

IN THE COURT OF APPEALS OF THE
STATE OF OREGON

STATE OF OREGON,
Plaintiff-Respondent,

v.

BENJAMIN KALEB VESA,
Defendant-Appellant.

Clackamas County Circuit Court
19CR17823, 18CR78326;
A173385 (Control), A173386

Ulanda L. Watkins, Judge.

Argued and submitted April 29, 2022.

Kali Montague, Deputy Public Defender, argued the cause for appellant. Also on the briefs was Ernest G. Lannet, Chief Defender, Criminal Appellate Section, Office of Public Defense Services.

Peenesh Shah, Assistant Attorney General, argued the cause for respondent. Also on the brief were Ellen F. Rosenblum, Attorney General, and Benjamin Gutman, Solicitor General.

Before Aoyagi, Presiding Judge, and Joyce, Judge, and Jacquot, Judge.*

AOYAGI, P. J.

In Case No. 19CR17823, reversed and remanded. In Case No. 18CR78326, remanded for resentencing; otherwise affirmed.

* Jacquot, J., *vice* James, J. pro tempore.

AOYAGI, P. J.

While executing a search warrant on defendant's cellphone in connection with a robbery investigation, police officers discovered nude photographs and sexually explicit videos of a minor, which led them to obtain a second warrant allowing a broader search of the cellphone. Defendant was subsequently indicted in two separate cases. He moved to suppress the seized images, arguing that the warrants were constitutionally invalid. The trial court denied suppression. In Case No. 19CR17823, defendant was convicted of using a child in a display of sexually explicit conduct and first-degree encouraging child sexual abuse, based on the seized images. In Case No. 18CR78326, he was convicted of attempted second-degree robbery, second-degree kidnapping, and menacing. Defendant was sentenced on all convictions together. In this consolidated appeal, defendant raises a single assignment of error, challenging the denial of his motion to suppress. We agree with defendant that the trial court should have granted the motion, because the first warrant did not satisfy the particularity requirement in Article I, section 9, of the Oregon Constitution, and the second warrant was derivative of the first warrant. Accordingly, we reverse and remand in Case No. 19CR17823, and we remand for resentencing in Case No. 18CR78326.

FACTS

E is defendant's former girlfriend. On or about November 15, 2018, defendant sent E a message on Instagram requesting that she unblock him. E had blocked defendant on her phone and social media since their break-up a few months earlier. E and defendant exchanged text messages from November 15 to 17. On November 17, they agreed to meet in person. E picked up defendant in her car, and they parked and talked. Eventually, they began to argue. According to E, defendant prevented her from leaving, lifted his shirt to reveal a handgun, and forced her to withdraw \$800 from an ATM to pay him back for allegedly overdrawing his bank account while they were together. During the incident, E saw defendant use his cellphone and believed that he was texting someone. E eventually escaped and ran for help. Defendant ran from the car, and the police

were unable to locate him until a week later, when he was arrested. Defendant's cellphone was seized at the time of his arrest.

On December 17, 2018, Detective Turpin applied for a warrant to search defendant's cellphone. In his supporting affidavit, Turpin summarized the robbery investigation, including E's interview statements. He also described what he knew from training and experience. As relevant here, he averred that smartphones contain large amounts of digital information, such as photographs, videos, audio recordings, text messages, text message logs, email messages, phone call logs, contact lists, voicemails, positioning information, computer applications (apps), passwords for other electronic devices and programs, financial records, internet search logs, internet usage logs, and location positioning information. He described how information from cellphones "can be important in a criminal investigation," including that text messages "can explain a person's thoughts, actions and plans," that photographs or videos "can depict a person's actions and experiences," that call logs "can indicate who a person has been communicating with," and that location information "can provide investigators with information regarding a person's whereabouts and path of travel." Regarding text messaging, he explained that there are "two main types" for cellphones: Short Message Service (SMS), which is just text, and Multimedia Messaging Services (MMS), which can contain "images, audio, videos and other digital files." Turpin also explained how data can be embedded in digital photographs and "can be very useful to investigators."

Based on E's statements and his own training and experience, Turpin asserted that he had probable cause to believe that defendant had committed first-degree robbery, second-degree kidnapping, unlawful use of a weapon, coercion, and menacing, and that evidence of those crimes would be found on defendant's seized cellphone. Turpin requested a warrant to search the cellphone for "any" evidence of those crimes, but then specified that the search would be limited to the date range of November 15, 2018, to November 23, 2018, and that it would be limited to photographs, videos, text messages (SMS and MMS), Facebook Messenger,

Snapchat, Twitter, Instagram, any other installed messaging applications, email, voice messages, voicemail messages, call logs, contact lists, and cloud storage. The signed warrant is consistent with those date and data type limitations.

In the course of executing the warrant, officers discovered nude photographs and sexually explicit videos of a 16-year-old girl, C, on defendant's cellphone. Turpin knew and recognized C, which is how he knew that C was a minor. On February 13, 2019, Turpin obtained a second warrant to search defendant's cellphone, this time for evidence of certain child sex crimes, with a date range of July 1, 2018, to November 23, 2018. For present purposes, it is undisputed that Turpin relied on nude photographs and sexually explicit videos of C that were within the scope of the first warrant to establish probable cause for the second warrant.¹ A total of six sexually explicit videos of C were seized during execution of the second warrant.

Defendant was indicted in two separate cases. Based on the incident with E, he was charged in Case No. 18CR78326 with first-degree robbery, second-degree robbery, second-degree kidnapping, unlawful use of a weapon, coercion, and menacing. Based on the six sexually explicit videos of C, he was charged in Case No. 19CR17823 with six counts of using a child in display of sexually explicit conduct and two counts of encouraging child sex abuse.

Defendant moved to suppress the evidence found on his cellphone—specifically the nude photographs and sexually explicit videos of C, which the parties agreed was the only relevant evidence that was found—based on the first warrant being invalid under Article I, section 9,² and the second warrant being derivative of the first warrant. Defendant conceded that Turpin's affidavit established probable cause

¹ In the trial court, defendant initially challenged the manner in which the first warrant was executed, which resulted in officers viewing 48,864 photographs and 1,617 videos on the cellphone without date limitation. However, upon questioning by the court, regarding the fact that the specific evidence that defendant was seeking to suppress came within the date range of the first warrant, defendant effectively abandoned that argument and does not pursue it on appeal.

² Defendant also challenged the warrant under the Fourth Amendment to the United States Constitution, but we do not discuss that argument, given our disposition.

to search the cellphone for text messages and Instagram messages and that the nine-day timeframe in the warrant was appropriate. He argued, however, that probable cause did not exist to search for any other types of data, such that the warrant was overbroad. He also argued that the search commands were not specific enough. The state defended the first warrant in all respects. As for the second warrant, both parties agreed that its validity depended on the validity of the first warrant. That is, if the first warrant was valid, then so was the second warrant, but if the first warrant was invalid, then so was the second warrant.

After hearing the parties' arguments, as well as the testimony of Turpin and the officer who forensically examined the cellphone, the trial court denied the motion to suppress. The court concluded that Turpin had probable cause to search defendant's cellphone for videos and photographs in the nine-day timeframe at issue and that the warrant was "specific enough in describing what it was seeking to find."

Defendant entered a conditional guilty plea in Case No. 19CR17823, reserving his right to appeal the denial of his motion to suppress, and was convicted of using a child in a display of sexually explicit conduct (Count 1) and first-degree encouraging child sexual abuse (Count 7). In Case No. 18CR78326, defendant pleaded no contest to attempted second-degree robbery (Count 2), second-degree kidnapping (Count 3), and menacing (Count 6) and was convicted on those charges. All other charges in both cases were dismissed. Defendant was sentenced together in both cases. He appeals both judgments in a consolidated appeal.

ANALYSIS

Article I, section 9, provides that "no warrant shall issue but upon probable cause, supported by oath, or affirmation, and particularly describing the place to be searched, and the person or thing to be seized." The particularity requirement includes two related but distinct concepts: specificity and overbreadth. *State v. Mansor*, 363 Or 185, 212, 421 P3d 323 (2018). A warrant must be specific enough to allow an officer to identify with reasonable effort the place to be searched and the items to be seized. *Id.* (applying *State*

v. Blackburn/Barber, 266 Or 28, 35, 511 P2d 381 (1973)). It also must not permit a search broader than the probable cause that the affidavit supports. *Id.* (citing *State v. Reid*, 319 Or 65, 71, 872 P2d 416 (1994)). We review particularity challenges, as relevant to the denial of a motion to suppress evidence found in a warranted search, for legal error. *State v. Paye*, 310 Or App 408, 413, 486 P3d 808 (2021).

In this case, defendant argues that the first warrant to search his cellphone was both overbroad and insufficiently specific. Because it is dispositive, we address only the specificity issue, while acknowledging that there is some slippage between the two issues, particularly when reading a warrant and affidavit together. As to specificity, defendant argues that the warrant's search commands were not specific enough, in that they referred to broad categories of data, including "photographs" and "videos," without any limitation except date. As he did in the trial court, defendant argues that the date limitation alone does not save the warrant from a lack of specificity. The state disagrees, arguing that, when read together with Turpin's affidavit, the search commands in the warrant are implicitly limited to searching for evidence of "communications" relevant to the alleged crimes against E, and thus the warrant was sufficiently specific. Defendant takes issue with the state's argument on appeal, contending that it is inconsistent with the prosecutor's arguments to the trial court, that it is inconsistent with the warrant on its face, and that it depends on a misconception of what it means to read a warrant and affidavit together under *Mansor*.

We begin our analysis with some preliminary matters. First, we will consider the warrant and affidavit together, as both parties acknowledge is appropriate, because defendant did not controvert that the affidavit was physically attached to the warrant. *See Mansor*, 363 Or at 203-04 (describing the defendant's burden of proof in a warrant challenge). Second, we agree with defendant that the only information that the trial court could consider in deciding whether the warrant was sufficiently particular was that contained in the warrant and affidavit, and we therefore do not consider the officers' testimony at the suppression hearing, nor do we consider any external sources cited

by the state at oral argument. See *State v. Cannon*, 299 Or App 616, 618, 450 P3d 567 (2019) (“In reviewing whether a search warrant was supported by probable cause, we consider only those facts put before the magistrate in the supporting affidavit, along with reasonable inferences that can be drawn from them.”).

Third, as previously mentioned, it is undisputed that there was probable cause to search defendant’s cellphone for text messages and Instagram messages for the period November 15, 2018, to November 23, 2018—and we therefore assume without deciding that the search commands for those data types were sufficiently particular and otherwise valid. Finally, as previously mentioned, the nude photographs and sexually explicit videos of C found on defendant’s cellphone are the only evidence that defendant seeks to suppress. The parties agree that that evidence was found during execution of the “photographs” and “videos” search commands. As such, although defendant challenges the specificity of all the search commands (with the possible exception of the text message and Instagram commands), the only commands actually at issue on appeal are the “photographs” and “videos” commands, so we limit our discussion to them.³

With those preliminary issues resolved, we turn to the main issue, which is whether the warrant was sufficiently specific. For searches of electronic devices, a warrant is specific enough to satisfy the particularity requirement if it “describe[s], with as much specificity as reasonably possible under the circumstances, *what* investigating officers believe will be found” on the device, including, “if available and relevant, the time period during which the information was created, accessed, or otherwise used.” *Mansor*, 363 Or at 187-88, 216 (emphasis in original). “[T]he essential ‘thing’ about which a warrant must be particular is the probative information, not types of files or their location within the computer’s file-management system[.]” *State v. Savath*, 298

³ Because the only evidence subject to suppression was found during execution of the “photographs” and “videos” search commands, we also need not consider (and no one has raised) the issue of severability. See *State v. Turay*, 313 Or App 45, 63-66, 493 P3d 1058, *rev allowed*, 369 Or 69 (2021) (regarding the possibility of severing invalid commands from an otherwise valid warrant).

Or App 495, 500, 447 P3d 1, *rev den*, 365 Or 722 (2019). In other words, the “‘what’ is a description of the *information* related to the alleged criminal conduct which there is probable cause to believe will be found” on the electronic device. *Mansor*, 363 Or at 216 (emphasis in original).

In this case, we agree with defendant that the warrant was not specific enough as to what information the officers executing the warrant were supposed to look for in the “photographs” and “videos” on defendant’s cellphone. In reaching that conclusion, we reject the state’s argument that the affidavit implicitly limits the search commands for “photographs” and “videos” to photographs and videos containing or constituting “communications” relevant to the alleged crimes against E. That argument is inconsistent with the prosecutor’s arguments in the trial court and essentially amounts to an alternative basis to affirm that was not raised below. Even assuming that the argument is properly made for the first time on appeal,⁴ we are unpersuaded that the affidavit gives rise to the “communications” limitation argued by the state.

Where an affidavit is considered part of the warrant, as here, we must read the warrant’s search commands “in conjunction with and limited by the descriptions in the affidavit.” *State v. Turay*, 313 Or App 45, 58, 493 P3d 1058, *rev allowed*, 369 Or 69 (2021). That is because “the supporting affidavit can operate to inform those executing a warrant as to what they are authorized to search for under a specific command—*i.e.*, limit the parameters of the search command.” *Id.* (footnote omitted). For example, in *Mansor*, the police were investigating fatal injuries that an infant sustained while in his father’s care, and they obtained a warrant to search the father’s computers. 363 Or at 189-91. The warrant itself did not contain any instructions or limitations on what to search for, but the incorporated affidavit

⁴ The requirements for us to consider an alternative basis to affirm that were not argued to the trial court are discussed in *Outdoor Media Dimensions Inc. v. State of Oregon*, 331 Or 634, 659-60, 20 P3d 180 (2001), and include that the record must be materially the same as would have developed had it been raised. Defendant contends that the *Outdoor Media* requirements are not met, but neither party has significantly briefed the issue, and our disposition obviates the need to settle that threshold disagreement.

described the father’s statements to police that, just before calling 9-1-1 on June 12, he used his computer to search the internet for first-aid advice. *Id.* at 204. The court concluded that the affidavit “described the ‘what’ to be searched for and the relevant time frame: [t]he June 12 internet search history,” which made the warrant sufficiently specific. *Id.* at 219.

Like defendant, we agree with the state that the warrant to search defendant’s cellphone must be read in conjunction with Turpin’s affidavit—there is no room for debate on that point—but we disagree with the state as to the effect of doing so.

We first consider the warrant itself. The warrant commands officers to search defendant’s cellphone for a long list of “electronic aspects and their associated history”—specifically, photographs, videos, text messages (SMS and MMS), Facebook Messenger, Snapchat, Twitter, Instagram, any other installed messaging applications, email, voice messages, voicemail messages, call logs, contact lists, and cloud storage—for the period of November 15, 2018, to November 23, 2018. The warrant does not identify the crimes under investigation, nor does it contain any description of the alleged incident with E. On its face, the warrant lacks the specificity required by Article I, section 9. *See Savath*, 298 Or App at 501 (explaining that “details regarding specific ‘locations’ within the phone do little if anything to satisfy the particularity requirement,” because it “says almost nothing about the information [officers] may seek”).

We next consider whether the attached affidavit provided the necessary specificity. In the affidavit, Turpin requests a warrant to search the same data categories listed in the warrant—photographs, videos, text messages (SMS and MMS), Facebook Messenger, Snapchat, Twitter, Instagram, any other installed messaging applications, email, voice messages, voicemail messages, call logs, contact lists, and cloud storage—for the period of November 15, 2018, to November 23, 2018. Unlike the warrant, the affidavit identifies the crimes for which Turpin believed that evidence would be found on defendant’s cellphone: first-degree robbery, second-degree kidnapping, unlawful use of a

weapon, coercion, and menacing. The affidavit also describes the alleged incident with E, including that defendant and E had sent text messages and Instagram messages to each other from November 15 to 17, and that E saw defendant using his cellphone during the November 17 incident and believed that he might have sent text messages.

The affidavit attached to the warrant thus clarifies what evidence Turpin believed would be found in a search of the text messaging and Instagram data on defendant's cellphone: text messages and Instagram messages with E between November 15 and 17, and text messages sent during the November 17 incident. By contrast, the affidavit is completely silent as to what evidence Turpin believed would be found in defendant's photographs, videos, Facebook Messenger, Snapchat, Twitter, other installed messaging applications, email, voice messages, voicemail messages, call logs, contact lists, and cloud storage.

The state argues on appeal that the affidavit implicitly limits the search commands for *all* data types listed in the warrant and affidavit to evidence of "communications." The state reasons that the listed data types are "largely related to communications" and that the only two types of data specifically mentioned in relation to the incident with E—text messages and Instagram messages—are types of communications data. In the state's view, a reasonable officer reading the warrant and affidavit together would understand that defendant's phone was to be searched for "communications" between defendant and E from November 15 to 17, or between defendant and someone else on November 17, including communications-related photographs and videos, such as one might send or receive in an MMS text message (because MMS allows for photographs and videos to be included in text messages) or through Instagram (an application that allows sharing of photographs and videos).

We disagree that Turpin's affidavit implicitly limited the warrant's search commands in the manner argued by the state. A warrant to search a digital device must describe with specificity the information related to the alleged criminal conduct which there is probable cause to believe will be found on the electronic device. *Mansor*, 363 Or at 218. Here,

the affidavit connects the search of defendant's text messages and Instagram messages with the specific facts of the November 17 incident and the circumstances leading up to it, and, as the state points out, it actually narrows the relevant date range for those data types to November 15 to 17. But the affidavit does not connect the search of numerous other data types with any facts specific to the November 17 incident or the circumstances leading up to it. We consider it highly unlikely that an officer executing the warrant would understand from the affidavit that the officer was meant to search only for "communications" in the photographs and videos (and other listed data) on defendant's cellphone, particularly when nothing in the affidavit suggests that defendant used any of those data types in connection with the November 17 incident.

The training-and-experience portion of the affidavit does not alter that conclusion. Turpin averred that cellphones are capable of storing the various types of data listed in the affidavit, that such data "can be important in a criminal investigation," that MMS text messages are capable of containing photographs and videos, and that data embedded in photographs "can be very useful to investigators." Such averments, although true, were unrelated to the facts of this particular investigation, and they did not impose any clarifying limitation on what was to be searched for on defendant's cellphone. *See Cannon*, 299 Or App at 626 ("Statements in the affidavit that are derived from an officer's training and experience may *** be considered" when assessing the adequacy of a supporting affidavit's facts to establish probable cause, but "the officer's knowledge must be connected to the facts of a particular case.").

Having concluded that the warrant authorized the police to search defendant's cellphone for photographs and videos generally, not only those containing or constituting "communications," we readily conclude that the warrant lacked the required specificity under Article I, section 9, as to what officers were supposed to search for in defendant's photographs and videos.⁵

⁵ We express no opinion as to what our disposition would be if we agreed with the state that the affidavit imported a "communications" limitation onto all

In *Turay*, we held that a warrant’s search command for “[a]ny evidence regarding the locations, including geolocation information, of [several] phones” over a three-month period was not specific enough, because there was nothing to guide the officers executing the warrant as to “what geolocation data would be evidence of any criminal activity.” 313 Or App at 51, 59. A command to search for any photographs of the defendant and two named witnesses that showed “an association with prostitution including any profiting from prostitution” also was not specific enough, because it provided “little, if any guidance as to what reasonably could be expected to be found on the phone.” *Id.* at 63. However, a search command for photographs, videos, and other data depicting specific people engaged in specified activities (“sexually explicit positions or conduct that relate to internet postings or advertisements”) was specific enough. *Id.* at 60; *see also Paye*, 310 Or App at 415-16 (holding that a warrant was sufficiently particular, even though it authorized a broad search of the defendant’s computer for any evidence of the crimes of promoting or compelling prostitution, including listing numerous data types, because the attached affidavit contained witness statements about the defendant’s specific prostitution-related activities and his use of his computer in those activities, such that it was apparent that the evidence expected to be found on the computer consisted of “images and videos of women he prostituted, contact information for people connected with the crimes, and communications about the crimes”).

The search commands for “photographs” and “videos” on defendant’s cellphone are similar to the general search commands deemed insufficiently specific in *Turay*. It is true, as the state emphasizes, that the warrant in this case included a nine-day time limitation—allowing a search of photographs and videos created, modified, or deleted between November 15, 2018, and November 23, 2018—and temporal limitations do help identify “with greater specificity the ‘what’ that is being searched for.” *Mansor*, 363 Or at

of the warrant’s search commands, except to note that it would not necessarily make the warrant specific enough. *See Savath*, 298 Or App at 501 (“file types and categories of communications data that might be found within the phone *** do little if anything to satisfy the particularity requirement” (emphasis added)).

218. But we are unpersuaded that the nine-day temporal limitation in the warrant alone made the search commands for photographs and videos on defendant’s cellphone specific enough to meet the particularity requirement in Article I, section 9.

Without the necessary specificity, the first warrant amounted to a general warrant to search any and all photographs and videos on defendant’s cellphone—albeit only for a nine-day period—and allowed the officers executing the warrant to decide for themselves what constituted evidence of the crimes allegedly committed against E on November 17. “Both we and the Supreme Court have explained that a warrant authorizing a search for all ‘evidence of a particular crime’ is not sufficiently specific to pass constitutional muster.” *State v. Bock* (A169480), 310 Or App 329, 336, 485 P3d 931 (2021). That is in part because “[a] warrant without clear limitations on the material subject to search and seizure [improperly] requires the executing officer to employ discretion in deciding what to search or seize.” *Id.* at 334.

In sum, we agree with defendant that the warrant issued on December 17, 2018, lacked the specificity required under Article I, section 9, and was therefore invalid. It follows that the second warrant, issued on February 13, 2019, was also invalid.⁶ The trial court erred in denying defendant’s motion to suppress the photographs and videos of C found on defendant’s cellphone during the execution of those warrants. That evidence was relevant to defendant’s convictions in Case No. 19CR17823, so we reverse and remand in that case. Defendant was sentenced together in both cases, so we remand for resentencing in Case No. 18CR78326.

In Case No. 19CR17823, reversed and remanded. In Case No. 18CR78326, remanded for resentencing; otherwise affirmed.

⁶ As previously noted, the state does not dispute that if the first warrant is invalid, then so is the second. See *State v. Johnson*, 335 Or 511, 520-21, 73 P3d 282 (2003) (where officers use unlawfully obtained information to secure a warrant, evidence found in the warranted search must be suppressed, unless the state shows that the evidence would have inevitably been discovered or otherwise was not tainted by the illegality).