IN THE COURT OF APPEALS OF THE STATE OF ALASKA

RICHARD MARTIN O'CONNOR, Appellant, v. STATE OF ALASKA, Appellee.	Court of Appeals No. A-12197 Trial Court No. 3AN-11-8501 CR MEMORANDUM OPINION No. 6786 — April 10, 2019

Appeal from the Superior Court, Third Judicial District, Anchorage, Michael L. Wolverton, Judge.

Appearances: Steven M. Wells, Steven M. Wells, P.C., Anchorage, for the Appellant. Donald Soderstrom, Assistant Attorney General, Office of Criminal Appeals, Anchorage, and Jahna Lindemuth, Attorney General, Juneau, for the Appellee.

Before: Mannheimer, Chief Judge, and Allard and Wollenberg, Judges.

Judge WOLLENBERG.

Following a bench trial, Richard Martin O'Connor was convicted of one count of distributing child pornography and five counts of possessing child pornography.[1]

[1] AS 11.61.125 and AS 11.61.127, respectively.

On appeal, O'Connor raises two challenges to the search warrants that authorized the police to search his residence. First, O'Connor argues that the search warrants were overbroad. Second, O'Connor argues that the detective who applied for the search warrants intentionally omitted material information from the search warrant affidavit. For the reasons we explain in this opinion, we reject these claims.

O'Connor also argues that the State failed to present sufficient evidence that the pornographic images on O'Connor's computers depicted real children. We conclude that there was sufficient evidence to establish this element of the State's proof.

Underlying facts and prior proceedings

On October 12, 2010, Anchorage Police Detective Tammy Dunn, a member of the cyber crimes unit, discovered that someone using a particular internet protocol (IP) address had digital files indicative of child pornography available for download on a shared folder. Detective Dunn discovered these files using an investigative software program. Unlike standard peer-to-peer file-sharing software — which collects portions of a user's requested content from numerous other available "peer" folders and compiles those pieces into a single file for the user — the law enforcement software that Dunn used is designed to connect to a single IP address and directly download content from that single source. The software identifies images of child pornography by matching the "hash values" of the user's computer files with the hash values of files known to be child pornography.[2]

Using this investigative program, Dunn downloaded thirty-one images of suspected child pornography from the targeted IP address. After downloading these

[2] A "hash value" is a mathematically calculated alphanumeric code that uniquely identifies a digital item or file. Altering a single pixel in a digital picture will generate a completely different hash value.

images, Dunn confirmed that the images constituted child pornography. Dunn then determined that the IP address was located in Anchorage and was assigned to a local internet provider, General Communication, Inc. (GCI).

In order to identify the subscriber who had this IP address, Dunn applied for, and received, a search warrant for GCI's records. These records showed that the internet account was registered to Richard O'Connor and that a woman (later determined to be O'Connor's girlfriend) was listed as the secondary account holder. Dunn confirmed through O'Connor's DMV records that he was associated with the same physical address listed on the internet account.

Based on this investigation, Dunn obtained a search warrant for O'Connor's residence. The officers who executed this warrant seized a Gateway computer that was running and plugged into a monitor, a Dell computer tower that was not connected to anything, and several portable digital storage devices. After leaving the apartment, the officers realized that they had inadvertently left behind a home-built computer tower; Dunn applied for and received another search warrant specifically to retrieve this computer.

Detective Mark Thomas performed a forensic analysis of the three computers seized from O'Connor's residence. The forensic analysis of the Gateway computer identified 146 images and six videos depicting child pornography in the computer's "allocated space," meaning that the files had not been deleted. These files were saved under a user account named "Richard" in a LimeWire folder. (LimeWire is a now-discontinued peer-to-peer file-sharing program.)

The forensic analysis of the Dell computer identified 174 images of child pornography in the allocated space of that computer. Thomas also found numerous documents linking the computer to O'Connor, including several resumes, letters from O'Connor to family members, and an essay by O'Connor about file-sharing.

The forensic analysis of the home-built computer identified 103 images of child pornography in the allocated space of that computer. Thomas discovered a folder on the computer that was titled "ME!" and which contained images of O'Connor that appeared to be self-taken.

A compact disc discovered in O'Connor's office contained five images and two videos of child pornography.

A grand jury indicted O'Connor on one count of distributing child pornography (based on the thirty-one images obtained by Dunn from the shared folder whose contents were available for downloading by other internet users), and five counts of possessing child pornography (one count for each of the four storage devices that contained pornographic images, and a fifth count for the videos found on the Gateway computer).[3]

Before trial, O'Connor filed two motions to suppress the evidence seized from his residence, arguing that (1) the search warrants for his residence were overbroad, and (2) Dunn intentionally omitted relevant information from the affidavit in support of the search warrants. The trial court denied both motions.

O'Connor waived his right to a jury trial, and he proceeded to a bench trial. The trial judge found O'Connor guilty of all six counts.

O'Connor's claims that the search warrants were overbroad

Both the United States Constitution and the Alaska Constitution provide that "no warrants shall issue, but upon probable cause . . . and particularly describing the

[3] AS 11.61.125 and AS 11.61.127, respectively.

place to be searched, and the persons or things to be seized."[4] Search warrants must be specific, both in particularity and in breadth. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based."[5]

O'Connor argues that the search warrants for his residence were overbroad in several respects.

O'Connor's primary argument is that the warrant authorizing the search of all of his electronic devices was deficient for not requiring investigators to follow a specific search protocol that would prevent the police from viewing documents and files when there was no reason to suspect that these documents and files contained child pornography. In support of his argument, O'Connor relies on a series of decisions by the Ninth Circuit in *United States v. Comprehensive Drug Testing* (the "*CDT* cases"),[6] in which the federal government seized testing records for hundreds of professional baseball players, even though the government only had probable cause to seize and search the records of ten players.[7]

In the Ninth Circuit's series of decisions, the court discussed at length the problem of striking an appropriate balance between the Fourth Amendment's prohibition on general warrants and the legitimate needs of law enforcement. In an early decision

---

[4] U.S. Const. amend. IV; Alaska Const. art. I, § 14.

[5] *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993) (quoting *In re Grand Jury Subpoenas Dated December 10, 1987*, 926 F.2d 847, 856-57 (9th Cir. 1991)); *see also Namen v. State*, 665 P.2d 557, 560 (Alaska App. 1983).

[6] *See United States v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085 (9th Cir. 2008) (*CDT I*), *on reh'g en banc*, 579 F.3d 989 (9th Cir. 2009) (*CDT II*), *opinion revised and superseded*, 621 F.3d 1162 (9th Cir. 2010) (*CDT III*).

[7] *See id.* at 1089-95.

in this series, the Ninth Circuit initially directed magistrates to require law enforcement to adhere to several specific guidelines when applying for and executing search warrants for electronic evidence.[8] However, in the last of the *CDT* cases, these guidelines were removed from the majority opinion (where they would have been binding law) and instead incorporated in a concurring opinion.[9] O'Connor urges us to adopt these guidelines as binding law in Alaska.

We decline to do so — primarily because we fail to see how application of these guidelines would entitle O'Connor to relief under the facts of this case. As an initial matter, we note that the Ninth Circuit has explicitly rejected the application of the *CDT* guidelines to a child pornography case with analogous facts.[10]

In *United States v. Schesso*, the police obtained a warrant to search and seize multiple electronic media and data storage devices from the defendant's home, based on an investigation that had identified the defendant's IP address as having uploaded, through a peer-to-peer file-sharing network, a video depicting child pornography.[11] The Ninth Circuit considered whether the search warrant was deficient for failing to require the police to follow a specific search protocol when they examined the electronic devices seized from the house.[12]

But the court concluded that no such protocol was required because the facts of *Schesso* "did not implicate the real concern" underlying the *CDT* protocol: "preventing the government from overseizing data and then using the process of

---

[8] *See CDT II*, 579 F.3d at 1004-07.

[9] *CDT III*, 621 F.3d at 1178-80 (Kosinski, J., concurring).

[10] *United States v. Schesso*, 730 F.3d 1040 (9th Cir. 2013).

[11] *Id.* at 1043-44.

[12] *Id.* at 1047-50.

identifying and segregating seizable electronic data 'to bring constitutionally protected data into . . . plain view.'"[13] In *Schesso* — unlike in *CDT* — the government properly executed the warrant, seizing only those items covered by the warrant and for which it had probable cause.[14]

In O'Connor's case, there is no indication in the record that the officers accessed unrelated documents for which there was no probable cause. Rather, the record reflects that, aside from images and videos of child pornography, the only other evidence the police seized from O'Connor's devices were items that the warrants separately authorized the police to search for and seize — items such as documents tending to establish that O'Connor had custody or control of the devices.

Moreover, although the search warrants in O'Connor's case did not prescribe an explicit search protocol, the detectives in this case employed a search tool that was designed specifically to identify child pornography. Detective Thomas (the officer who performed the forensic examination of O'Connor's digital devices) explained that he used a program called "Forensic Toolkit" — a program which employs a mathematical algorithm to match the hash values of suspect computer files against the list of hash values contained in a database of child pornography maintained by the National Center for Missing and Exploited Children (NCMEC).

O'Connor argues that the officers who executed the search warrant took no steps to protect the privacy of O'Connor's girlfriend, who also lived in the household. But O'Connor does not have standing to assert a violation of another person's Fourth

---

[13] *Id.* at 1047 (quoting *CDT III*, 621 F.3d at 1171 (per curiam opinion)).

[14] *Id.* at 1049.

Amendment rights.[15] Moreover, there is no evidence that the officers over-seized data in a way that violated the rights of O'Connor's girlfriend.

In any event, the search warrant was not specific to O'Connor. The warrant was based on probable cause to believe that *someone* was downloading child pornography at the residence associated with the IP address. The search warrant did not allege that a particular person had committed this crime; rather, the warrant asserted that there was probable cause to believe that evidence of this crime would be found at the specified residence. Both O'Connor and his girlfriend resided at this residence, and both of them were listed as subscribers on the internet account. There was therefore probable cause to search the computers and digital storage devices at that residence, regardless of whether O'Connor or his girlfriend owned the device.[16]

We therefore conclude that O'Connor's rights under the Fourth Amendment and the Alaska Constitution were preserved, and that application of guidelines akin to those discussed by the Ninth Circuit in the *CDT* cases would not have provided additional meaningful protection to O'Connor.[17]

---

[15] *See Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (noting that Fourth Amendment rights are personal rights, which may not be vicariously asserted).

[16] *See United States v. Adjani*, 452 F.3d 1140, 1146 (9th Cir. 2006) (noting that "[t]he 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") (quoting *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978)).

[17] We note that, to the extent evidence outside the scope of a warrant is seized, the remedy may not be suppression of the evidence against the defendant in the existing criminal case — but rather in any new criminal case premised on the discovery of those additional items (or in a civil lawsuit or action by a third party whose information was improperly seized).

O'Connor's next contention is that the warrants were facially overbroad because they authorized the seizure of items such as calendars, ledgers, and date books, for which the investigators lacked probable cause, as well as equipment like computer monitors, which normally have no storage capacity.

We question whether probable cause existed for the seizure of several of these items, and one might reasonably conclude that the warrant should not have authorized the police to seize these items.

But there is no indication in the record that the detectives seized items other than O'Connor's computers and digital storage devices. As O'Connor himself acknowledged in his motion to suppress in the trial court, even if the detectives lacked probable cause to seize items like calendars, ledgers, and date books, this would not invalidate the entire warrant in this case. Rather, it would result solely in suppression of those items.[18] And since none of these challenged items were introduced at O'Connor's trial, there is no basis for reversing O'Connor's convictions on this ground.

Finally, we note that there is one passage in O'Connor's opening brief in which he appears to assert that it was improper for the search warrants to authorize the seizure of all digital media in the residence, when Detective Dunn's initial investigation revealed pornographic images in only one shared LimeWire folder. However, O'Connor offers no substantive argument on this point — and in his reply brief, O'Connor seems

---

[18] *See United States v. Tamura*, 694 F.2d 591, 597 (9th Cir. 1982) ("Generally, the exclusionary rule does not require the suppression of evidence within the scope of a warrant simply because other items outside the scope of the warrant were unlawfully taken as well."); *Aday v. Superior Court*, 362 P.2d 47, 52 (Cal. 1961) (holding that, absent some indication that the warrant process was being abused, valid portions of a warrant were severable from invalid portions for which there was no probable cause); 2 Wayne R. LaFave, *Search and Seizure* § 4.6(f), at 814-17 (5th ed. 2012) (endorsing the "*Aday* rule," at least where there is no issue of pretext and the valid portions of the warrant are not an "insignificant or tangential part of the warrant") (internal quotations omitted).

to disclaim any such argument. We therefore conclude that, to the extent O'Connor intended to raise such a claim, it is inadequately briefed.[19] We also note that courts in other jurisdictions have consistently upheld search warrants authorizing the seizure of all digital storage devices and computer systems under similar circumstances — *i.e.*, where there is evidence that an individual is in possession of child pornography but no way of identifying (absent a further search) the particular devices on which the digital images are stored.[20]

---

[19] *See Petersen v. Mut. Life Ins. Co. Of N.Y.*, 803 P.2d 406, 410 (Alaska 1990) ("Where a point is not given more than a cursory statement in the argument portion of a brief, the point will not be considered on appeal.").

[20] Federal Courts: *See, e.g.*, *Schesso*, 730 F.3d at 1045 (upholding search warrant for all digital devices because law enforcement had no way of knowing where the illicit files might be stored); *United States v. Richards*, 659 F.3d 527, 541-42 (6th Cir. 2011) (holding that, in light of the information known at the time the search warrant was issued, the warrant to search the entire content of the defendant's server was not overbroad because the scope of the warrant was restricted to evidence of child pornography crimes and there was at least one red flag that the additional contents of the server might be tied to child pornography offenses); *United States v. Brobst*, 558 F.3d 982, 993-94 (9th Cir. 2009) (holding that the search warrant described the items to be seized — *i.e.*, all computer-related items — in the narrowest terms reasonably likely to contain the images, because law enforcement could not have known what storage media the defendant used to obtain child pornography from the internet); *United States v. Summage*, 575 F.3d 864, 871-72 (8th Cir. 2009) (concluding that, because there was no indication of the nature of the format in which the child pornographic materials were created or stored, the warrant validly allowed a search for a broad array of items for the relevant materials); *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir. 2000) (concluding that a warrant was not overly broad when it authorized the seizure of any computer equipment that may have been used in the production, distribution, or possession of child pornography); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (concluding that the description in the warrant — authorizing law enforcement to seize "any and all computer software and hardware, . . . computer disks, disk drives" — "was about the narrowest definable search and seizure reasonably likely to obtain the images" of child pornography); *United States v. Hall*, 142 F.3d 988, 996-97 (7th Cir. 1998) (upholding search (continued...)

For these reasons, we affirm the trial court's denial of O'Connor's suppression motion based on the breadth of the search warrant. We nonetheless take this opportunity to reiterate that law enforcement officers and judges should exercise great care in drafting and ratifying a search warrant's description of the things to be searched — particularly searches of digital computing and storage devices, where "the likelihood of the seizure of innocent articles by mistake is the most substantial."[21]

---

[20] (...continued)
warrants that authorized seizure of any digital storage devices because the warrants emphasized that the items sought were those related to child pornography); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (affirming validity of search warrant for all of defendant's computer equipment because law enforcement did not know whether the defendant had stored child pornography on the hard drive or any of the defendant's many computer disks).

State Courts: *See, e.g.*, *Commonwealth v. Molina*, 71 N.E.3d 117, 127-28 (Mass. 2017) (holding that a warrant that permitted a search of all computing devices found in an apartment was not overbroad when the police had information that child pornography had been sent and received through a computer device connected to an IP address assigned to the defendant); *State v. Aston*, 125 So.3d 1148, 1157 (La. App. 2013) (holding that possession and transmission of child pornography by a computer employing a particular IP address supported a search warrant for the entire residence linked to that IP address); *State v. Lehman*, 736 A.2d 256, 260-61 (Me. 1999) (holding that a "warrant was not unconstitutionally overbroad when it authorized the seizure of all computer-related equipment in [the defendant's] house" because the police "knew only that the images of the girls who [the defendant] allegedly sexually exploited were taken by a digital camera and downloaded to a computer").

[21] *Pohland v. State*, __ P.3d __, Op. No. 2632, 2019 WL 421247, at *7 (Alaska App. Feb. 1, 2019) (internal quotations and brackets omitted).

O'Connor's claim that the search warrant application contained material misstatements or omissions

O'Connor filed a motion to quash the search warrants (and to suppress the evidence seized under their authority) based on allegations that the officer who applied for the warrants (Detective Dunn) misrepresented material facts in her supporting affidavit. The trial court denied this motion, finding that the warrant applications "did not contain any material misstatements or omissions."

On appeal, O'Connor argues that Detective Dunn misled the magistrate in three ways. First, O'Connor argues that Detective Dunn failed to reveal to the magistrate that she had discovered child pornography at O'Connor's IP address on only a single occasion. But the affidavit thoroughly explained Dunn's investigation, including the fact that she downloaded thirty-one images of child pornography from O'Connor's IP address on October 12, 2010. The clear implication of Dunn's affidavit was that she had only accessed the IP address on October 12.

Second, O'Connor argues that Detective Dunn failed to disclose the existence of a subsequent injunction against LimeWire (the file-sharing utility that O'Connor was using), or the fact that this injunction applied to the version of LimeWire that O'Connor was using to download images of child pornography.[22] O'Connor argues that a "typical case involves repeated analysis of the same IP address," and he maintains that, once the injunction against LimeWire went into effect, Dunn could no longer

[22] *See* Tim Arango, *Judge Tells LimeWire, the File-Trading Service, to Disable Its Software*, The New York Times (Oct. 26, 2010), https://www.nytimes.com/2010/10/27/technology/27limewire.html.

conduct an investigation into whether O'Connor was continuing to download child pornography.[23]

But the fact that an injunction may have caused O'Connor's version of LimeWire to cease operation did not affect Dunn's investigation of O'Connor's activities *prior* to the injunction, nor did it impugn the evidence that Dunn collected before the injunction was issued. The search warrant in this case was based on evidence indicating that, prior to the date of the injunction, someone at O'Connor's residence was already in possession of, and offering to distribute, images of child pornography in a shared folder.

O'Connor's real argument appears to be that Dunn was required to investigate further before seeking a search warrant — *i.e.*, that she was required to access the shared folder on more than one occasion because, potentially, changes in the folder's contents might have shed light on whether O'Connor knowingly possessed the pornographic images.

But Dunn's failure to conduct further investigation does not constitute an "omission" of material information. Rather, it presents a question of whether Dunn had gathered enough evidence to establish probable cause to support the search. Although O'Connor raised this lack-of-probable-cause argument in the trial court, he does not expressly renew it on appeal as an independent ground for reversal. We therefore do not address it further.

---

[23] O'Connor's trial attorney did not actually proffer any evidence as to whether O'Connor was unable to use LimeWire following the injunction, nor did he request an evidentiary hearing on this motion. But the subsequent trial testimony contradicts O'Connor's assertion that LimeWire became completely inoperable following the injunction. At trial, Dunn testified that the injunction did not "completely shut down" LimeWire's file-sharing programs, and when officers executed the warrant in January 2011, a version of LimeWire was still running on O'Connor's Gateway computer.

Finally, O'Connor argues that Detective Dunn omitted material information from the search warrant application when she failed to disclose that another person (O'Connor's girlfriend) was residing at the residence and was listed on the internet subscriber account. But this omission was not material to the probable cause determination. As we discussed above, Dunn's investigation revealed that *someone* was using the IP address associated with O'Connor's residence to make child pornography available for sharing on the internet. The fact that both O'Connor and his girlfriend were living at that address, and that both of them were subscribers to the internet account, was immaterial to the question of whether there was probable cause to believe that evidence of the crime would be found in the computers and digital storage devices at the residence.

Here, probable cause to search the residence was linked to the IP address, not to a particular person. In fact, the search warrant affidavit explicitly stated that the seizure of evidence from the residence would "assist in the identification of the individual(s)" involved.

For these reasons, we uphold the trial court's denial of O'Connor's motion to quash the search warrants.

There was sufficient evidence for the trial judge to conclude that O'Connor possessed pornographic images of actual children

To establish each charge of distributing or possessing child pornography, the State was required to prove (among other things) that the pornographic images in O'Connor's possession depicted actual children under the age of eighteen.[24] O'Connor

[24] *See* AS 11.61.127(a); AS 11.61.125(a); *Ferrick v. State*, 217 P.3d 418, 421 (Alaska App. 2009).

argues that the State failed to establish that the images on O'Connor's computer depicted real children.

O'Connor's argument is premised on a mistaken view of the record. O'Connor argues that the State relied on Thomas's and Dunn's testimony about the NCMEC database to establish that the images in this case depicted real children. O'Connor contends that the detectives' reliance on this database violated his right to confrontation under the federal and Alaska constitutions, since neither Thomas nor Dunn personally investigated those images and personally confirmed that those images depicted actual children.

But Thomas testified, based on his own training and experience, that the images depicted actual children. Thomas also explained that he had techniques for discovering whether an image had been digitally altered, and he testified that the images found on O'Connor's computers had not been altered. The trial judge (sitting as the finder of fact) based his verdict not only on Thomas's testimony (which the judge found credible), but also on the judge's own review of the pornographic images themselves.

When a defendant challenges the sufficiency of the evidence to support a criminal conviction following a bench trial, an appellate court must evaluate whether there is "substantial evidence" to support the court's verdict.[25] This is the same test that an appellate court applies to jury verdicts.[26] Under this test, this Court is obliged to view the evidence, and all reasonable inferences to be drawn from that evidence, in the light most favorable to upholding the trial judge's verdict.[27] The question is whether, based

---

[25] *Helmer v. State*, 608 P.2d 38, 39 (Alaska 1980).

[26] *Shayen v. State*, 373 P.3d 532, 535 (Alaska App. 2015).

[27] *Id.*

on this view of the evidence, a reasonable fact-finder could conclude that the State had proved its case beyond a reasonable doubt.[28]

Based on the evidence presented at O'Connor's trial, including Detective Thomas's testimony and the images themselves, a reasonable fact-finder could conclude that the State proved beyond a reasonable doubt that the images on O'Connor's digital devices depicted actual children.[29]

To the extent O'Connor is raising an independent confrontation clause challenge to the admission of any information about the contents of the NCMEC database, we note that the trial judge expressly admitted Thomas's and Dunn's testimony regarding the NCMEC database for the non-hearsay purpose of establishing the detectives' general investigative procedures. O'Connor does not challenge this ruling on appeal. Because this testimony was offered for a non-hearsay purpose, its admission did not violate O'Connor's right to confrontation.[30]

---

[28] *Id.*; *Johnson v. State*, 188 P.3d 700, 702 (Alaska App. 2008).

[29] *See United States v. Salcido*, 506 F.3d 729, 733-34 (9th Cir. 2007) (concluding that pornographic images themselves are sufficient to prove the depiction of actual minors); *United States v. Rodriguez-Pacheco*, 475 F.3d 434, 439 (1st Cir. 2007) (recognizing that there is no "per se rule that the government must produce expert testimony in addition to the images themselves, in order to prove beyond a reasonable doubt that the images depicted are of real children") (citing *United States v. Nolan*, 818 F.2d 1015, 1018-20 (1st Cir. 1987)); *United States v. Kimler*, 335 F.3d 1132, 1142 (10th Cir. 2003) (concluding that there is no broad, categorical requirement that, absent direct evidence of identity, an expert must testify that the unlawful image is of a real child); *United States v. Vig*, 167 F.3d 443, 449-50 (8th Cir. 1999) (holding that the pornographic images themselves provided sufficient evidence from which a jury could reasonably infer that the subjects were actual minors).

[30] *See Estes v. State*, 249 P.3d 313, 316 (Alaska App. 2011).

Conclusion

We AFFIRM the judgment of the superior court.