IN THE SUPREME COURT OF THE
STATE OF OREGON

STATE OF OREGON,
Petitioner on Review,
v.
AHMED GBANABOM TURAY, JR.,
Respondent on Review.
(CC 17CR59493) (CA A166973) (SC S068894)

On review from the Court of Appeals.*

Argued and submitted May 3, 2022.

Peenesh Shah, Assistant Attorney General, Salem, argued the cause and filed the briefs for petitioner on review. Also on the briefs were Ellen F. Rosenblum, Attorney General, and Benjamin Gutman, Solicitor General.

Morgen E. Daniels, Deputy Public Defender, Office of Public Defense Services, Salem, argued the cause and filed the brief for respondent on review. Also on the brief was Ernest G. Lannet, Chief Defender.

Kelly K. Simon, American Civil Liberties Union of Oregon, Portland, filed the brief for *amici curiae* the American Civil Liberties Union and the American Civil Liberties Union of Oregon. Also on the brief were Rachel Dallal, American Civil Liberties Union of Oregon, Portland, and Jennifer Stisa Granick, American Civil Liberties Union Foundation, San Francisco.

Before Flynn, Chief Justice, Duncan, Garrett, DeHoog, and Bushong, Justices, and Balmer and Walters, Senior Judges, Justices pro tempore.**

---

* On appeal from the Washington County Circuit Court, Oscar Garcia, Judge. 313 Or App 45, 493 P3d 1058 (2021).

** Nelson, J., resigned February 25, 2023, and did not participate in the decision of this case. James, J., did not participate in the consideration or decision of this case.

FLYNN, C. J.

The decision of the Court of Appeals is affirmed in part and reversed in part. The judgment of the circuit court is reversed, and the case is remanded to the circuit court for further proceedings.

Duncan, J., concurred and filed an opinion in which Walters, S. J., joined.

FLYNN, C. J.

Defendant in this criminal case was convicted of compelling prostitution, based in part on incriminating images and text messages that law enforcement found pursuant to a warrant to search his cell phone for nine categories of information (search categories). Defendant challenges the warrant, and that challenge presents the opportunity for this court to further consider the constitutional requirement that search warrants "particularly describe" the place to be searched or thing to be seized, Or Const, Art I, § 9, in the context of warrants that authorize law enforcement to search for digital data. *See generally State v. Mansor*, 363 Or 185, 421 P3d 323 (2018) (discussing and analyzing application of that "particularity" requirement to the search of a computer). And, because it is undisputed that the warrant in this case contained some search categories that failed to particularly describe the evidence sought, this case also requires us to decide whether and to what extent those unlawful search categories require suppression of evidence obtained through the search of defendant's phone. That question, in turn, involves a two-step inquiry: whether the unlawful search categories invalidated the warrant *in toto* and, if not, how the trial court should determine whether Article I, section 9, prohibits the state from using evidence that it obtained through executing the partially unlawful warrant to search for digital data.

As explained below, we conclude that five of the nine search categories set out in the warrant to search defendant's cell phone failed to satisfy the constitutional particularity requirement and, thus, that those categories failed to authorize a lawful search. We further conclude, however, that the inclusion of those unlawful search categories in the warrant does not necessarily require suppression of all evidence found on defendant's phone, for the following reasons. First, because the state extracted and examined data from defendant's phone in an effort to find evidence that no lawful category of the warrant authorized it to search for (in addition to the lawfully authorized categories), defendant has established a minimal factual nexus between a constitutional violation and the challenged evidence. Second, that minimal factual nexus undermines the presumption of

validity that ordinarily attends warrant-based searches and therefore requires suppression unless the state establishes that the challenged evidence was not tainted by the constitutional violation. We finally conclude that, in this case, the appropriate disposition is a remand for development of a factual record and for the trial court to make the required factual findings under the correct legal standard.

I. FACTS

The search warrant at issue authorized law enforcement to search two cell phones belonging to defendant. The affidavit supporting that warrant recited that Detective Opitz of the Beaverton Police Department had obtained information in August 2017 that had prompted him to suspect that defendant and an adult female, Gregg, were promoting and compelling a 17-year-old victim, J, into prostitution. Opitz located "numerous prostitution related postings" associated with Gregg—some with Gregg and the victim advertised as a "2 for 1" deal—on websites that he knew to be used by individuals offering sex for sale. Opitz then set up an undercover prostitution engagement with J by text message, including an arranged date, time, location, and price. On that arranged day, Opitz saw a car arrive at the designated parking lot just as J texted to say that she was arriving. Opitz recognized J when she exited the car, and other officers then stopped the car and arrested the driver—defendant. During an ensuing search of the car, officers found and seized two cell phones that they determined belonged to defendant.

Opitz later interviewed J, who told Opitz how she used her own cell phone to conduct business—that she had used her phone to communicate with customers and that she had posted, but not paid for, advertisements on a prostitution-related website (the website). She also told Opitz that she had met Gregg about 12 weeks prior and that Gregg had introduced her to defendant and also to prostitution. J further recounted that both Gregg and defendant knew that she was a minor; that she had engaged in joint prostitution engagements together with Gregg; and that she and defendant were "boyfriend/girlfriend," but also that defendant and Gregg had been in a relationship. Not long

thereafter, defendant was indicted on one count of compelling prostitution in relation to J, ORS 167.017.

Opitz then prepared an affidavit and accompanying search warrant to search various cell phones, including the two belonging to defendant.[1] The affidavit included extensive information about Opitz's background and training, as well as several statements—based on his knowledge and experience—relating to the connection between sex trafficking and the use of the internet and cell phones. Those aspects of the affidavit further discussed how various information could be stored and retrieved on cell phones, including an explanation of various cell phone features. The affidavit then described facts relating to the investigation of defendant, including those set out above.[2]

Finally, the affidavit identified the cell phones to be searched—including defendant's phones—and described nine search categories of digital data to be searched for, seized, and analyzed:

> "(1) Any and all communications (voice, email, text, or otherwise) between [J, defendant,] and/or *** Gregg.
>
> "(2) Evidence related to the relationship between [J, Gregg,] and/or [defendant].
>
> "(3) Evidence regarding any communications (voice, email, text, or otherwise) involving prostitution related activities.
>
> "(4) Any photos of [J, defendant, or Gregg] that show an association with prostitution including any profiting from prostitution.
>
> "(5) Images, videos and/or data which depict [J or Gregg] in sexually explicit positions or conduct that relate to internet postings or advertisements.

[1] The warrant also authorized the search of two cell phones belonging to J and another belonging to Gregg, but defendant's motion to suppress concerned only defendant's phones, and the record reflects that only one of defendant's phones was ultimately searched.

[2] The affidavit also stated that, in mid-September 2017, defendant and Gregg each had been indicted in federal district court on one count of sex trafficking of a minor. We discuss additional detail from the affidavit later in this opinion.

"(6) Any evidence related to use of internet sites associated with prostitution, including [the website] for a period of time 06/15/2017 to 09/06/2017.

"(7) Any evidence related to the use of Uber or other ride-sharing or taxicab companies.

"(8) Any evidence regarding the locations, including geolocation information, of the phones for a period of time from 06/15/2017 to 09/06/2017.

"(9) Any other evidence related to the crimes of Prostitution (ORS 167.007), Promoting Prostitution (ORS 167.012) and/or Compelling Prostitution (ORS 167.017)."[3]

The accompanying warrant was attached to the affidavit and repeated that wording verbatim.

A magistrate issued the warrant, and another detective, McNair, executed the search on all the phones listed in the warrant, using proprietary software that enabled the forensic examination of mobile devices. From one of defendant's cell phones, McNair retrieved two types of evidence: multiple incriminating photographs of J and others, some of which were screenshots from the website; and two extraction reports that set out multiple incriminating text messages between that phone and a contact named "baby," whom Opitz had determined to be J.[4] Notably, other than McNair's explanation at trial about how the software functioned as a general matter and also about the nature of the extraction reports that showed the text messaging, no testimony or other material in the record below described how the search of defendant's phone actually had been conducted—for example, the record does not show whether all, or just some, data was extracted before being analyzed; it does not show the order in which certain steps of the process occurred; and it does not show whether each of the described categories of evidence from the warrant was the subject of its own search when the incriminating evidence was discovered.

[3] The parties refer to those nine search categories as "search commands," but they are not "search commands" in the technical sense—instead, they are separately described categories of the digital data that was the object of the search.

[4] One extraction report was more comprehensive than the other, setting out similar, but also more extensive, text messaging between defendant and a contact who turned out to be J.

Before trial, defendant moved to suppress all evidence resulting from the search of his cell phone, arguing that the warrant had violated the particularity requirement set out in Article I, section 9.[5] The trial court denied that motion, and the state thereafter introduced the incriminating photos and text messages at trial. A jury convicted defendant on one count of compelling prostitution, and he appealed.

On appeal, defendant renewed his argument that the state had obtained the incriminating evidence in violation of the particularity requirement and that the trial court therefore should have granted his motion to suppress. In addressing those contentions, the Court of Appeals first determined that three of the search categories described in the warrant—the third, the fifth, and the sixth—satisfied the particularity requirement. *State v. Turay*, 313 Or App 45, 60, 61-62, 493 P3d 1058 (2021). But that court concluded that the remaining six categories fell short—either due to the absence of various limiting detail (such as location, time, or subject matter), or because they otherwise lacked the requisite specificity to permit the executing officer to reasonably identify the information sought. *Id.* at 58-62. Finally, the court concluded that, because it could not determine from the record which (if any) aspects of the state's challenged evidence had been discovered through execution of one of the three lawful search categories, it must remand to the trial court for further development of the record about how the forensic search of defendant's cell phone in fact had been conducted. *Id.* at 65-66.

The state petitioned for review, challenging the decision of the Court of Appeals. Although the state concedes that some of the search categories described in the warrant were insufficiently particular, it challenges the Court of Appeals' other key conclusion that other search categories failed to satisfy the constitutional particularity requirement, and it contends that no remand is needed because all the challenged evidence was properly admitted

[5] Defendant also argued that the warrant had not been supported by probable cause. The Court of Appeals rejected that argument, and defendant has not challenged that aspect of the Court of Appeals decision.

as falling objectively within the scope of lawful search categories. We allowed the state's petition for review, and, as explained below, we agree with the Court of Appeals that the case must be remanded for the development of a factual record and additional factual findings, although our conclusions differ from that court in two respects: (1) we agree with the state that one search category that the Court of Appeals assessed as constitutionally deficient satisfied the particularity requirement; and (2) our instructions on remand differ from those set out by the Court of Appeals.[6]

II. ANALYSIS

A. *Legal Background*

We begin by setting out the legal background that frames the parties' dispute. That background includes the particularity requirement itself, together with our case law construing that requirement—including, most recently, in the digital data context in *Mansor*, 363 Or 185.

1. *Particularity requirement generally*

The particularity requirement for warrants is set out in Article I, section 9, of the Oregon Constitution:

> "No law shall violate the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure; and 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*."

(Emphasis added.) The historic motivation for Article I, section 9, was a reaction to "general warrants," which were "'writs that authorized the bearer to search unspecified places or arrest persons suspected of having been involved with a criminal offense.'" *Mansor*, 363 Or at 206 (quoting Jack L. Landau, *The Search for the Meaning of Oregon's Search and Seizure Clause*, 87 Or L Rev 819, 822-23 (2008));

[6] The Court of Appeals' stated disposition was to vacate the trial court's judgment and then remand for a determination of how the search had been conducted. *Turay*, 313 Or App at 66. We conclude, however, that the appropriate disposition is to reverse (not vacate) the trial court's judgment, with remanded proceedings as described later in this opinion. We therefore affirm in part and reverse in part the decision of the Court of Appeals.

see also State v. Carter, 342 Or 39, 43, 147 P3d 1151 (2006) (explaining that the historical motivation for Article I, section 9, "was a fear of general warrants," which "gave the bearer an unlimited authority to search and seize" (internal quotation marks omitted)). In keeping with that purpose, the particularity requirement "exists to 'narrow the scope of the search,'" so that officers search only those premises or items "'for which a magistrate has found probable cause to authorize the search.'" *Mansor*, 363 Or at 212 (quoting *State v. Trax*, 335 Or 597, 602, 75 P3d 440 (2003)); *see also State v. Devine*, 307 Or 341, 343, 768 P2d 913 (1989) (explaining that the particularity requirement minimizes the risk of intrusion into premises other than those as to which a magistrate has found probable cause to search).

Until this court's recent decision in *Mansor*, we had addressed the particularity requirement only in the context of warrants authorizing searches of the physical world. In that context, we have held that the particularity requirement is satisfied if the warrant's description permits the executing officer to "locate with reasonable effort the premises to be searched." *Trax*, 335 Or at 603 (internal quotation marks omitted). Also, as to that type of warrant, the fact that one or more certain known facts might have enabled the drafting of a *more* particularized warrant does not necessarily mean that the warrant as drafted was *not* sufficiently particularized. *Id.* at 610. Rather, the question is whether the description, as written, was sufficiently clear to identify the premises to be searched with a "reasonable degree of certainty." *Id.* at 605-06, 610. If a warrant authorizing a search of physical premises fails to describe the location of the search with the required degree of particularity, however, then any search pursuant to the warrant "is illegal, whether of the premises actually intended or not, because of the danger that the privacy of unauthorized premises will be invaded." *State v. Blackburn/Barber*, 266 Or 28, 35, 511 P2d 381 (1973).

2. *The particularity requirement as applied to warrants to search for digital data*

In *Mansor*, we considered the proper analytical framework for applying the particularity requirement to the

search of a personal computer containing digital data. 363 Or at 212. We identified aspects of that requirement that differ from the context of a warrant to search the physical world, and we identified a special limitation on the state's use of information that it obtains pursuant to a warrant to search for digital data. Because *Mansor* is fundamental to the parties' arguments and our resolution of aspects of this case, we discuss it next in some detail.

In *Mansor*, police suspected that the defendant had played a role in the death of his infant son. 363 Or at 189. Based on information learned during their investigation, police sought a warrant to seize, search, and forensically examine several computers that they had seen in the defendant's home. *Id.* at 189-91. The warrant "contained no instructions or limitations regarding how the computers were to be analyzed," but it was supported by an attached affidavit describing evidence that might be found on the computers, most notably, internet search history associated with the date and approximate time when the defendant had called 9-1-1 to report the injury that had led to his son's death. *Id.*[7]

In directing and then conducting the ensuing search of the defendant's computers, detectives developed lists of search terms associated with the type of injury that the defendant's son had suffered (or associated with related surrounding circumstances), and forensic examiners later added additional terms of their own. *Id.* at 191. Ultimately, with minor exceptions, the examiners assembled a "complete Internet history" of the defendant's computers, including deleted internet history records. *Id.* at 192. Not all the records were associated with identified dates and times, and the final forensic analysis incorporated records dating back more than six years, including results for the search term

[7] The warrant in *Mansor* itself had merely authorized the seizure and search of the computers (and other equipment); it had contained no detail about the information sought or how the computers were to be analyzed. One issue in that case therefore involved the extent to which the attached affidavit could be considered as providing the "particularity" description required of the warrant, with the court concluding that it would consider the object of the search described in the affidavit to be part of the warrant. 363 Or at 203. For clarity here, references to the "warrant" in *Mansor* mean the warrant read in conjunction with the attached affidavit.

"abuse" covering a 16-month period before the defendant's son's death. *Id.* at 192-93.

Before trial, the defendant moved, unsuccessfully, to suppress all evidence discovered on his computers, arguing that the warrant had been "worded so broadly as to constitute a general warrant." *Id.* at 193 (internal quotation marks omitted). The state later relied on aspects of the forensic analysis at trial, and a jury convicted the defendant of murder and multiple other felonies. *Id.* at 194-95. The Court of Appeals reversed and remanded, and this court did as well, although on narrower grounds—ultimately concluding that the warrant had been sufficiently particular, but that the execution of the warrant had involved a forensic examination that exceeded the defined scope of the warrant and that the trial court had erred in admitting the state's evidence obtained as a result of that more extensive forensic examination. *Id.* at 196, 223.

Mansor discussed in detail the characteristics of digital data that alter how we understand the particularity requirement of Article I, section 9. Our first key point pertained to the nature of digital data itself and the ways in which such data, "whether stored on a computer or other digital device, differs from physical evidence"—that is, physical evidence that may be the subject of a more conventional warrant that must particularly describe the *place* to be searched. *Id.* at 197. Those differences included the fact that, to be meaningful, raw digital data must be processed and displayed by intermediating programs and hardware, *id.*; some data may not be in the form of "files," *id.*; and, with digital data, an examiner has no way to know what data a file contains without opening it, "meaning that desired data may be located in any part of the digital media or organizational structure," including in multiple places, and it even can be "inaccurate to think of the data as being located at any particular 'place' or 'places,'" *id.* at 198; *see also id.* at 214 (observing that, unlike in the physical world, in which "'different spatial regions are used for different purposes,'" with computers, "there is 'no way to know ahead of time where *** a particular file or piece of information may be located'" (quoting Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum L Rev 279, 303 (2005))).

Simply stated: Digital data is of a markedly different character than tangible, physical evidence, and it is stored in an entirely different manner—including in ways that pose a more pronounced or enhanced risk of intrusion into a person's privacy interests than otherwise would be permissible.

The next key point discussed in *Mansor* focused on how the process of searching for digital data necessarily differs from the process of searching for physical evidence. We explained that commentators and courts "sometimes refer to searches of computers in a criminal investigation as involving 'two basic steps: the data acquisition phase and the data reduction phase.'" *Id.* at 199 (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv L Rev 531, 547 (2005)). Analogizing to the proverbial needle in a haystack, we described the "data acquisition" step as "collecting the hay," and the "data reduction" step as "looking through the haystack for the needle"—"an examination ('search') of the digital data, *** by a forensic examiner, to identify the particular data that may be useful as evidence." *Id.* (quoting Kerr, 119 Harv L Rev at 545). We added that, because "the location or form of specific information on a computer often cannot be known before the computer is actually examined, examiners conducting a reasonable computer search" may need to "look widely on the computer's hard drive to ensure that all material within the scope of the warrant is found." *Id.* at 199-200. Stated another way, the forensic examination authorized by a warrant "necessarily may require examination of at least some information that is beyond the scope of the warrant." *Id.* at 220.

We relatedly considered in *Mansor* a United States Supreme Court decision, *Riley v. California*, 573 US 373, 134 S Ct 2473, 189 L Ed 2d 430 (2014), which had involved a warrantless seizure and search of a cell phone incident to arrest. In *Riley*, the Supreme Court rejected the notion that the search of all data on a phone was "'materially indistinguishable'" from searches of other physical items found on an arrestee's person, explaining that cell phones "'differ in both a quantitative and a qualitative sense'" from other physical items, including as to their immense storage capacity, their collection of many distinct types of information, and their capability of revealing personal internet search

history, interests, locations, political views, medical information, and myriad other personal information. *Mansor*, 363 at 201-02 (quoting *Riley*, 573 US at 393 (internal quotation marks omitted)). In other words, unlike the circumscribed search of a physical place or item, the search for digital data on a cell phone inherently carries with it—from the very outset of the search—an enhanced risk of extensive governmental intrusion into the privacy interests of the owner of the phone.

Taking those considerations into account, this court in *Mansor* then set out several governing principles, to ensure protection of "an individual's right to be free from unreasonable searches and seizures while also recognizing the government's lawful authority to obtain evidence in criminal investigations, including through searches of digital data." 363 Or at 187, 206. We began with the well-established principle that "'[t]he privacy interests protected from unreasonable searches under Article I, section 9, are defined by an objective test of whether the government's conduct would significantly impair an individual's interest in freedom from scrutiny, *i.e.*, [the individual's] privacy.'" *Id.* at 206-07 (quoting *State v. Wacker*, 317 Or 419, 425, 856 P2d 1029 (1993) (first brackets in *Mansor*; some internal quotation marks omitted)). We also recognized—as did the Supreme Court in *Riley*—that more conventional searches involve protected privacy interests "commonly *** circumscribed by the space in which they exist and, more particularly, by the barriers to public entry *** that define that private space"; and we emphasized that Article I, section 9, "must be read in light of the ever-expanding capacity of individuals and the government to gather information by technological means." *Id.* at 207 (internal quotation marks omitted). "That is, Article I, section 9, applies to 'every possible form of invasion—physical, electronic, technological, and the like.'" *Id.* (quoting *State v. Smith*, 327 Or 366, 373, 963 P2d 642 (1998)).

Applying those principles, we further considered in *Mansor* how the particularity requirement applies in the context of a warrant to search for digital data. We initially concluded that, although the execution of a lawful warrant to search digital data might require the examination of

some information that is beyond the scope of that warrant, the individual's privacy interests preclude the state from using that information unless a warrant exception applies. *Id.* at 220-21.

We next explained that the particularity analysis—in any context—is informed by "two related, but distinct, concepts," "specificity" and "overbreadth." 363 Or at 212. First, the warrant must be "sufficiently specific in describing the items to be seized and examined[.]" *Id.* Second, "even if the warrant is sufficiently specific, it must not authorize a search that is broader than the supporting affidavit supplies probable cause to justify."[8] *Id.* (internal quotation marks omitted). We further explained in *Mansor*, as discussed next, that the specificity component gives rise to special requirements in the context of a warrant to search for digital data.

Before *Mansor*, we had explained that a warrant authorizing a search of the physical world satisfies the specificity component of the particularity requirement if its description (1) "'permits the executing officer to locate with reasonable effort the premises to be searched,'" *id.* (quoting *Trax*, 335 Or at 603 (internal quotation marks omitted)); and (2) describes "items to be seized and examined" in a way "that the officers can, 'with reasonable effort[,] ascertain' those items to a 'reasonable degree of certainty,'" *id.* (quoting *Blackburn/Barber*, 266 Or at 35). In *Mansor*, though, we determined that a warrant to search for digital data also "must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used." *Id.* at 218. And we explained that, "when a time-based description of the information sought on a computer is relevant and available to the police," that detail "ordinarily should be set out in the affidavit" and included in the warrant's description of the evidence sought, as a way of

[8] Overbreadth as an aspect of the particularity inquiry differs from the fundamental requirement of Article I, section 9, that "no warrant shall issue but upon probable cause, supported by oath, or affirmation." The overbreadth inquiry arises even when there is probable cause for a warrant to issue and asks, essentially, whether an individual search category reaches beyond the scope of the probable cause that supports the warrant.

"identifying with *greater* specificity the 'what'" that is the object of the search. *Id.* (emphasis added).

We further emphasized in *Mansor*, however, that the warrant need not prescribe how a search for digital data is to be conducted. Given the challenges of identifying beforehand the location or form in which specified information will be found on a computer, we explained, "courts generally have not required that warrants include specific search protocols or *ex ante* limitations on computer searches." 363 Or at 200. We added that a magistrate reviewing a warrant application "would have little basis to make an informed decision as to whether proposed protocols regarding the seizure and search of a computer are sufficient to protect constitutional privacy interests or impose a constitutionally unnecessary burden on a criminal investigation." *Id.* And we rejected the defendant's contention that a sufficiently particular warrant must limit where on the computer officers may look to find the information described in the warrant. *Id.* at 216.

Ultimately, this court in *Mansor* determined that the affidavit in question had supplied probable cause that the defendant's computer would contain evidence of his internet search history from around the time that he had called 9-1-1, which would be relevant to the criminal investigation into the death of the defendant's son. *Id.* at 219. Given that probable cause, we determined that the warrant (informed by the affidavit) satisfied the particularity requirement because it described the information sought with sufficient specificity and limited the extent of the authorized search to no "broader than the supporting affidavit supplie[d] probable cause to justify." *Id.* (internal quotation marks omitted). We also concluded, however, that the actual forensic examination—that is, the execution of the warrant—had involved the review of information outside of the limited time period that the warrant had described. *Id.* at 221.

Accordingly, we turned to the question of whether the state could use information that it had discovered by searching beyond the scope of a lawful warrant. *Id.* at 220. We reiterated that "the purpose of rules requiring the suppression of evidence gathered in violation of the constitution is to restore the parties to the position they would have

been in had the violation not occurred." *Id.* at 221. And we explained that "the privacy interests underlying Article I, section 9, are best protected by recognizing a necessary trade-off when the state searches a computer that has been lawfully seized." *Id.* at 220. Thus, we concluded that, "when the state looks for other information or uncovers information that was not authorized by the warrant, Article I, section 9, prohibits the state from using that information at trial, unless it comes within an exception to the warrant requirement." *Id.* at 221; *see also* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex Tech L Rev 1, 24 (2015) (suggesting a "use restriction" for data that is "nonresponsive" to the search warrant). And because the warrant in *Mansor* had not authorized law enforcement to search for and recover "much of the *** voluminous material" discovered on the defendant's computer, we concluded that the state was prohibited from introducing that evidence against the defendant at trial and that the defendant's pretrial motion to suppress the evidence therefore should have been granted. *Id.* at 223.

Mansor significantly informs the two questions that we must resolve in this case: (1) whether the Court of Appeals correctly determined that six of the nine search categories in the warrant to search defendant's cell phone failed to describe the evidence sought with the particularity required by Article I, section 9; and (2) the extent to which the state is permitted to rely on any evidence that it obtained through the search of defendant's phone when—as the state concedes—some of the search categories failed to satisfy the particularity requirement. We turn next to the first of those questions.[9]

B. *Satisfaction of the Particularity Requirement*

As described more fully below, the warrant in question authorized law enforcement to search defendant's cell phone for nine separately numbered categories of digital data, and the Court of Appeals determined that six of those

[9] Unlike *Mansor*, this case does not involve the question whether execution of the warrant exceeded its defined scope.

nine search categories failed to satisfy the constitutional particularity requirement of Article I, section 9. The state challenges that conclusion only in part, because it concedes that the Court of Appeals correctly identified three of the search categories as deficient. But the state contends that the six other search categories satisfied the particularity requirement.

Focusing on the overbreadth and specificity concepts that inform the particularity analysis, the state proposes that the former ensures that the scope of the authorized search reaches no farther than the probable cause that supports the warrant and the latter requires that those executing the warrant can understand with a "reasonable degree of certainty" the information to be sought. The state relies on that formulation to support its contention that six of the nine search categories were sufficiently particular.

Defendant disagrees with the state's framing of the specificity component, and he urges us to conclude that a variety of specific details must be included when describing the evidence sought in a search for digital data. But he does not specifically challenge the conclusion that the Court of Appeals reached with respect to the particularity of the individual search categories. Instead, he contends that some of the categories that the Court of Appeals held were insufficiently particular were so constitutionally deficient that they effectively subsumed all the other categories and rendered the entire warrant unlawful. As we will explain, defendant's latter argument is one that conceptually fits with the second question that we address: the extent to which some unconstitutional search categories in the warrant required the trial court to suppress evidence obtained through the search that the warrant purported to authorize. Before reaching that question, we will resolve the parties' dispute regarding what particularity requires in the context of a search for digital data and determine which search categories satisfied the particularity requirement.

1. *The particularity analysis*

As set out above, the state proposes ways of understanding both the overbreadth and specificity concepts that inform our analysis of the constitutional particularity

requirement. We agree with the state's framing of the overbreadth requirement—that it ensures that the warrant is not purporting to authorize a search for evidence beyond what "the supporting affidavit supplies probable cause to justify." *Mansor*, 363 Or at 212 (internal quotation marks omitted). We also agree in part with the state's framing of the specificity requirement—that it ensures that the warrant's description of the information sought allows a reasonable officer to ascertain with a reasonable degree of certainty whether a particular item or piece of information falls within that scope. *See id.* at 219 (concluding that the warrant's description of information of internet search history for a specific date "informed those executing the warrant as to what they were to look for with a reasonable degree of certainty" (internal quotation marks omitted)).

But the state adds an additional proposition: that a warrant will be sufficiently specific *as long as* its description permits law enforcement to identify with a reasonable degree of certainty whether a given piece of data falls within the search category, *no matter how broad the scope of the description*. We disagree. As explained in *Mansor*, the specificity concept serves another, critically important purpose as to warrants to search for digital data: Beyond providing sufficient direction to law enforcement, specificity limits, at the outset, the enhanced risk of extensive governmental intrusion into a defendant's privacy interests that may occur when law enforcement collects and examines digital data to find the evidence described in the warrant. *See id.* at 215-16 (favorably quoting *Wheeler v. State*, 135 A3d 282, 305 (Del 2016), in which the Delaware Supreme Court concluded that a warrant purporting to authorize an unlimited examination of a defendant's digital media "paved the way for 'unconstitutional exploratory rummaging'").

That is, the requirement from *Mansor* that a warrant to search for digital data "must describe, with as much specificity as reasonably possible under the circumstances, *what* investigating officers believe will be found on the electronic devices," 363 Or at 216 (emphasis in original), serves to appropriately narrow the described scope of the search in two ways. First, it ensures that the description permits law enforcement exercising reasonable effort to identify with

a reasonable degree of certainty the information sought. Second, it limits the enhanced risk of extensive governmental intrusion by ensuring that that intrusion is as limited "as reasonably possible under the circumstances."[10] *Id.* at 218. The state's proposed test for specificity ignores the additional protection that *Mansor* requires for warrants to search for digital data.

Turning to defendant's arguments, we begin by observing that his underlying *premise* is correct: At its outset, a search for digital data inherently carries with it an enhanced risk of extensive governmental intrusion into personal privacy interests that are equal to, or even surpass, the privacy interest in one's home. *Mansor*, 363 Or at 222. That premise established the foundation for the framework set out in *Mansor*, which imposes the following requirement for specificity in the context of a search for digital data: The warrant "must describe the information the state seeks (the 'what') with as much specificity as reasonably possible under the circumstances, including, if available and relevant, a temporal description of when the information was created, accessed, or otherwise used." *Id.* And, of course, the warrant also must satisfy the "overbreadth" component: It must not authorize a search that is "broader than the supporting affidavit supplies probable cause to justify." *Id.* at 212 (internal quotation marks omitted).

But we are not persuaded by defendant's additional suggestion that a warrant to search for digital data be subject to "heightened" requirements, beyond those imposed in *Mansor*. In considering that argument, we first clarify that *Mansor* already imposed specificity requirements beyond those required for a conventional warrant to search a physical place: Unlike a warrant to search a physical place,

[10] We note that the specificity requirement may at times be conflated with the related concept of overbreadth—for example, a description that is insufficiently specific creates a risk that the description will be understood by officers to authorize a broader search than the probable cause supports. But that lack of a clear description is more precisely a specificity problem; rather than "authoriz[ing] a search that is broader than" probable cause would support, the lack of specificity creates ambiguity about the scope of the search that is authorized. *See Mansor*, 363 Or at 212 (describing those "related, but distinct, concepts" (internal quotation marks omitted)). Although the concepts are related, they are distinct and call for distinct analysis.

information that is the object of a search for digital data must be described "as specifically *as reasonably possible* in the circumstances," and that description *must* include, so long as "relevant and available, the time period during which that information was created, accessed, or otherwise used." *Id.* at 218 (emphasis added); *cf. Trax*, 335 Or at 603 (warrant to search a physical place "satisfies the particularity requirement if it permits the executing officer 'to locate with reasonable effort the premises to be searched'"; under the circumstances in *Trax*, the warrant at issue satisfied that requirement even though it could have been "more particularized" by specifying that another residence was located on the second floor of the house at issue (quoting *State v. Cortman*, 251 Or 566, 568-69, 446 P2d 681 (1968))).[11] As just explained, that heightened specificity standard serves to limit the enhanced risk of extensive governmental intrusion into personal privacy interests that is inherent in a search for digital data. *Mansor*, 363 Or at 222.

Although defendant acknowledges that standard from *Mansor*, he proposes that a description in a warrant to search for digital data must set out *all* available and pertinent limiting details, whether temporal or otherwise, given the extensive amount of data that is exposed to scrutiny when the warrant is executed. As explained, *Mansor* already requires that such warrants include available and pertinent limiting details—temporal or otherwise—in requiring that a warrant describe the evidence sought "as specifically as reasonably possible in the circumstances." *Id.* at 218. To the extent, however, that defendant proposes a reframing of the *Mansor* specificity test as a categorical requirement that a warrant to search for digital data incorporate *all* known and

[11] The warrant in *Trax* had "listed the street address of what turned out to be a multi-unit dwelling" and named the defendants as persons to be searched. 335 Or at 604. Because officers were able to learn which unit belonged to the defendants and "then searched only that residence," this court concluded that the warrant satisfied the particularity requirement. *Id.* The warrant in *Cortman* had named the defendant and identified his apartment building by street number, but had not specified an apartment number; however, the executing officer had known in which apartment the defendant resided and searched only that apartment. The court concluded that, because the officer had been able to execute the warrant "without straying into premises which he ha[d] no authority to enter," the warrant had not been fatally defective under the particularity requirement. 251 Or at 568-69.

pertinent details, we reject his proposed reframing. As this case aptly illustrates, what is or is not a pertinent or available detail is often in dispute and, in the end, a determination that often can be made only in hindsight. *See id.* at 216 (stating, in rejecting the notion that the description include a file type, that, "[g]iven the protean variety of factual settings in which such warrants are likely to be sought, it would be a fool's errand to set out, in the abstract, detailed guidelines for determining how specific the 'what' of the search must be to meet the particularity requirement" in the digital search context). More importantly, defendant's approach effectively would remove the concept of "reasonableness" in the circumstances, whenever an additional detail is later identified as "pertinent." That would run counter to the entire foundation of Article I, section 9—which, as explained above and also in *Mansor*, is grounded in reasonableness. *See id.* at 206-07 (providing that "'[t]he privacy interests protected from unreasonable searches under Article I, section 9, are defined by an *objective* test of whether the government's conduct would significantly impair an individual's interest in freedom from scrutiny, *i.e.*, [the individual's] privacy'" (quoting *Wacker*, 317 Or at 425 (first brackets in *Mansor*; some internal quotation marks omitted; emphasis added)).

Defendant relatedly argues that, given the nature of the intrusion that may occur during a search for digital data, the description in a warrant must provide sufficient direction "such that all officer discretion is eliminated" during the search. Again, however, that proposition is at odds with our emphasis in *Mansor* that the data sought on a digital device "may be located in any part of the digital media or organizational structure" and that "the location or form of specific information on a computer often cannot be known before the computer is actually examined." 363 Or at 198-99. Thus, "[a] forensic examiner who locates intentionally (or unintentionally) hidden information on a computer likely has responded to clues, followed instincts, and pursued many dead ends before being successful." *Id.* at 199. We added—as described above—that a magistrate reviewing a digital search warrant "would have little basis to make an informed decision" about "search protocols," *id.* at 200, and we rejected the defendant's contention that a sufficiently

particular warrant must constrain the examiner's discretion regarding where to look for the described information, *id.* at 216. We emphasized in *Mansor*, and we re-emphasize now, that warrants to search for digital data must describe the evidence sought with a heightened degree of specificity to satisfy the constitutional particularity requirement, but that specificity does not extend to limitations on how the search may be carried out.[12]

And *Mansor* itself illustrates that point. There, we concluded that the warrant to search the defendant's computer had identified with sufficient specificity the information sought: the defendant's internet search history for an identified date, based on an accompanying description that, during the 15 minutes before calling 9-1-1, he had searched online "what he should do" based on his son's physical condition. *Id.* at 189, 219. We did not require a more particularized description—such as, for example, the recitation of any particular search term—because, in the circumstances at hand, the description of internet search history in the identified timeframe had been sufficient to tell law enforcement executing the warrant "what they were to look for 'with a reasonable degree of certainty.'" *Id.* at 219 (quoting *Blackburn/Barber*, 266 Or at 35). We decline to adopt defendant's contrary rule that a warrant satisfies the particularity requirement only if it precludes officer discretion in the execution of the search.

In sum, we adhere to the standard announced in *Mansor*, as clarified above. To satisfy the particularity requirement, a warrant to search for digital data must describe the information sought "as specifically as reasonably possible in the circumstances." 363 Or at 218. That standard requires the warrant to include, if available and relevant, a temporal description of when the information was created, accessed, or otherwise used. *Id.* And it also requires that the warrant include, if available and relevant, other nontemporal limiting details—but, again, governed by a standard of reasonableness in the circumstances. Ultimately, to limit the

[12] Challenges to how a digital search was carried out, including claims that law enforcement examined more data than the scope of the search categories justified, are challenges to the execution of the warrant. But the execution of the warrant is not at issue here.

enhanced risk of extensive governmental intrusion into a defendant's privacy interests, the description in the warrant "must identify, as specifically as reasonably possible in the circumstances, the information to be searched for," *see id.* at 218, and the description must permit law enforcement, exercising reasonable effort, to identify the information sought with a reasonable degree of certainty. If the warrant describes the information sought with that degree of specificity, and if the supporting affidavit supplies probable cause to justify the described search, then the warrant satisfies the particularity requirement of Article I, section 9. *See id.* at 219-20 (applying that standard and concluding that the warrant to search for internet history from a specific date was not facially unlawful).

2. *Application*

Again, the Court of Appeals determined that six of the nine search categories described in the warrant to search defendant's cell phone failed to satisfy the constitutional particularity requirement, and the state disputes that conclusion as to three of those categories. Before analyzing those three search categories, we first briefly describe the three categories that the state concedes were unlawful, to illustrate more fully the application of the particularity requirement in the context of a warrant to search for digital data.

a. Second, seventh, and ninth search categories

The Court of Appeals concluded that the second, seventh, and ninth search categories lacked the specificity necessary to satisfy the particularity requirement. *Turay*, 313 Or App at 58-59. Those categories authorized the search for:

(2) "Evidence related to the relationship between [J, Gregg,] and/or [defendant]."

(7) "Any evidence related to the use of Uber or other ride-sharing or taxicab companies."

(9) "Any other evidence related to the crimes of Prostitution ***, Promoting Prostitution *** and/or Compelling Prostitution ***."

The state has not challenged the Court of Appeals' conclusions regarding those categories, but we offer a few observations.

The second category authorized the search for data "related to the relationship" between J, Gregg, "and/or" defendant. We agree with the Court of Appeals that the lack of any restriction "on the time or subject matter of the information that [was] sought" made that description "insufficient to apprise an executing officer of which information was or was not subject to the warrant." *Id.* As that court explained, the lack of a time limitation caused the search category to be "disconnected from the specific crime of investigation," and the phrase "evidence related to the relationship" describes a category "so broad that nearly anything could be contemplated." *Id.*[13]

The seventh category sought information from defendant's cell phone about any use of Uber, ride sharing, or taxicab companies, at any time, in any location, in any circumstance, and the ninth category sought "[a]ny other evidence" relating to prostitution-related crimes. As the Court of Appeals observed, those categories both failed to include "dates, subject matter limitations, or other parameters" that would have provided "a reasonable degree of specificity to an officer executing those commands"—despite the fact that more specific details about time periods and physical locations were known to the investigating detective. *Id.* at 59. We agree with the Court of Appeals that, as a result, both the seventh and ninth categories lacked the specificity necessary to satisfy the particularity requirement. And we further emphasize that the ninth search category failed to describe the evidence sought with *any* specificity—let alone with as much specificity as reasonably possible under the circumstances—so as to limit the enhanced risk of intrusion into defendant's privacy interests. *See Mansor*, 363 Or at 213-14 (rejecting a similar argument from the state that

[13] Although the Court of Appeals faulted the second category as "*so broad* that nearly anything could be contemplated," *Turay*, 313 Or App at 59 (emphasis added), we emphasize that the crux of that determination focused on a lack of specificity, not "overbreadth" in the sense that the description reached more broadly "than the supporting affidavit supplies probable cause to justify." *See Mansor*, 363 Or at 212 (internal quotation marks omitted).

a warrant that authorizes the search of a computer for "evidence of a particular crime" is, in itself, sufficiently specific).

b. First, fourth, and eighth categories

With the benefit of that illustration offered by the three search categories that more clearly failed to provide the required degree of specificity necessary to satisfy that component of the particularity requirement, we turn to the three search categories that are in dispute:

(1) "Any and all communications (voice, email, text, or otherwise) between [J, defendant,] and/or *** Gregg."

(4) "Any photos of [J, defendant, or Gregg] that show an association with prostitution including any profiting from prostitution."

(8) "Any evidence regarding the locations, including geolocation information, of the phones for a period of time from 06/15/2017 to 09/06/2017."

The state insists that all three search categories were sufficiently specific, but its arguments rely in part on its framing of the specificity requirement that we have rejected above. *See* 371 Or at 145 (rejecting the state's argument that a warrant will be sufficiently specific as long as its description permits law enforcement to identify with a reasonable degree of certainty whether a given piece of data falls within the search category, no matter how broad the scope of the description). Applying the standard that we have identified, we agree with the Court of Appeals that the first and eighth search categories did not satisfy the particularity requirement.

The first category describes the information sought as "[*a*]*ny* and all communications" between J, Gregg, and defendant, regardless of whether that communication was reasonably linked to evidence of the crimes of prostitution, promoting prostitution, or compelling prostitution. (Emphasis added.) As the Court of Appeals emphasized, the first category did not include any restriction "on the time or subject matter of the information sought." *Turay*, 313 Or App at 58. Given what officers knew about the criminal activity under investigation, the warrant could have more specifically described the first category of information sought as

limited to communications "involving prostitution related activities" or communications "that relate to internet postings or advertisements," but it did not.

Although the state insists that the first category "allowed a reasonable degree of certainty as to whether a given piece of data falls within its reach," we have emphasized that more is required in the context of a search for digital data. As we explained in *Mansor*, to ensure that the governmental intrusion into a defendant's privacy interests in digital data is as limited "as reasonably possible under the circumstances," the particularity requirement of Article I, section 9, requires a warrant to search digital data to "describe the information the state seeks (the 'what') with as much specificity as reasonably possible under the circumstances, including, if available and relevant, a temporal description of when the information was created, accessed, or otherwise used." 363 Or at 222.[14] Thus, as emphasized earlier in this opinion, even a description that provides sufficient direction to law enforcement may fail the specificity requirement if it does not limit the governmental intrusion as much "as reasonably possible under the circumstances." Because the first category did not restrict the search for communications with as much specificity as reasonably possible under the circumstances, it failed to satisfy the particularity requirement.

In addition, the first search category failed to satisfy the other component of the particularity requirement: By purporting to authorize a search for "[a]ny and all communications" between Gregg and defendant—whom the affidavit described as having been in a relationship that was not limited to illegal activity—the first search category authorized a search for information beyond the scope of what the affidavit supplied probable cause to justify. By contrast, the similar authorization to search for communications between

[14] We emphasize that *Mansor*'s description of the particularity requirement, when applied to warrants to search for digital data, assumes that the "intrusion"—the officer's acquisition of the proverbial "haystack" in which the needle will be found—will include "at least some information that is beyond the scope of the warrant," 363 Or at 220, but the scope of that intrusion is still limited by the requirement that the information sought must be described with as much specificity "as reasonably possible in the circumstances." *Id.* at 218.

either Gregg *or* defendant and J stayed within the scope supported by probable cause because, viewed as a whole, the affidavit described essentially the sole reason for the relationships—and thus, communications—between J and defendant, and between J and Gregg, to be for the purpose of engaging in prostitution-related activities.[15]

We also agree with the Court of Appeals that the eighth search category—evidence regarding the locations, including geolocation information, of defendant's cell phones for a defined period of time—failed to describe the information sought with sufficient particularity. *Turay*, 313 Or App at 59-60. Of course, that description did include a general temporal limitation—the 12-week period in which J had known Gregg and defendant. And it did provide a description of the *type* of information sought—evidence of location, including geolocation, of defendant's phone during that time frame. But describing the information sought as "*any* evidence regarding" the phone's location over a 12-week period nonetheless omitted additional limiting factors that were known to law enforcement. Given the nature of the activity being investigated—prostitution activity—and officers' suspicion as to where that activity was taking place, the warrant should have limited the scope of the search for location information to align with where officers suspected the prostitution activity to have occurred. Stated another way, in the circumstances here, the warrant did not describe the eighth category of evidence "as specifically as reasonably possible in the circumstances," because it did not limit the enhanced risk of extensive intrusion into defendant's

[15] The affidavit described that J met Gregg about 12 weeks before defendant's arrest; that Gregg had introduced J to defendant and to prostitution, including how to post advertisements online; that online advertisements had included a photograph of J and Gregg, posing in front of a car that resembled the car that defendant had been driving on the day of his arrest; that J had earned most of her money engaging in prostitution by going on "duo" engagements with Gregg; that Gregg took and kept the money that they made together and that J assumed that Gregg later gave the money to defendant; that the three had lived together for a time at Gregg's home, with many of J and Gregg's prostitution engagements occurring there; that J "[did] prostitution dates" for defendant; and that, at the time of his arrest, defendant had been holding funds that J had earned from a recent engagement. Thus, the first category, although insufficiently specific, was not overbroad with regard to communications between J and defendant and between J and Gregg.

privacy interests that would occur upon execution of the warrant.[16]

We agree with the state, however, that the Court of Appeals erred in concluding that the fourth search category—any photos of J, defendant, or Gregg that showed an association with prostitution, including any profiting from prostitution—did not satisfy the particularity requirement. The Court of Appeals concluded, as to specificity, that the "vague phrase 'association with prostitution including profiting from prostitution'" provided "little, if any guidance" to law enforcement about data that reasonably could be expected to be found on defendant's cell phone. *Turay*, 313 Or App at 63. But that phrasing—while not ideal—set out with as much specificity as reasonably possible in the circumstances the information that law enforcement believed would be found on defendant's cell phone. By its nature, the word "prostitution" narrowed the evidence sought to only photos that suggested prostitution-related activities (or related profiting activities), not merely sexually explicit photos of any sort. And, as noted, that description narrowed the range of photos sought to those of only the three individuals extensively described in the affidavit—J, Gregg, and defendant. In the circumstances, that description provided sufficient direction to law enforcement and limited the enhanced risk of intrusion into defendant's personal privacy interests, and thus was sufficiently specific. And, because that description also was within the scope of the probable cause that the affidavit supported, it satisfied the particularity requirement.

c. Summary of particularity requirement analysis

In sum, the following aspects of the warrant to search defendant's cell phone either satisfied the constitutional particularity requirement, or were determined to satisfy that requirement by the Court of Appeals with no challenge on review:

[16] The state contends that, in assessing the eighth described category as unduly broad, the Court of Appeals may have been more concerned with overbreadth than specificity. But we do not read the Court of Appeals' decision as concluding that the eighth category fell short as to overbreadth; rather, the Court of Appeals concluded—and we agree—that the wide-ranging scope of information described fell short on specificity. *See Turay*, 313 Or App at 59 ("The eighth command *** likewise *lacks specificity*[.]" (Emphasis added.)).

(3) "Evidence regarding any communications (voice, email, text, or otherwise) involving prostitution related activities."

(4) "Any photos of [J, defendant, or Gregg] that show an association with prostitution including any profiting from prostitution."

(5) "Images, videos and/or data which depict [J or Gregg] in sexually explicit positions or conduct that relate to internet postings or advertisements."

(6) "Any evidence related to use of internet sites associated with prostitution, including [the website] for a period of time 06/15/2017 to 09/06/2017."

By contrast, the following fell short:

(1) "Any and all communications (voice, email, text, or otherwise)" between [J, defendant,] and/or *** Gregg."

(2) "Evidence related to the relationship between [J, Gregg], and/or [defendant]."

(7) "Any evidence related to the use of Uber or other ride-sharing or taxicab companies."

(8) "Any evidence regarding the locations, including geolocation information, of the phones for a period of time from 06/15/2017 to 09/06/2017."

(9) "Any other evidence related to the crimes of Prostitution (ORS 167.007), Promoting Prostitution (ORS 167.012) and/or Compelling Prostitution (ORS 167.017)."

We turn next to the second question presented in this case: Whether Article I, section 9, requires suppression of the challenged evidence because some—but not all—of the search categories were insufficiently particular.

C. *The Extent to which Article I, section 9, Prohibited the State from Using Evidence Obtained through Execution of the Search Warrant*

Ordinarily, a search that is "performed under authority of a warrant" is "subject to a presumption of regularity, and the party challenging the evidence bears the burden to prove the unlawfulness of the search or seizure." *State v. Unger*, 356 Or 59, 75, 333 P3d 1009 (2014). Conversely,

when no part of a search warrant satisfies the particularity requirement, then any search pursuant to that warrant is unlawful. *See Blackburn/Barber*, 266 Or at 35 (explaining that, when a warrant "is sufficiently ambiguous that it is impossible to identify with a reasonable degree of certainty the particular premises authorized to be searched, the warrant may not be executed and any search pursuant to it is illegal"). But we have yet to confront the question that is the primary focus of the parties' dispute in this case: the extent, if any, to which evidence obtained in a search performed pursuant to a warrant can be considered lawfully obtained when the warrant combined some search categories that satisfied the constitution's particularity requirement with others that did not. The parties propose different rules for determining what a court must do to address the constitutional violation in this case. Both primarily argue that we should determine from an examination of the warrant itself whether the challenged evidence must be suppressed, although both advance alternative arguments in the event that we are not persuaded that the suppression dispute can be resolved on the basis of the warrant alone.

According to the state, under a "mixed warrant" of this type, Article I, section 9, requires suppression of only evidence that falls outside the scope of any lawful search category. In other words, the state effectively argues that the single warrant should be treated as though the state had sought and executed two warrants—one entirely lawful—and that any evidence falling within the scope of the lawful warrant should be treated as though it had been obtained pursuant to a lawful search. The state describes that approach as turning on an objective inquiry that compares the nature of the evidence obtained to the terms of the warrant, without regard to how the warrant in fact was executed. The state contends that the most damaging of the challenged evidence at defendant's trial—incriminating photographs of J and extraction reports that set out incriminating text messages between defendant's phone and a contact determined to be J—all fell within the scope of search categories that describe the evidence sought with sufficient particularity: the third (evidence regarding any communications

involving prostitution-related activities); the fourth (photos of J, defendant, or Gregg showing an association with prostitution, including profiting therefrom); and the fifth (images depicting J or Gregg in sexually explicit positions or conduct relating to internet postings or advertisements). And the state further argues that any other text message evidence admitted at trial was either substantively harmless or cumulative considering similar unchallenged evidence obtained from J's cell phone.

According to defendant, however, it is irrelevant that some search categories may have described evidence with sufficient particularity, because the unlawful "catch-all" categories—including the second, which sought "[e]vidence related to the relationship between [J, Gregg,] and/or [defendant]," and the ninth, which authorized a search for "any other" evidence of prostitution—allowed such an extensive invasion of his privacy that the warrant was entirely invalid. As a result, defendant contends, the entire search of his phone was unlawful, and all evidence obtained from his phone must be suppressed.

As we will explain, however, neither party's argument is entirely consistent with this court's prior decisions under Article I, section 9, which—in cases involving some established constitutional violation—have determined what evidence must be suppressed by considering how and why that evidence was discovered. *See, e.g.*, *State v. DeJong*, 368 Or 640, 642, 497 P3d 710 (2021) (explaining that, if there is a "minimal factual nexus" between a constitutional violation and the challenged evidence, then the state must "establish that the challenged evidence was untainted by" that violation).

1. *The state's proposal*

The state's argument that evidence is lawfully obtained if it falls within the scope of a lawful search category relies, to a significant extent, on a passage from *Mansor*, mentioned earlier, in which this court required a restriction on the "use" of digital data obtained during a search pursuant to a warrant. In *Mansor*, we explained that, "when the state conducts a reasonably targeted search of a person's computer for information pursuant to a warrant that

properly identifies the information being sought, the state has not unreasonably invaded the person's privacy interest." 363 Or at 221. In such circumstances, we continued, "the state may use the information identified in the warrant in a prosecution or any other lawful manner." *Id.* "But when the state looks for other information or uncovers information that was not authorized by the warrant, Article I, section 9, prohibits the state from using that information at trial, unless it comes within an exception to the warrant requirement." *Id.* The state characterizes that aspect of *Mansor* as imposing a "use" restriction that permits the state to "use" (*i.e.*, admit against a defendant) any evidence obtained through a search supported by a lawful warrant.

But *Mansor* did not answer the question with which we are presented in this case, because the search in *Mansor* was based on a warrant that lawfully authorized a search for a single category of evidence, not one that included a lawful search category combined with an unlawful category. The approach that this court adopted in *Mansor* resolved the tension between the principle that it is "lawful and appropriate" for the state to conduct "a reasonably targeted search of a person's computer for information pursuant to a warrant that properly identifies the information being sought," and the practical reality that even reasonably targeted searches pursuant to a warrant "necessarily may require examination of at least some information that is beyond the scope of the warrant." *Id.* at 220-21. Under those circumstances, the state has not violated a defendant's rights under Article I, section 9, and, therefore, "the state may use the information identified in the warrant in a prosecution or any other lawful manner." *Id.* at 221. In that context, we imposed a limitation on the state's use of evidence out of recognition that, although a warrant to search for digital data may be lawful, the execution of that lawful warrant might require the examination of some information that is beyond the scope of the warrant and invades the individual's privacy interests. *Id.* at 220-21.

Unlike *Mansor*, in which this court fashioned a rule to address the possibility that the defendant's privacy may be lawfully invaded during the course of "a reasonably targeted search" based on an entirely lawful warrant, this case requires

a rule that addresses the certainty that defendant's privacy was unlawfully invaded during the course of a search that was based on a warrant that contained multiple unlawful search categories. Importantly, as we explained in *Mansor*, "the purpose of rules requiring the suppression of evidence gathered in violation of the constitution is to restore the parties to the position they would have been in had the violation not occurred." *Id.* at 221; *see also State v. Davis*, 295 Or 227, 237, 666 P2d 802 (1983) (explaining that the "rules of law designed to protect citizens against unauthorized or illegal searches *** are to be given effect *** by restoring the parties to their position as if the state's officers had remained within the limits of their authority").

Here, as noted at the outset, the trial record contained only minimal evidence about how the actual forensic examination of defendant's cell phone—that is, the execution of the search itself, pursuant to the warrant—had been conducted. For example, the record showed that data had been extracted using forensic examination software, but it did not establish the nature or extent of that extraction: It did not establish whether all data was extracted initially or whether various extraction steps were taken, and, if so, what those steps were. And, although the record showed that the software had permitted law enforcement to extract certain photographic images and to retrieve the two extraction reports showing text messaging between defendant and J, it did not show which categories of evidence the state was looking for when that incriminating evidence was discovered. Thus, we have no basis on which to conclude that simply ignoring the unlawful search categories would restore defendant to the position that he would have been in had the violation not occurred. Moreover, the state's focus on the scope of the lawful search categories could allow it to offer evidence against defendant that may actually have been the product of a constitutional violation—but Article I, section 9, prohibits that result.

2. *Defendant's proposal*

Defendant's argument for categorically suppressing all evidence found on his cell phone is equally problematic. His argument rests on the premise that the unlawful search

categories in the warrant to search his cell phones were so permissive and lacking in specificity that they "subsumed" the lawful categories, resulting in a prohibited "general warrant." Under those circumstances, defendant argues, Article I, section 9, requires us to treat the warrant as invalid *in toto* and to suppress all evidence obtained during the search pursuant to the warrant. Defendant relies on our statement in *Mansor* that, without specificity, digital searches "raise the possibility of computer search warrants becoming the digital equivalent of general warrants and of sanctioning the undue rummaging that the particularity requirement was enacted to preclude." 363 Or at 220 (internal quotation marks omitted). And he insists that invalidating the entire warrant must be the answer because, otherwise, the state could "write and execute a general warrant in every instance, secure in the knowledge that the inclusion of a narrower [search category] will 'save' the warrant."

We agree with defendant only in part. As discussed above, the first, second, seventh, eighth, and ninth search categories were insufficiently particular to satisfy Article I, section 9. The Court of Appeals concluded that the second search category—"[e]vidence related to the relationship between [J, Gregg,] and/or [defendant]"—"amount[ed] to a general warrant for a search of anything incriminating." *Turay*, 313 Or App at 59. And defendant contends that a similar criticism could be leveled at the ninth search category, which authorized an unlawful search for "[a]ny other evidence" of prostitution crimes. Whether or not "general warrant" is the correct label, those search categories unquestionably—and unlawfully—allowed the "undue rummaging that the particularity requirement was enacted to preclude." *Mansor*, 363 at 220. And, had the warrant included *only* those insufficiently particular search categories, there would be no question that the entire search was unlawful. *See, e.g.*, *Blackburn/Barber*, 266 Or at 35 (explaining that, when a warrant fails to describe premises to be searched with sufficient particularity, "any search pursuant to it is illegal").

As the state correctly observes, however, the warrant in this case also included several lawful search categories.

We have rejected the state's contention that it is possible to simply ignore the violation that occurred when the state searched defendant's cell phone for digital data that the warrant failed to describe with sufficient particularity. But, given the focus of Oregon's exclusionary rule on restoring defendants to the position that they "would have been in had the violation not occurred[,]" *Mansor*, 363 Or at 221, it is appropriate to consider what remedy Article I, section 9, would require if the state had not combined the lawful and unlawful search categories in the same warrant. Had the state, hypothetically, obtained two warrants—one containing only the sufficiently particular search categories—then the entire search performed under that hypothetical warrant would have been presumptively lawful, and the only question would be whether any other circumstance had rendered the search unlawful. *See State v. Walker*, 350 Or 540, 554, 258 P3d 1228 (2011) (describing shifting inquiry). Additionally, the constitutional violation that occurred when the state searched defendant's cell phone in an effort to find evidence that no lawful category of the warrant authorized it to search for might well require suppression of all evidence obtained pursuant to that warrant, but it would not necessarily require suppression of evidence obtained from the same phone pursuant to the sufficiently particular warrant.

In this case, of course, the state did not obtain two warrants; it obtained a single warrant containing both the sufficiently particular search categories and the other categories that fell constitutionally short of authorizing a lawful search. But we are not persuaded that the mixing of the lawful and unlawful search categories in the same warrant necessarily changes the analysis. The unlawful invasion of defendant's protected privacy interest is not necessarily greater than if the state had searched his cell phone pursuant to two separate warrants, and the remedy that is required to restore defendant to the position that he "would have been in had the violation not occurred[,]" *Mansor*, 363 Or at 221, also is not necessarily greater. Thus, we are not persuaded by defendant's contention that all evidence found on his phone necessarily must be suppressed as a result of the warrant's inclusion of search categories that unlawfully allowed the "undue rummaging that

the particularity requirement was enacted to preclude." *Id.* at 220 (internal quotation marks omitted); *see also* Wayne R. LaFave, 2 *Search and Seizure: A Treatise on the Fourth Amendment* § 4.6(f) (6th ed 2022) ("[I]t would be harsh medicine indeed if a warrant issued on probable cause and particularly describing certain items were to be invalidated *in toto* merely because the affiant and magistrate erred in seeking and permitting a search for other items as well.").

3. *What Article I, section 9, requires*

As our rejection of defendant's categorical rule suggests, to determine the extent to which evidence must be suppressed as the product of a constitutional violation, our case law directs us to consider what actually transpired. The Court of Appeals recognized that the question of suppression in this case ultimately turns on how the search in fact was executed. *See Turay*, 313 Or App at 66 (remanding for "development of a record as to how the forensic search of the phone was conducted"). But it reached that conclusion after applying "severability" principles and concluding that the unlawful search categories could be "severed" from the warrant and the remaining categories saved. *See id.* at 63-64. That is an approach that the Court of Appeals has long followed when considering warrants that contain a mix of sufficiently particular and insufficiently particular categories. *See, e.g.*, *id.* at 63 ("Ordinarily, '[i]f a portion of a search warrant fails to describe the items sought with sufficient particularity, that portion may be excised and the balance of the warrant upheld.'" (Quoting *State v. Vermaas*, 116 Or App 413, 416, 841 P2d 664 (1992), *rev den*, 316 Or 142 (1993) (brackets in *Turay*))). The import of that approach is that the "balance of the warrant" containing the lawful search categories is upheld and the search pursuant to those search categories considered lawful. *Turay*, 313 Or App at 63; *see also State v. Burnham*, 289 Or App 783, 785, 412 P3d 1233 (2018) (trial court "did not err by admitting evidence covered by the valid portions of the warrant").

This court has not yet addressed whether to adopt the "severance" doctrine at all, let alone in the context of warrants to search for digital data. And we decline to do so

in this case, because—as we will explain—our existing case law does not permit us to presume that the state lawfully obtained any evidence through the search of defendant's cell phone.

Under our Article I, section 9, case law, if an evidentiary dispute involves both a warrant-based search and unlawful police conduct, the first question is whether the defendant can "establish a minimal factual nexus between [a constitutional violation] and the challenged evidence"; if so, then the second question is whether the state can "establish that the challenged evidence was untainted by" the constitutional violation. *DeJong*, 368 Or at 642. In other words, when the defendant establishes a minimal factual nexus between a constitutional violation and challenged evidence that was obtained pursuant to a warranted search, there is a presumption that the challenged evidence must be suppressed, but the state has the opportunity to rebut that presumption. *State v. Johnson*, 335 Or 511, 520, 73 P3d 282 (2003) (endorsing federal approach that shifts the burden to the government to prove that challenged evidence is "untainted" by a constitutional violation, when the defendant establishes a "factual nexus between the unlawful police conduct and the challenged evidence" (internal citations omitted)).

For example, in *Johnson*, after a trial court had ruled that the state had unlawfully seized items of clothing belonging to the defendant, the state responded by obtaining a warrant authorizing it to seize and analyze the same clothing, and the defendant moved to suppress. 335 Or at 514-15. We acknowledged the "oft-cited rule that, when state agents have acted under authority of a warrant, the burden is on the party seeking suppression," but we held that the "presumption of regularity" that is ordinarily afforded to a warrant-based search "is undermined" when a defendant is able to show that evidence obtained during the search "is connected to some prior governmental misconduct." *Id.* at 520-21. And we concluded that the defendant in *Johnson* had shown the requisite factual nexus between the evidence and the original unlawful seizure. *Id.* at 521. But we did not conclude that the unlawful seizure inherently tainted the later seizure of the same evidence. Instead, we accepted the state's proposition that the defendant's clothes

would not be subject to suppression if the state proved that "the warrant that the police ultimately obtained truly was independent of the earlier illegal seizure," although we ultimately affirmed the trial court's finding that the state's evidence was not sufficiently persuasive. *Id.* at 522, 526.

We applied that "minimal factual nexus" approach more recently in *DeJong*, which involved a lawful search based on a warrant that law enforcement had obtained after unlawfully seizing the defendant's home and speaking with another resident. 368 Or at 643-44. We reiterated that the "[d]efendant's burden of establishing a factual nexus is *minimal* and intended merely to rebut the presumption of regularity attendant to warranted searches." *Id.* at 654-55 (emphasis in original). And we concluded that the defendant in *DeJong* had met that minimal burden by showing that the unlawful seizure of her residence had allowed officers to obtain statements from the other resident, which they then had used to obtain the warrant. *Id.* Given that nexus, we considered whether the state had met its burden to establish that the evidence it discovered during the search pursuant to the warrant "was untainted by the preceding unlawful seizure of defendant's residence," but we ultimately concluded that the state's evidence was legally insufficient to permit a finding that it had met its burden. *Id.* at 656, 659. Accordingly, Article I, section 9, required suppression of the evidence. *Id.*

Those principles are applicable to this case. Admittedly, there are factual differences between cases applying the "minimal factual nexus" test, where the constitutional violation preceded the lawful warranted search, and the search of defendant's cell phone here, which was conducted pursuant to a warrant that included unlawful search categories. But we are not persuaded that those potential chronological distinctions alter the relevance of the minimal factual nexus test. As in cases describing that test, the state here obtained a warrant supported by probable cause to conduct the search at issue, but it also violated defendant's Article I, section 9, rights when it extracted and examined data from defendant's phone in an effort to find evidence that no lawful category of the warrant authorized it to search for. Accordingly, we will not presume that any of the evidence was lawfully obtained, so long as defendant

has established a minimal factual nexus between that constitutional violation and the challenged evidence.

4. *Application of the minimal factual nexus test*

As we explained in *DeJong*, the defendant's "burden of establishing a factual nexus is *minimal* and intended merely to rebut the presumption of regularity attendant to warranted searches." 368 Or at 654-55 (emphasis in original). Accordingly, the threshold question asks only if the defendant has shown "that the evidence obtained 'is *connected to* some prior governmental misconduct.'" *Id.* at 651 (quoting *Johnson*, 335 Or at 521 (emphasis in *DeJong*)). We emphasized that "satisfying that minimal standard does not require a defendant to identify and produce evidence related to discrete factual theories connecting the unlawful conduct with the challenged evidence." *Id.* at 655.

Applying those principles here, it is apparent that there is a minimal factual nexus between the constitutional violation and the challenged evidence, because the state found the evidence during the execution of a single search warrant that purported to authorize the state to extract and examine data from defendant's cell phone in an effort to find evidence that it had no lawful authority to search for. In other words, given the nature of a search for digital data, everything obtained from defendant's phone is connected—to some extent—to the search categories described in the warrant, some of which purported to authorize unconstitutional "rummaging" through the data on that phone. *See Mansor*, 363 Or at 220. Those unlawful categories included "[e]vidence related to the relationship between [J, Gregg,] and/or [defendant]" and "[a]ny other evidence" of prostitution-related crimes, and those descriptions could easily apply to the incriminating images and text messages that the state introduced below. Thus, the execution of the warrant establishes as much connection as can be identified absent evidence of how the search actually was conducted. As only the state is in a position to know how the search actually was conducted, we conclude that defendant has established the minimal factual nexus required to shift the burden to the state to demonstrate that the challenged evidence was untainted by the constitutional violation.

5. *The proper disposition*

Ordinarily, our conclusion that there is a minimal factual nexus between the constitutional violation and the challenged evidence would take us to the next step set out in *DeJong* and *Johnson*: a determination whether the state met its burden to establish that the challenged evidence was untainted by the constitutional violation. It is undisputed, however, that the existing record precludes a resolution of that question, because the record contains no evidence regarding how the unlawful search categories in the warrant affected the data that the state extracted from defendant's cell phone.

The Court of Appeals concluded that the proper disposition was a "remand for development of a record as to how the forensic search of the phone was conducted." *Turay*, 313 Or App at 66. And it explained that the question on remand was whether the challenged evidence "was discovered while police were executing one of the lawful search commands as opposed to one of the invalid commands." *Id.* Both aspects of that remand instruction are in dispute.

The state understands the Court of Appeals to have held that the evidence must be suppressed unless the state can demonstrate that it, in fact, separately executed a search for each category of evidence and actually obtained the challenged evidence while executing a search for one of the sufficiently particular categories. At oral argument, the state insisted that that test is too limited and reflects a misunderstanding of how digital search warrants are executed.

Defendant, on the other hand, agrees with the Court of Appeals that any factual inquiry on remand should be limited to whether the state can show that it actually discovered the evidence while police were executing one of the lawful search categories. But he primarily contends that this court should reverse *without* remanding, because he insists that the state had the opportunity to develop a record below and should not be given another opportunity on remand.

We turn first to the question that will affect future similar cases—whether evidence collected during the execution of a warrant that, in part, failed to satisfy the

particularity requirement must be suppressed unless the state can prove that it in fact separately executed the lawful search categories of the warrant and discovered the challenged evidence while executing one of the lawful search categories. We agree with the state that the remand instruction from the Court of Appeals unduly constrains how the state may meet its burden to avoid suppression. As explained above, when there is a minimal factual nexus between a constitutional violation and evidence found pursuant to a search warrant, the evidence must be suppressed unless the state can "establish that the challenged evidence was untainted by" the constitutional violation. *DeJong*, 368 Or at 642. Here, as explained above, the constitutional violation was the state's extraction and examination of data from defendant's cell phone in an effort to find evidence that no lawful category of the warrant authorized it to search for, and that violation bears a minimal factual nexus to all the evidence found on defendant's phone. Thus, unlike *Mansor*, in which the warranted search had involved no constitutional violation, all evidence found on defendant's phone *presumptively* must be suppressed. And the state can avoid suppression only by establishing that the challenged evidence is untainted by the constitutional violation. It may be, as the Court of Appeals reasoned, that the state can meet its burden in cases like this—involving warrants to search for digital data—only with proof that the challenged evidence in fact "was discovered while police were executing one of the lawful search commands as opposed to one of the invalid commands." *Turay*, 313 Or App at 66. But it is premature to predict whether that is the *only* showing that will satisfy the state's burden of proof, and we decline to do so.[17]

The remaining question is whether the state should be afforded the opportunity on remand to develop a factual record on the question whether the challenged evidence was

[17] We understand the state to have expressed concern that the manner in which warrants to search for digital data are executed could make it difficult for the state to show that a particular search category did not affect the discovery of particular evidence. If that continues to be true, then it is particularly important that law enforcement avoid requesting, and magistrates avoid issuing, warrants that include the kind of search categories that the state now concedes were insufficiently particular.

untainted by the constitutional violation. We agree with the Court of Appeals, as a general matter, that that is the appropriate disposition in this case. Although defendant contends that the state already has had the opportunity to develop a record and is not entitled to an additional opportunity, defendant's arguments in the trial court contended only that the warrant was unlawful in its entirety. The possibility that the warrant may have contained some lawful search categories, and that those lawful categories might allow the state to rely on some of the challenged evidence, arose following issuance of the Court of Appeals decision. Those are issues that this court has not previously addressed. And, in addressing them now, we have held for the first time that the unlawful search categories establish that all the challenged evidence is presumptively a product of the constitutional violation as to particularity, but that defendant is not entitled to suppression if the state can prove that the challenged evidence was untainted by that violation. In other words, given defendant's arguments in the trial court, questions about how the search was or would have been conducted were irrelevant. Neither party had the opportunity below to address the standard that we have now identified as governing whether the challenged evidence must be suppressed when a warrant contains some search categories that satisfy the particularity requirement and others that do not. And neither party was alerted to the need to create a factual record to determine whether, under that standard, the evidence must be suppressed. Thus, it is appropriate to remand for the trial court to determine which, if any, of the challenged evidence must be suppressed under Article I, section 9. *See State v. Mills*, 354 Or 350, 373-74, 312 P3d 515 (2013) (after overruling prior case law that had required the state to prove venue of the offense beyond a reasonable doubt, court remanded to afford both parties the opportunity to present evidence on the question of the appropriate venue).

III. CONCLUSION

We conclude that five of the nine search categories in the warrant to search defendant's cell phone unlawfully authorized a search for evidence that was not described with sufficient specificity to satisfy the particularity requirement set out in Article I, section 9, and paved the way for

unconstitutional exploratory rummaging, including for "[a]ny other evidence" of prostitution crimes. We also conclude that there was a minimal factual nexus—between the state's extraction and examination of data from defendant's phone in an effort to find evidence that no lawful category of the warrant authorized it to search for, and all evidence found during the search—that requires the evidence obtained through the search to be suppressed, unless the state can prove that that evidence was untainted by the constitutional violation. Those conclusions require us to reverse the decision of the trial court. And, given the procedural circumstances of this case, we conclude that it is appropriate to remand for the development of a factual record, and for the trial court to make findings, regarding the standard that we have articulated.

The decision of the Court of Appeals is affirmed in part and reversed in part. The judgment of the circuit court is reversed, and the case is remanded to the circuit court for further proceedings.

DUNCAN, J., concurring.

I concur in the majority's opinion, which concludes that the warrant in this case includes invalid search categories and remands the case to the trial court for further proceedings. I write separately to highlight the law relevant on remand.

Article I, section 9, of the Oregon Constitution protects individuals against unreasonable government searches and seizures, and it requires that warrants be based on "probable cause" and "particularly describ[e] the place to be searched, and the person or thing to be seized."

This case concerns Article I, section 9's particularity requirement in the context of searches for digital information, a subject that this court addressed in *State v. Mansor*, 363 Or 185, 421 P3d 323 (2018). As we explained in *Mansor*, "[o]ur cases have identified two related, but distinct, concepts that inform the particularity analysis—specificity and overbreadth." *Id.* at 212. "A warrant must be sufficiently specific in describing the items to be seized and examined

[so] that the officers can, 'with reasonable effort ascertain' those items to a 'reasonable degree of certainty.'" *Id.* (quoting *State v. Blackburn/Barber*, 266 Or 28, 35, 511 P2d 381 (1973)). "But, even if the warrant is sufficiently specific, it must not authorize a search that is 'broader than the supporting affidavit supplies probable cause to justify.'" *Mansor*, 363 Or at 212 (quoting *State v. Reid*, 319 Or 65, 71, 872 P2d 416 (1994)).

In addition, warrants to search computers or other digital devices are subject to a heightened specificity requirement: They must "identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including if relevant and available, the time period during which the information was created, accessed, or otherwise used." *Mansor*, 363 Or at 218. That heightened specificity requirement exists because of the unique characteristics of computers and other digital devices, which contain vast amounts of data of different types and on different subjects. *Id.* at 201-02 (describing unique characteristics of computers and other digital devices, including cell phones); *see also id.* at 202 (quoting *Riley v. California*, 573 US 373, 396-97, 134 S Ct 2473, 189 L Ed 2d 430 (2014), for the proposition that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is" (emphasis in original).).

Not only are warrants to search computers or other digital devices subject to a heightened specificity requirement, there is a limit on what information resulting from the execution of such warrants can be used by the state. *Mansor*, 363 Or at 220-23. As we explained in *Mansor*, as a result of the way that information is stored on digital devices, officers executing a search warrant may have to examine digital information to determine whether it is the type specified in the warrant. *Id.* at 217-18. To account for that possibility, the state is not allowed to use evidence found during a search of a digital device "unless a valid warrant authorized the search for that particular evidence, or it is admissible under

an exception to the warrant requirement." *Id*. at 188; *id*. at 221. As we explained,

> "the privacy interests underlying Article I, section 9, are best protected by recognizing a necessary trade-off when the state searches a computer that has been lawfully seized. Even a reasonable search authorized by a valid warrant necessarily may require examination of at least some information that is beyond the scope of the warrant. Such state searches raise the possibility of computer search warrants becoming the digital equivalent of general warrants and of sanctioning the 'undue rummaging that the particularity requirement was enacted to preclude.' [*State v.*] *Mansor*, 279 Or App [778,] 803[, 381 P3d 930 (2016)] (internal quotation marks omitted). Although such searches are lawful and appropriate, individual privacy interests preclude the state from benefiting from that necessity by being permitted to use that evidence at trial. *We thus conclude that the state should not be permitted to use information obtained in a computer search if the warrant did not authorize the search for that information, unless some other warrant exception applies*."

Mansor, 363 Or at 220-21 (emphasis added). Thus, under *Mansor*, even if a warrant is valid, the state may not use digital information obtained as a result of the execution of the warrant unless the warrant authorized the search for "that particular evidence" or the evidence "is admissible under an exception to the warrant requirement." *Id.* at 188.

Unlike *Mansor*, this case involves a warrant with invalid search categories. As the majority states, several of the search categories "failed to satisfy the constitutional particularity requirement and, thus, *** those categories failed to authorize a lawful search." 371 Or at 130. Nevertheless, *Mansor* is relevant, because it establishes the requirements that must be satisfied in order for evidence obtained pursuant to a warrant to be admissible when all of the search categories are valid, and the requirements cannot be lower for a warrant that contains invalid search categories. Thus, on remand, the trial court cannot admit any evidence derived from the execution of a warrant unless the warrant "authorized the search for that particular evidence, or it is admissible under an exception to the warrant requirement." *Mansor*, 363 Or at 188.

Consequently, on remand, the only evidence that the trial court could possibly admit is evidence that satisfies *Mansor*; that is, evidence that was either (1) particularly described by a valid search category and discovered during a "reasonably executed" search, *id.* at 218 n 15, or (2) is admissible under an exception to the warrant requirement. Moreover, even if the evidence satisfies *Mansor*, it must also satisfy the additional requirement established by the majority's opinion in this case. As the majority concludes, because the warrant contained invalid search categories, evidence obtained as a result of the execution of the warrant is inadmissible unless the state can prove that the evidence is not tainted by those invalid search categories. 371 Or at 166-67.

When determining whether the evidence is tainted, the court should consider, among other things, how the evidence was discovered, including whether the evidence was discovered during, after, or otherwise as a result of a search for evidence in one of the invalid search categories. *Id.* at 161-62 (stating that the searches conducted pursuant to the invalid search categories would be unauthorized); *see Mansor*, 363 Or at 221 ("'[R]ules of law designed to protect citizens against unauthorized or illegal searches or seizures of their persons, property, or private effects are to be given effect by denying the state the use of evidence secured in violation of those rules against the persons whose rights were violated, or, in effect, by restoring the parties to their position as if the state's officers had remained within the limits of their authority.'" (Quoting *State v. Davis*, 295 Or 227, 237, 666 P2d 802 (1983) (brackets in *Mansor*).)). Thus, as the Court of Appeals explained in this case, "[o]n remand, the parties can further address the manner in which this warrant was executed and trace the discovery of the evidence that is the subject of defendant's motion to suppress," to determine what evidence was lawfully discovered. *State v. Turay*, 313 Or App 45, 66, 493 P3d 1058 (2021).

In addition to determining how the evidence was discovered, the trial court should consider whether the warrant was intended to be, or was used as, a warrant akin to a "general warrant," which Article I, section 9, was meant to prohibit. *Blackburn/Barber*, 266 Or at 34 (stating that "the

historical motivation for [Article I, section 9,] was a fear of 'general warrants,' giving the bearer an unlimited authority to search and seize" (internal quotation marks omitted)). The particularity requirement was enacted to preclude "undue rummaging," and if a warrant was obtained to authorize, or was used to conduct, "undue rummaging," evidence obtained pursuant to the warrant must be suppressed, in order to effectuate the purpose of Article I, section 9, which is to protect against government conduct that "would significantly impair an individual's interest in freedom from scrutiny, *i.e.*, his privacy." *Mansor*, 363 Or at 206-07 (internal quotation marks and citation omitted); *see also Turay*, 313 Or App at 64 ("'We recognize the danger that warrants might be obtained which are essentially general in character but as to minor items meet the requirement of particularity, and that wholesale seizures might be made under them, in the expectation that the seizure would in any event be upheld as to the property specified. Such an abuse of the warrant procedure, of course, could not be tolerated.'" (Quoting *Aday v. Superior Court*, 55 Cal 2d 789, 797, 362 P2d 47, 52 (1961).)); *State v. Sanger*, 12 Or App 459, 471 n 6, 506 P2d 510 (1973) (also citing *Aday* for that proposition).

In sum, on remand, the trial court should determine whether the evidence at issue satisfies *Mansor*, and, if it does, whether the state has proven that, despite the presumptive taint that follows from that fact that the warrant included invalid search categories, the state has carried is burden of rebutting that presumption. When determining whether the state has done so, the trial court should consider, among other things, whether the evidence was obtained in, or as a result of, a search for evidence in an invalid search category and whether the warrant was intended to authorize, or was used to conduct, unconstitutional "undue rummaging."

Walters, S. J., joins in this concurring opinion.