the search warrant affidavit did not establish probable cause that "the [initial] downloaded images were [not] constitutionally-protected speech [and instead] illicit child pornography." A search warrant affidavit must establish probable cause, meaning it must demonstrate that "a reasonably prudent person, based upon the facts known by the officer, would be justified in concluding that the items sought are connected with the *criminal activity* and that they would be found at the place to be searched." *Buccini*, 167 Ariz. at 556 (emphasis added) (quoting *State v. Carter*, 145 Ariz. 101, 110 (1985)); *see also* A.R.S. § 13-3913. Further, we concluded in *Hazlett* that § 13-3553, which prohibits possession of "any visual depiction in which a minor is engaged in exploitive exhibition or other sexual conduct," is limited to "material involv[ing] actual children." 205 Ariz. 523, ¶¶ 21-22.

¶44 Zuck argues on appeal, as he did below, that the warrant affidavit was required to point to evidence, other than the downloaded illicit media itself, establishing it portrayed actual minors. The state counters that such evidence was provided, specifically, that "the Roundup

[14]In this section of his opening brief, Zuck does not identify the specific language in the affidavit with which he takes issue. However, earlier in his brief, he points to a section of his motion to suppress that highlights the language, "*identified* a computer with the IP address." (Emphasis added.) In its answering brief, however, the state refers to a section of the affidavit stating, "I successfully completed downloading 1 file(s) from the computer with [the] IP address." We address the former passage.

software was searching exclusively for known and verified child pornography" and that the files' contents had already been verified.

¶45 In this respect, we conclude the affidavit established probable cause sufficient to support the search warrant. The affidavit states police sought to gather, within Zuck's residence, several "[e]lectronic data processing and storage devices, computers[,] and computer systems." Supporting this, the affidavit explains how a file verified as "depict[ing] children under the age of 18 engaged in sexual acts and/or exploitive exhibition" was downloaded from the IP address linked to Zuck's home address, and that there was no "unsecured wireless network coming from the residence." Further, the affidavit provides information on another file downloaded from that IP address, including the descriptive file name and details of what it depicted. The affidavit plainly states, "This is a video file of a prepubescent female between 9-12yoa." Given this, a reasonable and prudent person would be justified in concluding the items sought at Zuck's home were connected with the criminal activity, specifically, possession of prohibited files depicting actual minors.

Staleness

¶46 Zuck further challenges the search warrant affidavit, arguing "[e]vidence that an image was downloaded in September 2013 was stale when there was no reason to believe the image was retained." "[P]robable cause to justify the issuance of a search warrant must exist at the time the warrant is issued." *State v. Hale*, 131 Ariz. 444, 446 (1982). However, "staleness depends more on the nature of the activity than on the number of days that have elapsed since the . . . information was gathered." *Id.* Thus, there is no arbitrary period of time in which information supporting a warrant affidavit becomes stale. *See id.*

¶47 Zuck restates his argument that the allegation that an illicit image was traced to his IP address about three months before the warrant was issued could not support probable cause to search his home. The state, however, responds that "[g]iven the nature of the conduct involved—sharing and collecting child pornography—and especially in light of [the detective's] testimony that he has seen pornographic files retained for more than twenty years, there was no evidence supporting any argument that the information was stale."

¶48 We conclude a reasonably prudent person would be justified in determining that the items sought in Zuck's home when the warrant was issued would be "connected with" the files traced to his IP address. *Buccini*, 167 Ariz. at 556 (quoting *Carter*, 145 Ariz. at 110); *see Hale*, 131 Ariz. at 446.

Here, police downloaded the initial illicit media from a computer associated with Zuck's home IP address. And, consistent with assertions in other cases that "collectors and distributors [of child pornography] rarely, if ever, dispose of their collections," the affidavit states that such collectors typically retain these files "for many years." *United States v. Carrol*, 750 F.3d 700, 704 (7th Cir. 2014) (alteration in *Carrol*) (quoting *United States v. Prideaux-Wentz*, 543 F.3d 954, 958 (7th Cir. 2008)). Based on this, a reasonable person would be justified in concluding the media at issue remained stored on a device associated with the IP address[15] for the nearly three months between the detection of the files and the warrant being issued.[16] We therefore find no error in the trial court's denial of Zuck's second motion to suppress.

Disposition

¶49 For the foregoing reasons, we affirm Zuck's convictions and sentences.

[15]Zuck also claims that because "a visitor . . . to [his] residence could have accessed" its modem, and thus its IP address, "the affidavit did not provide any probable cause . . . that the device to which the image was downloaded in September 2013 would still be [there] in December 2013 because it may have only been [there] for a very short time." We disagree. *See State v. Sisco*, 239 Ariz. 532, ¶ 15 (2016) ("[P]robable cause requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." (alteration in *Sisco*) (quoting *Illinois v. Gates*, 462 U.S. 213, 243 n.13 (1983))).

[16]Zuck also again claims the inclusion of his prior conviction for attempted molestation of a child in the affidavit "did not support a probable cause determination," and thus the search warrant would completely lack support in the absence of the other assertions he argues should not have been considered. Based on our discussion above, we conclude the affidavit provided probable cause absent this assertion and thus, we need not address it.