#### IN THE COURT OF APPEALS OF THE STATE OF OREGON

# STATE OF OREGON, *Plaintiff-Respondent*,

v.

### JORGE ULISES SERRANO, Defendant-Appellant. Marion County Circuit Court 19CR02471; A173250

Thomas M. Hart, Judge.

Argued and submitted January 24, 2022.

Sara A. Werboff, Deputy Public Defender, argued the cause for appellant. Also on the briefs was Ernest G. Lannet, Chief Defender, Criminal Appellate Section.

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

Before Tookey, Presiding Judge, and Lagesen, Chief Judge, and Aoyagi, Judge.\*

TOOKEY, P. J.

Conviction on Count 5 reversed; convictions on Counts 1, 3, 4, 6, 7, and 8 reversed and remanded; otherwise affirmed.

Aoyagi, J., concurring.

<sup>\*</sup> Lagesen, C. J., vice Sercombe, S. J.

#### TOOKEY, P. J.

Defendant appeals a judgment of conviction, by nonunanimous verdicts, for two counts of first-degree rape, ORS 163.375 (Counts 1 and 3); and by unanimous verdicts for three counts of second-degree sexual abuse, ORS 163.425 (Counts 4, 7 and 8); one count of using a child in a display of sexually explicit conduct, ORS 163.670 (Count 5); and one count of first-degree encouraging child sexual abuse, ORS 163.684 (Count 6).<sup>1</sup> For the reasons that follow, we reverse defendant's conviction on Count 5 and reverse and remand his convictions on Counts 1, 3, 4, 6, 7, and 8.

### I. BACKGROUND

We summarize the facts as expressly or implicitly found by the trial court. *State v. Ehly*, 317 Or 66, 75, 854 P2d 421 (1993). Most of the facts are procedural and undisputed.

Defendant's convictions stem from evidence police obtained through searches of the data from defendant's cell phone pursuant to two search warrants, the first in December 2018, and the second in February 2019. The first warrant was secured based on statements by CB—who is not a victim in this case. CB reported to police in 2018, that, in 2015, at the age of 18 or 19, she had had sexual encounters with defendant. CB filed the police report after learning that images and videos from those 2015 encounters had been uploaded without her permission to the pornography internet site PornHub during a time frame from October 2017 through December 2018. Through investigation, police learned defendant's username and that defendant had also posted videos of CB on Hclips, another pornography website.

Several weeks after the initial investigation, defendant attempted to initiate communication with CB on Snapchat, a communication platform. In text conversations between defendant and CB and between defendant and a police officer posing as CB, defendant stated that he had had vaginal and anal intercourse with CB when she was unconscious and that he had multiple photos and videos of her on his computer and on his old and new cell phones. In

<sup>&</sup>lt;sup>1</sup> The court acquitted defendant of Count 2, attempted unlawful dissemination of an intimate image, ORS 163.472; ORS 161.405.

those text conversations, defendant sent a photo of himself and revealed his employment and that he had posted videos of CB on Pornhub.

Based on that information, in December 2018, police sought and obtained the first warrant for a search of defendant's cell phones and computer for evidence of first-degree rape and first-degree sodomy of CB. The warrant commanded a search of defendant's residence and car for his cell phones and computer. It authorized a seizure and search of defendant's digital devices for the following: evidence "related to the crimes under investigation" in media form, including pictures and videos and the recording, storing, duplication, and transmitting of pictures, videos, and associated data; evidence of defendant's internet usage for access and browsing of Pornhub and Hclips during the period October 2017 through December 2018; evidence of defendant having connected his cell phone to other devices to transfer the related files; evidence of defendant having uploaded videos from Pornhub and Hclips to cloud storage; evidence of defendant's communications with CB during the period March 2015 through December 2018; evidence of information identifying the user and/or owner: evidence of contact information for users and associates; the user's identification, contact information, and location between the dates of March 2015 through April 2015; evidence of "ownership, use, and access" of and to defendant's Snapchat, Pornhub and Helip accounts during specific time frames; and "[a]ny other evidence of the crimes of ORS 163.405 Sodomy I and ORS 163.375 Rape I."

Officers were able to execute the first warrant and retrieve the data from defendant's cell phone. An investigation of that data disclosed images of potential victims other than CB, which, in turn, led police to seek and execute the second search warrant, in February 2019.<sup>2</sup> The second warrant authorized a complete search of defendant's cell phone, which revealed information that led to the charges and convictions of defendant in this case, for engaging in nonconsensual sexual intercourse or contact with two adult women,

 $<sup>^{\</sup>rm 2}$  That investigation also led to charges against defendant based on his conduct with CB, not at issue on this appeal.

II and KT, and intercourse and sexually explicit conduct with a 17-year-old girl, AG, and capturing sexually explicit conduct with AG on video.

Defendant filed a motion to suppress evidence obtained from the searches of the data from his cell phone, contending among other points that the warrants violated the particularity requirement of Article I, section 9, of the Oregon Constitution. The trial court denied the motion, concluding that the warrants were sufficiently particular. Defendant also filed a motion for a judgment of acquittal on Count 5, using a child in a display of sexually explicit conduct, and a motion to sever trial of the charges relating to AG from trial of those relating to the adult victims, II and KT, both of which the trial court denied. On appeal, defendant challenges the trial court's denial of his motion to suppress, the trial court's denial of his motion to sever.

## II. DEFENDANT'S CHALLENGE TO THE TRIAL COURT'S DENIAL OF HIS MOTION TO SUPPRESS

Defendant does not dispute that the first search warrant was supported by probable cause that defendant had committed rape and sodomy of CB. But defendant contends in his first and second assignments of error that that probable cause only authorized a warrant for the search of defendant's cell phone for material related to offenses against CB that were known to have been committed in a particular time frame. Although defendant concedes that some of the first warrant's commands were specific to evidence of the crimes involving the victim CB during the relevant time frame, he contends that other portions of the first warrant allowed a more generalized search that was not adequately specific. In particular, on appeal, defendant cites the command to search defendant's digital "media" for "evidence related to the crimes under investigation."<sup>3</sup> Defendant contends that, because the warrant did not limit the search of media to the crimes of a sodomy and rape against CB during a particular time frame, the warrant lacked specificity and

<sup>&</sup>lt;sup>3</sup> On appeal, defendant also cites the command to search the cell phone for "any other evidence" of the crimes of sodomy and rape. However, defendant's motion to suppress did not specifically put at issue that command.

authorized an overbroad search, and that the trial court therefore erred in denying his motion to suppress evidence obtained through the searches.<sup>4</sup> See Or Const, Art I, § 9 (a search warrant must "particularly describ[e] the place to be searched, and the person or thing to be seized").

We review the trial court's ruling on defendant's motion to suppress for errors of law. State v. Stephens, 184 Or App 556, 560, 56 P3d 950 (2002), rev den, 335 Or 195 (2003). The Supreme Court explained in State v. Bridewell. 306 Or 231, 247, 759 P3d 1054 (1988), that "[t]he goals of constitutional search and seizure provisions are to restrain the government[.]" Article I, section 9, enshrines that goal by requiring that a warrant must "particularly describ[e] the place to be searched, and the person or thing to be seized." The "particularity requirement" was intended to "prevent the use of general warrants" by "ensur[ing] that a warrant describes with particularity the person to be seized, the place to be searched, or the thing to be seized." State v. Carter, 342 Or 39, 44, 147 P3d 1151 (2006). Thus, a warrant authorizing a governmental search or seizure of places or things "must allow the executing officer to identify with 'reasonable effort' the things to be seized 'for which a magistrate has found probable cause." State v. Mansor, 363 Or 185, 212, 421 P3d 323 (2018) (quoting State v. Trax, 335 Or 597, 602-03, 75 P3d 440 (2003)).

A search of digital devices necessitates additional precautions. The court in *Mansor* explained that, with regard to digital devices, to comport with the particularity requirement of Article I, section 9, a search warrant 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 (emphasis added).

We agree with defendant that the search command for "media" in the first warrant, read in isolation from the

 $<sup>^4</sup>$  The court granted defendant's motion in part, suppressing any evidence from outside the date range of March 2015 to February 2019.

affidavit, fell short for lack of specificity. The search command did not specify that the search was limited to media relating to CB. Nor did the command list a time or date range for the media materials, although that information was known by the state. The fact that the media command limited the media search to "evidence related to the crimes under investigation" did not cure the overbreadth. See State v. Bock (A169480), 310 Or App 329, 336, 485 P3d 931 (2021) (citing the Supreme Court's caution in Mansor, 363 Or at 213, that a warrant's command to find "evidence of a particular crime" does not create specificity sufficient to pass constitutional muster).

But the state is correct that the affidavit cured the lack of specificity in the first warrant.<sup>5</sup> See State v. Turay, 313 Or App 45, 57, 493 P3d 1058, rev allowed, 369 Or 69 (2021) ("In assessing whether the commands are sufficiently particular, we consider not only the warrant itself but [the] affidavit in support of the warrant[.]"). The affidavit described in detail the videos and photos that the officer believed were evidence of the charges of sodomy and rape of CB and that would be found on defendant's phone. The affidavit described the possible date ranges when the videos and photos were taken and when they had been uploaded to Pornhup and HClips. We conclude that the warrant, together with the affidavit, allowed the executing officer to understand precisely what information was being targeted in the command to examine media files.

Matthew Osterman, a digital forensics investigator with the Washington County District Attorney's Office, performed the search of defendant's cell phone. Osterman testified that he removed all of the data from defendant's cell phone and searched that data for items responsive to the search warrant. In the process, he bookmarked items that he thought constituted evidence of sexual crimes. He passed the bookmarks on to the police.

<sup>&</sup>lt;sup>5</sup> Defendant contended below, but does not contend on appeal, that the affidavit was not attached to the warrant at the time of the search. *See State v. Mansor*, 279 Or App 778, 788, 381 P3d 930 (2016), *aff'd on different grounds*, 363 Or 185, 421 P3d 323 (2018) (court will consider a warrant's supporting affidavit only if that affidavit was attached or incorporated by reference into the warrant, noting that it is a defendant's burden to show that).

Police determined that some of the bookmarked items did not to relate to evidence of offenses against CB but to offenses against other persons. *See Mansor*, 363 Or at 218 ("We emphasize, \*\*\* based on our discussion of digital devices and computer searches above, *see* 363 Or at 197-202, that the forensic examination likely will need to examine, at least briefly, some information or data beyond that identified in the warrant."). If only the first warrant had issued, there is no question that information that was outside the scope of the first warrant would not have been available to use against defendant at trial. *Mansor*, 363 Or at 220-21 ("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.").

But based on that information, police suspected that defendant had committed other offenses, and so they conducted a further investigation of the data, which led them to the identification of the victims in this case and to request a second warrant for a second search of the data that had been taken from defendant's cell phone, relating to the potential crimes of rape, encouraging child sexual abuse, using a child in a display of sexually explicit conduct, and unlawful dissemination of an intimate image. The affidavit in support of the second warrant described in detail the investigation and why the officer believed there was a need for a broad search of defendant's cell phone data. We have reviewed the second warrant and conclude that, when considered in light of the affidavit, it also was supported by probable cause. State v. Van Osdol, 290 Or App 902, 907-08, 417 P3d 488 (2018) ("Probable cause exists when the facts, as set forth in the affidavit, along with any reasonable inferences, could permit a neutral and detached magistrate to determine that seizable evidence probably would be found at the place to be searched.").

Defendant contends, however, that because the investigation that led to the second warrant originated with information that was outside the scope of the first warrant, the second warrant was tainted by that prior "illegality" and cannot be viewed as having been obtained independently of the prior illegality. See State v. DeJong, 368 Or 640, 654, 497 P3d 710 (2021) ("When a defendant seeks to suppress evidence discovered in a legally authorized search on the basis of a prior illegality, the focus of the inquiry is not on the legality of the act providing authority to search, it is on the effect that the prior illegality may have had on the authorized search."); State v. Johnson, 335 Or 511, 519, 73 P3d 282 (2003) (the independent source doctrine "permits the introduction of 'evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality'") (quoting *Murray v. United States*, 487 US 533, 537, 108 S Ct 2529, 101 L Ed 2d 472 (1988)). Thus, defendant contends, the evidence obtained from execution of the second warrant was tainted and could not be used at trial.

We disagree with defendant's characterization of the material incidentally uncovered during the execution of the first warrant as "illegal." The material incidentally disclosed in execution of the search, although unauthorized by the warrant, was not unlawfully obtained. Mansor, 363 Or at 220-21 (search of digital devices incidentally disclosing material outside of the warrant's authorization is "lawful and appropriate"). But we nonetheless agree with defendant that, under Mansor, that material was tainted as a source of investigative material for the potential crimes that it revealed. It is undisputed that the state identified the current victims from the nonresponsive material obtained in execution of the first warrant and that the investigation that led to the request for the second warrant was based on evidence, including text messages, videos, and images of individuals other than CB, that police found as a result of their further investigation of the nonresponsive material disclosed in the execution of the first warrant. Cf. State v. Tardie, 319 Or App 229, 242, 509 P3d 705, rev den, 370 Or 303 (2022) (officer averred that he had not relied on suppressed evidence unlawfully discovered under the second warrant to request a third warrant). To allow the police to benefit from that material for further investigation would be inconsistent with *Mansor*, where the court said:

"[T]o protect the right to privacy and to avoid permitting the digital equivalent of general warrants, we \*\*\* hold that Article I, section 9, prevents the state from using evidence found in a computer search unless a valid warrant authorized the search for that particular evidence, or it is admissible under an exception to the warrant requirement."

### 363 Or at 188.

We recognize that *Mansor* does not deal directly with the issue presented here; the Supreme Court did not have before it in *Mansor* a question whether or to what extent law enforcement personnel can use nonresponsive or unauthorized material uncovered on a cell phoneincluding evidence of other potential crimes-as a basis for further investigation of and the issuance of a warrant for a search related to those other crimes, that is, crimes other than those for which the original warrant authorized a search. But the court clearly was aware of that potential circumstance. See id. at 214-18 (discussing Wheeler v. State. 135 A3d 282 (Del 2016), which reversed a defendant's conviction for possession of digital child pornography based on nonresponsive evidence discovered in the execution of an unconstitutionally overbroad warrant for the search of the defendant's computer and other digital equipment as part of an investigation into the defendant's alleged witness tampering).

We recently held in *Bock* that the use at trial of images of a weapon on the defendant's cell phone could not be supported by the plain view doctrine, where the section of the warrant directing a search for evidence of felon in possession of a firearm was insufficiently particular and therefore invalid, because a firearm itself cannot be located on a cell phone. 310 Or App at 337. We explained, citing *Mansor*, 363 Or at 220, that the breadth of a search required of digital material "is what renders the plain view doctrine inapplicable; the alternative would sanction the sort of general warrant that the plain view doctrine was never meant to authorize." *Bock (A169480)*, 310 Or App at 340.

*Bock*, like *Mansor*, emphasized the unique privacy issues presented in searches of digital devices and highlighted the Supreme Court's rationale for imposing additional limitations: "The very nature of a digital device such as a cell phone renders it a 'repository with a historically unprecedented capacity to collect and store a diverse and vast array of personal information.' [Mansor, 363 Or] at 208. Accordingly, to ensure that Article I, section 9, continued to fulfill its purpose of protecting individuals' privacy and avoided 'sanctioning the undue rummaging that the particularity requirement was enacted to preclude,' an additional limitation on the use of data falling outside the scope of an electronic search warrant was necessary. Id. at 220 (internal quotation marks omitted). Specifically, the state is prohibited from introducing into evidence any 'information obtained in a computer search if the warrant did not authorize the search for that information, unless some other warrant exception applies.' Id. at 220-21."

*Bock (A169480)*, 310 Or App at 337. But like *Mansor*, *Bock* did not address the issue presented here, whether nonresponsive material discovered in plain view in a *lawful* search of the digital material of a cell phone may provide a basis for further investigation of the same digital material for crimes other than those for which the warrant was issued. In our view, in light of *Mansor*, the Supreme Court would say no.

Noting the purpose of Article I, section 9, to protect against "governmental intrusions," the Supreme Court has said that "[t]his right against intrusion should be stringently protected by the courts." *State v. Davis*, 295 Or 227, 243, 666 P2d 802 (1983). As the Supreme Court has long recognized, the remedy for governmental intrusion upon the personal right guaranteed under Article I, section 9, is "to restore the parties to the position they would have been in" prior to the governmental intrusion. *State v. Craigen*, 370 Or 696, 712, 524 P3d 85 (2023); *Mansor*, 363 Or at 221; *see also Davis*, 295 Or at 237 (stating same, and noting court's adherence to that remedy since *State v. Laundy*, 103 Or 443, 204 P 958 (1922)). The court said in *Mansor*:

"[T]he 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.' Mansor, 279 Or App at 803 (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. \*\*\* Put differently, 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, and the state may use the information identified in the warrant in a prosecution or any other lawful manner. 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."

363 Or at 220-21 (emphasis added.) The court emphasized the constitutional privacy interest at stake in a search of a person's cell phone, quoting from its opinion in *Davis*:

"That approach is consistent with our explanation 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:

"'[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.'"

Mansor, 363 Or at 221 (quoting Davis, 295 Or at 237).

We recognize, as the state points out, that in *Mansor* the court said that the nonresponsive material could not be used *at trial*, *id*. at 221, and that the court did not have

before it and made no comment on whether the state could use the nonresponsive material as a basis for further investigation. But we reject the state's contention that the court's opinion showed that it intended to limit the use of the nonresponsive material only in the instant trial. Defendant had a privacy interest in the contents of his cell phone. Id. at 188. If, as the Supreme Court said, the rationale of avoiding an unreasonable invasion of a person's privacy interest protects the nonresponsive material from being used at trial because the constitution requires that "the parties [be restored] to their position as if the state's officers had remained within the limits of their authority," id.; see State v. Tyler, 218 Or App 105, 109, 178 P3d 282 (2008) ("The rationale for suppressing unlawfully obtained evidence under Oregon law is remedial-that is, its purpose is to restore the defendant to the same position as if the government had stayed within the law."), we think that it is likely that the court would also conclude that, in the absence of an independent source, the nonresponsive material cannot provide a basis for further investigation. If, as the court held in Mansor, a defendant must be restored to the position he was in but for the discovery of the nonresponsive material, the nonresponsive material could not provide a source for investigation of defendant's potential crimes. Thus, the second warrant was unlawful, and the trial court erred in denying defendant's motion to suppress.<sup>6</sup>

The state asserts that we should hold that *Mansor* prohibits only the use of nonresponsive material in judicial proceedings such as a trial or an application for a warrant and does not require that police "turn a blind eye" to criminal activity. In the state's view, nonresponsive information learned from data permissibly observed in executing a search warrant may be used for further investigation, even

<sup>&</sup>lt;sup>6</sup> Based on our understanding of *Mansor*, law enforcement personnel may not use nonresponsive material as a basis for initiating an investigation of potential crimes revealed by that nonresponsive material. However, *Mansor* does not prevent law enforcement personnel from investigating those potential crimes if the origin of the investigation is a source independent of and completely separate from the nonresponsive material. *See Tardie*, 319 Or App at 241 (discussing independent source doctrine). The state does not contend that the origin of its investigation was independent of the nonresponsive material found on defendant's cell phone.

if that data is outside the scope of the warrant's search commands in the way contemplated by Mansor's use restriction. We reject the contention. As explained above, in Mansor, the court held that "Article I, section 9, prevents the state from using evidence found in a computer search unless a valid warrant authorized the search for that particular evidence" in order to "protect the right to privacy and to avoid permitting the digital equivalent of general warrants," to "restore the parties to the position they would have been in" prior to the governmental intrusion. 363 Or at 188, 221. That principle holds true under the Fourth Amendment as well, which requires "'not merely [that] evidence so acquired shall not be used before the Court but that it shall not be used at all." Wong Sun v. United States, 371 US 471, 485, 83 S Ct 407, 9 L Ed 2d 441 (1963) (emphasis added; guoting Silverthorne Lumber Co. v. United States, 251 US 385, 392, 40 S Ct 182, 64 L Ed 319 (1920)).

As we understand *Mansor*, preventing the state from "using" evidence means not permitting use of it: not at trial, not to obtain a warrant as part of an investigation, or, as in this case, not as the basis for a new investigation that ultimately leads to probable cause for a new warrant. If nonresponsive evidence found in the warranted search of a computer can provide a basis for initiating a new investigation, leading to a new warrant, then the state has "used" that evidence and permitted the digital equivalent of a general warrant, and the right to privacy afforded by Article I, section 9, has been abrogated. <sup>7</sup>

Having concluded that the trial court erred in denying defendant's motion to suppress, we must now address the state's argument that the error was harmless. A trial court's error is harmless if there is "little likelihood" that it affected the jury's verdict. *State v. Lachat*, 298 Or App 579, 589, 448 P3d 670 (2019), *rev den*, 366 Or 257 (2020). It

 $<sup>^7</sup>$  Of course, not all investigative use of nonresponsive material is barred. For example, if the data revealed a crime in progress or an intended crime, then exigent circumstances could support further investigation without a warrant. State v. Meharry, 342 Or 173, 177, 149 P3d 1155 (2006) (noting the "exigent circumstances" exception "allows the police to conduct a search without a warrant if the search is both supported by probable cause and conducted under exigent circumstances").

is true, as the state contends, that the convictions at issue here, with the exception of the charge of using a child in a display of sexually explicit conduct, did not include as an element the material discovered on defendant's cell phone, and that there was other evidence, including the testimony of victims, that supplied the elements of the charges. Thus, the state contends, defendant's convictions are unlikely to have been based on the evidence obtained from defendant's cell phone. But all of the charges in this case stem from the investigation triggered by discovery of the nonresponsive material on defendant's cell phone. Police discovered the existence and identities of II, KT, and AG because of that investigation. In the absence of the nonresponsive material, the need for any follow-up investigation would not have been otherwise discovered.

Additionally, the state introduced multiple pieces of evidence from defendant's phone, including nude images of II taken without her knowledge or consent, and sexually explicit videos of AG that formed the bases of the charges of use of a child in a sexually explicit display and encouraging child sexual abuse. In addition to depicting the underlying sexual acts, the videos also contained evidence of AG's age and defendant's awareness of AG's age. We cannot say that the admission of that evidence had little likelihood of affecting the verdict. The denial of the motion to suppress therefore was not harmless, because the charges in this case stem from the investigation triggered by discovery of the nonresponsive material on defendant's cell phone, and highly probative evidence used to prove the state's case came from the nonresponsive material discovered on defendant's cell phone.

We emphasize our awareness, as the concurrence points out, that we already expect a lot from law enforcement in terms of knowing how to apply constitutional concepts such as reasonable suspicion, probable cause, freedom to leave, and the invocation of rights, and that our holding will have practical implications for the conduct of investigations by law enforcement personnel. But under the fruit of the poisonous tree doctrine, law enforcement is routinely expected not to "use" information in its possession. *See, e.g.*, *Silverthorne Lumber Co.*, 251 US at 392 ("The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all."). We acknowledge that the nuances of this area of law relating to digital searches are complex and developing.

## III. DEFENDANT'S CHALLENGE TO THE DENIAL OF HIS MOTION FOR A JUDGMENT OF AQUITTAL

We turn to defendant's third assignment of error, in which he contends that trial court erred when it denied his motion for judgment of acquittal on Count 5. Defendant was charged and convicted in Count 5 of use of a child in a sexually explicit display with respect the victim AG, who was 17 years old at the time of the offense.

A person commits that offense "if the person employs, authorizes, permits, compels or induces a child to participate or engage in sexually explicit conduct for any person to observe or to record in a visual recording." ORS 163.670(1). Here, the state charged that defendant "compelled" AG to engage in sexually explicit conduct that defendant recorded. The evidence at trial was that AG willingly engaged in sexually explicit conduct with defendant and also willingly allowed defendant to take video of their sexual conduct. Defendant contends that the evidence cannot support a finding that defendant *compelled* AG to participate in a sexually explicit recording, as the Supreme Court defined it in *State* v. Marshall, 350 Or 208, 220, 253 P3d 1017 (2011), which analyzed the term "forcible compulsion" as used in ORS 163.427(1)(a), defining sexual abuse in the first degree.<sup>8</sup>

We need not address whether "compel," as the court defined it in *Marshall* for purposes of ORS 163.427(1)(a), has the same meaning in ORS 163.670(1). On appeal, the state does not assert that the evidence would support a finding

<sup>&</sup>lt;sup>8</sup> In *Marshall*, the Supreme Court said that "to compel" "conveys a range of meanings, centered around achieving compliance or submission by some level of force." The court explained that the force "need not [have risen] to the level of violence," but it "must [have been] sufficient to 'compel' the victim, against the victim's will, to submit to or engage in the sexual contact." *Id.* at 225.

Here, defendant contends, because the evidence could not support a finding that defendant forced AG against her will to engage in sexually explicit conduct, the state has failed to establish that element of the offense.

of compulsion, and we agree that it would not. We further reject the state's suggestion that the means of committing the offense listed in ORS 163.670(1) are interchangeable descriptions rather than distinct means of committing the offense. As the court held in State v. Medina, 357 Or 254, 271-72, 355 P3d 108 (2015), when the differences in the means by which an offense can be committed render them "distinct acts," the state is bound by the substantive allegation in the indictment. Id. Here, the state alleged that defendant had committed the offense of use of a child in a sexually explicit display by compelling AG. At trial, the state's theory was that defendant had compelled the victim to act, and the state relied exclusively on that alleged means. The jury received three instructions relating to the offense that explained the state's burden to show that defendant had compelled the sexually explicit conduct. The state is bound by the substance of its allegation as well as its theory at trial. See State v. Samuel, 289 Or App 618, 410 P3d 275 (2017) (state not permitted to prove a different theory of defendant's felon status than it alleged in the indictment in prosecution for felon in possession of firearm).<sup>9</sup>

Because we agree with defendant (and with the state's implicit concession) that the evidence does not support a finding that defendant "compelled" AG, we conclude that the trial court erred in denying his motion for a judgment of acquittal on Count 5. Thus, defendant's conviction on Count 5 must be reversed.

### IV. DEFENDANT'S CHALLENGE TO THE TRIAL COURT'S DENIAL OF HIS MOTION TO SEVER

In his fourth assignment of error, defendant contends that the trial court erred in declining to sever trial of the charges relating to AG from those relating to the adult victims, II and KT. The trial court found that the circumstances of the charges, and the conduct and the evidence on

<sup>&</sup>lt;sup>9</sup> We note the unfair prejudice to a defendant if, having been charged and tried on a theory of compelling the victim to act, the defendant could be convicted based on less forceful conduct of inducing, permitting, or authorizing the victim to act. *State v. Boitz*, 236 Or App 350, 356, 236 P3d 766 (2010) (declining to determine whether a variance concerned a material element because, even if it did not, the variance was impermissible because it was prejudicial).

which they were based, were sufficiently similar that the charges could be joined. We have reviewed the record and conclude without further discussion that the trial court did not  $\rm err.^{10}$ 

Conviction on Count 5 reversed; convictions on Counts 1, 3, 4, 6, 7, and 8 reversed and remanded; otherwise affirmed.

### Aoyagi, J., concurring.

In State v. Mansor, 363 Or 185, 220, 223, 421 P3d 323 (2018), the Supreme Court held that when law enforcement conducts a reasonable forensic examination of a computer pursuant to a lawful warrant, and the examination "reveal[s] information that is beyond the scope of the warrant"—by virtue of the inherent nature of a forensic examination, rather than any overreaching by law enforcement—"a defendant's Article I, section 9, privacy rights prevent the state from using such information unless it comes within an exception to the warrant requirement."

The Supreme Court left open in *Mansor* whether and to what extent the plain-view doctrine might apply in such a situation. *See id.* at 210-11. We closed that door in *State v. Bock (A169480)*, 310 Or App 329, 340, 485 P3d 931 (2021), holding that the plain-view doctrine is "inapplicable" to computer searches. The Supreme Court also arguably left open in *Mansor* whether incidentally found information may be used for any purposes other than as evidence at trial. *See Mansor*, 363 Or at 220-21 (focusing on use of evidence at trial). We close that door in this case and its companion case, holding that essentially any "use" of such information

<sup>&</sup>lt;sup>10</sup> In light of our conclusion that the trial court erred in denying defendant's motion to suppress, the case must be remanded for a new trial. We note, however, that the state concedes error on defendant's fifth and sixth assignments of error, in which defendant contends that his convictions of first-degree rape (Counts 1 and 3), which were based on nonunanimous verdicts, must be reversed and remanded under *Ramos v. Louisiana*, 590 US \_\_\_\_, 140 S Ct 1390, 1391, 206 L Ed 2d 583 (2020). The state also concedes error on defendant's seventh assignment contending that the trial court erroneously instructed the jury that it could convict defendant on less than a unanimous verdict. However, because the verdicts on the remaining counts were unanimous, the instructional error was harmless as to those counts. *See, e.g., State v. Flores Ramos*, 367 Or 292, 333-34, 478 P3d 515 (2020).

is prohibited, including as an impetus for investigation. See 324 Or App at 464-65 & n 6 (holding that the second warrant was unlawful, where it was obtained after investigating "nonresponsive material" found in executing the first warrant, and noting that "law enforcement personnel may not use nonresponsive material as a basis for initiating an investigation of potential crimes revealed by that nonresponsive material."); State v. Serrano (A174829), 324 Or App 475, 476, \_\_\_ P3d \_\_\_ (2023) (reversing denial of motion to suppress evidence that "was derived from an investigation that had its source in material incidentally uncovered from a search of defendant's cell phone").

I cannot fault the majority for relying on *Mansor* to conclude that any "use" of information that was found incidentally during a lawful search of an electronic device—but that was beyond the scope of the warrant under which that device was searched—is prohibited. In *Mansor*, the state used incidentally found information as evidence at trial. 363 Or at 188. In concluding that such evidence should have been suppressed, the court's opinion sometimes refers to "use at trial," *see, e.g., id.* at 208, 210, and other times refers to "use" more generally, *see id.* at 188, 205, 223. For example:

"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. See [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 use restrictions for data 'nonresponsive' to the warrant). Put differently, 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, and the state may use the information identified in the warrant in a prosecution or any other lawful manner. 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. at 221 (emphases added).

Of course, the Supreme Court had no need to consider in *Mansor* the outer limits of the use restriction that it was adopting, because *Mansor* involved use at trial, which is the most obvious type of use to prohibit. I am not as confident as the majority that, were the Supreme Court to address other types of use, it would necessarily adopt the broad use restriction that we do in the present case. See 324 Or App at 464-65. In my view, it would be defensible to treat information that was lawfully obtained differently from information that was unlawfully obtained, so long as the relevant considerations are appropriately balanced. Other than Mansor, which I do not read as resolving the present issue, existing case law addresses only unlawfully discovered evidence. E.g., State v. Craigen, 370 Or 696, 711, 524 P3d 85 (2023) ("Under Oregon constitutional law, when the state violates an individual's constitutional right, the state cannot use evidence obtained as a result of that violation.").

Notably, the use-restriction model adopted in Mansor derives from the academic writings of Professor Orin Kerr. See Mansor. 363 Or at 221 (citing with approval Orin S. Kerr, Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, 48 Tex Tech L Rev 1 (2015)). As Kerr aptly states, "If courts adopt a use restriction, the next issue is what counts as 'use.'" Kerr, 48 Tex Tech L Rev at 29. Kerr advocates for the prohibition of two types of "use" of nonresponsive data found incidentally in a lawful search of an electronic device: (1) use of the data "in court to prove the suspect's crime," which Kerr describes as "a core case of use"; and (2) use of the data "as a basis for cause to justify an additional search or seizure for more responsive data"—"either by copying it and submitting it in the warrant application or simply by describing its discovery in an affidavit[.]" Id. Beyond those two categories, "[t]he outer bounds of a use restriction are less certain." Id. This case falls along that uncertain boundary—images that were incidentally found on defendant's cell phone during a lawful warranted search prompted an investigation that led officers to new victims and new evidence, which was then used to support a second warrant.<sup>1</sup>

<sup>&</sup>lt;sup>1</sup> The affidavit in support of the second warrant is unclear as to the exact circumstances of the officers viewing the incidentally discovered data that spurred the

Given how *Mansor* is written. I am inclined to look to the Supreme Court to clarify its own intentions as to the breadth of the use restriction announced in that case. For that reason, I join the majority, even though I have some concerns about the broad use restriction that we adopt in this case. I am particularly concerned about the unique practical challenges that our holding poses for law enforcement. Historically, law enforcement could rest assured that, so long as officers respected the constitutional rights of citizens, including lawfully obtaining and executing warrants, the information that they gathered generally would be usable for investigative purposes and at trial. Conversely, any information obtained or derived from the violation of a citizen's constitutional rights likely would not be usable. The latter limitation might be frustrating to law enforcement at times, particularly when a constitutional violation was unintentional, but it is an intuitively understandable consequence of police overreaching.

Together, *Mansor*, *Bock*, and *Serrano* change that fundamental precept. The practical import of this new line of cases is that law enforcement officers must turn a blind eye to criminal activity that *lawfully* comes to their attention. Such a rule does not have the same intuitive appeal as the longstanding "fruit of the poisonous tree" principle. *See, e.g., Craigen*, 370 Or at 713 ("The state cannot benefit from a violation of a defendant's constitutional rights."); *State v. Arreola-Botello*, 365 Or 695, 714, 451 P3d 939 (2019) (recognizing the longstanding principle that "evidence will be suppressed if the evidence was the product of an unconstitutional act"). The tree is not poisonous, the state is not benefitting from any illegality, and yet any fruit will still be suppressed.

Moreover, law enforcement officers will now have to regularly assess the lawful scope of warrants. Otherwise, they will end up wasting resources by investigating crimes based on information that was lawfully obtained but should have been ignored, leading to the suppression of all of the results of their investigation. That puts law enforcement in

new investigation. Those types of factual details could be relevant to suppression, if the Supreme Court were to adopt a more nuanced use restriction than we do.

a new position. Until now, law enforcement officers could largely look to judges to ensure valid warrants—that is why warrants are issued by judges—with a resultingly low risk that evidence found during a warranted search would be suppressed. Now, with respect to searches of electronic devices such as computers and cell phones, officers will be called upon to assess for themselves, without judicial oversight, whether information found during a lawful search may be "used" for investigative purposes.

We already expect a lot from law enforcement in terms of knowing how to apply constitutional concepts like reasonable suspicion, probable cause, freedom to leave, invocation of rights, and the like. However, I suspect that officers will face new challenges in having to evaluate whether it is safe to rely on information lawfully found during a warranted search of a computer or cell phone in pursuing an investigation or, conversely, whether doing so will result in a pointless investigation of an effectively unprosecutable crime. I therefore hope that, if the Supreme Court disagrees with our understanding of *Mansor*, it will act quickly to clarify the scope of the prohibition on the state "using" nonresponsive information found incidentally on an electronic device during a lawful warranted search.

Accordingly, I concur.