

IN THE SUPREME COURT OF THE
STATE OF OREGON

STATE OF OREGON,
Appellant,

v.

LANGSTON AMANI HARRIS,
Respondent.

(CC 20CR28186) (SC S068481)

On appeal from an order of the Washington County Circuit Court under ORS 138.045(1)(d), ORS 138.045(2), and ORAP 12.07.*

Argued and submitted November 2, 2021; resubmitted January 25, 2022.

Benjamin Gutman, Solicitor General, Salem, argued the cause and filed the briefs for appellant. Also on the briefs were Ellen F. Rosenblum, Attorney General, and Jennifer S. Lloyd, Assistant Attorney General.

Kevin Sali, Kevin Sali LLC, Portland, argued the cause and filed the brief for respondent. Also on the brief was John Robb.

Before Walters, Chief Justice, and Balmer, Flynn, Duncan, Nelson, Garrett, and DeHoog, Justices.**

FLYNN, J.

The order of the circuit court is affirmed.

* Janelle F. Wipper, Judge.

** Nakamoto, J., retired December 31, 2021, and did not participate in the decision of this case.

FLYNN, J.

This case involves the state's direct and interlocutory appeal of an omnibus pretrial order granting numerous defense motions to suppress evidence that the state obtained through wiretaps and search warrants. *See* ORS 138.045(1)(d) (authorizing state to appeal from "[a]n order made prior to trial suppressing evidence"); ORS 138.045(2) (specifying that "the state shall take the appeal to the Supreme Court if the defendant is charged with murder or aggravated murder"). The trial court ruled: (1) that the wiretaps violated federal law because the applications did not indicate that the elected district attorney personally was even aware of the applications, and (2) that roughly two dozen search warrants for cell phone data and social media accounts were invalid for multiple reasons, including that the warrants were overbroad and that, after excising from later warrant applications all information derived from the invalid earlier warrant(s), the state lacked probable cause to support the later warrants. We affirm those rulings of the trial court.

I. FACTS

Defendant has been charged with first-degree and second-degree murder, first-degree robbery, promoting prostitution, and other crimes. In this pretrial posture, the following facts are undisputed for purposes of this direct appeal.

The murder charges arise from the death of RBH, who was shot outside of his apartment building in the early morning hours of September 20, 2017. RBH had had an argument with his wife the evening before and had left their home to spend the night in his pickup truck. RBH's wife spoke to him about 3:00 a.m., while he was sitting in his truck in the parking lot outside of their building. Officers were called to the scene the next morning and found RBH on the ground near his truck, with a gunshot wound to the head. It appears that the shooting occurred at about 3:30 a.m., based on the report of a neighbor who heard sounds that might have been gunfire and saw a car driving away from where the body was found.

When officers arrived at the scene, they found two cell phones on RBH's body. Although his wife could identify only one cell phone as belonging to RBH, officers eventually determined that the second phone belonged to him as well. With consent from RBH's wife, police obtained a search warrant for the call and text records for the second phone. Through those records, officers identified a phone number, -2494, that had called RBH nine times between 3:13 a.m. and 3:21 a.m. on the morning of the murder. Four of the calls were not completed, another four had gone to voicemail, and the final call had been answered and had lasted over four minutes.

Based on that information, the state applied for a search warrant for records of phone number -2494 from the service provider, T-Mobile. The affidavit supporting the application explained that the "aforementioned" facts gave rise to probable cause "to believe that evidence of the crimes of Murder (ORS 163.115) and Manslaughter in the First Degree (ORS 163.118)" could be found in the records associated with that phone number because of the repeated calls to [RBH's] phone "minutes before witnesses reported hearing two popping sounds in the area of where [RBH's] body was eventually found." The affidavit explained that

"[t]he records are going to provide evidence of the crime of murder because the records will help identify people who may be able to provide witness information or details about what was happening or have information about the murder because the calls were so close in time to reports of 'pops' by neighbors."

The affidavit requested a warrant to obtain detailed records for the period from 8:00 a.m. on September 19, 2017, through 8:00 p.m. on September 21, including "location data" for the phone, "details of all voice, message, and data usages (incoming and outgoing)," and "all incoming and/or outgoing SMS and/or MMS messages and related records." The warrant issued on September 22, 2017.

Around the time that officers received records in response to the September 22 warrant for phone number -2494, which the state later linked to defendant, officers learned from an analysis of RBH's phone records that he

had exchanged numerous text messages and phone calls in the hour before his death with multiple phone numbers that police linked to online advertisements for prostitution services. One of these calls to RBH's phone was made at 3:27 a.m., from a phone number linked to prostitution advertisements for a woman named Sterling-Clark.

Relying in part on the additional information from RBH's phone and in part on records obtained in response to the September 22 warrant, officers then sought and obtained orders for the records of multiple additional phone numbers. And those records, in turn, led to still other search warrants. As relevant here, the state would eventually obtain more than twenty additional search warrants directed against defendant based on the information developed from the September 22 warrant. Those additional warrants were primarily for phone numbers, but also included warrants for online accounts, that were owned or used by defendant.

In addition, the state applied for and obtained orders to intercept oral, electronic, and wire communications (wiretaps) for multiple phone numbers allegedly used by defendant, a process that is restricted under federal law. *See* 18 USC §§ 2510-2520 (setting out when state and federal courts may authorize the interception of wire, electronic, and oral communications).

The state's theory of the case, which it expects the evidence will support, is that defendant and Sterling-Clark were part of a prostitution ring operating in Washington County. On the night that RBH was murdered, he had responded to an online ad for prostitution services and had arranged to meet Sterling-Clark. Defendant, who helped arrange the encounter, drove Sterling-Clark to meet RBH. At some point, defendant and Sterling-Clark decided to rob RBH, who had texted them a picture of a large amount of cash. In the course of the robbery, defendant shot and killed RBH. Later, defendant tried to intimidate Sterling-Clark into concealing his role in the murder.

After being indicted, defendant filed numerous pretrial motions, including motions to suppress evidence intercepted through the wiretaps and obtained through

search warrants for cell phone records, beginning with the September 22 warrant. The trial court granted some of defendant's motions to suppress, and the state filed this pretrial appeal pursuant to ORS 138.045(1)(d), (2).

II. DISCUSSION

As described at the outset, the state divides its challenges to the pretrial rulings into two assignments of error. The first assignment of error challenges the grant of defendant's motion to suppress evidence obtained through the wiretap orders on the basis that the applications failed to satisfy the requirements of federal law. The second assignment of error challenges the court's combined ruling granting two dozen motions to suppress evidence derived from search warrants for cell phone records on the basis that each warrant was invalid for multiple alternative reasons. As the facts are undisputed, we review the trial court's rulings on the motions to suppress for legal error. *See State v. Turnidge (S059155)*, 359 Or 364, 399, 374 P3d 853 (2016). And we conclude that the trial court did not err.

A. Wiretap Evidence

1. Motion to suppress and trial court order

Defendant sought to suppress the evidence obtained as a result of the four wiretap orders. Federal law—enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), Pub L 90-351, 82 Stat 197 (1968)—restricts in several ways the ability of both state and federal government officials to obtain judicial wiretap orders. Most pertinent to this appeal, the act prohibits all courts, federal and state, from admitting any wiretap evidence obtained in violation of the act in any trial, hearing, or other similar proceeding. 18 USC § 2515; *see also id.* § 2518(10)(a) (setting out procedures for suppression).¹

The relevant restriction on wiretaps is set out in 18 USC section 2516(2), which provides that wiretap

¹ The act also specifies that the permissible use of a wiretap is limited to developing evidence of certain serious offenses, *see* 18 USC § 2516 (listing offenses); that the application for a wiretap must contain prescribed information, *id.* § 2518(1); and the court must make certain findings before granting the order, *id.* § 2518(3). None of those requirements is in dispute here.

applications at the state level must be made by “[t]he principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State[.]”

In this case, all of the challenged applications for wiretaps were made by a deputy district attorney. The applications stated that the deputy district attorney was

“authorized by District Attorney Robert Hermann for Washington County, Oregon to make this application pursuant to ORS 133.724(1)(a)[.]”

The affidavits provided no further information about the authorization.

In his motion to suppress, defendant argued that the “principal prosecuting attorney” under section 2516(2) is limited to the Attorney General or an elected district attorney and that the district attorney cannot delegate the authority to make wiretap applications. Defendant recognized that Oregon law purports to authorize district attorneys to delegate to a deputy their authority to apply for wiretaps. *See* ORS 133.724(1) (permitting wiretap applications by “the individual who is the district attorney or a deputy district attorney authorized by the district attorney”). But he contended that federal law precludes that delegation of the authority to seek wiretaps. Because the wiretap applications in this case were submitted by a deputy district attorney, without any indication that the elected district attorney even had participated in the process, defendant contended that the wiretap orders were issued in violation of federal law and that the trial court should suppress the wiretap evidence as “unlawfully intercepted.” *See* 18 USC § 2518(10)(a)(i) (so providing).

The state did not dispute that the phrase “principal prosecuting attorney” in the federal act refers to the district attorney. It contended, however, that the federal law does not preclude Oregon from permitting district attorneys to delegate their authority to apply for wiretaps. It also argued in the alternative that, regardless of the validity of the wiretap applications, the evidence should not be suppressed because the state had acted in good faith.

The trial court rejected the state’s argument and suppressed the wiretap evidence. It concluded that states are prohibited from creating less restrictive wiretapping requirements than those in section 2516(2). And it concluded that the Oregon statute authorizing delegation, ORS 133.724(1), is less restrictive because it allows delegation to deputy district attorneys to apply for wiretaps. Because in this case “the official responsive to the political process did not indicate that he or she was aware of the wiretap application[s],” the court held that the wiretaps violated federal law. The court concluded that no “good faith exception” applies and that the evidence obtained in response to the wiretaps must be suppressed.

2. *Delegation by “principal prosecuting attorney”*

The issue regarding the wiretap evidence is entirely one of federal law.² To determine whether section 2516(2) permits a “principal prosecuting attorney” to delegate authority to a subordinate, we follow the methodology prescribed by the federal courts. “Federal courts generally determine the meaning of a statute by examining its text and structure and, if necessary, its legislative history.” *Corp. of Presiding Bishop v. City of West Linn*, 338 Or 453, 463, 111 P3d 1123 (2005); *see also City of Eugene v. Comcast of Oregon II, Inc.*, 359 Or 528, 545, 375 P3d 446 (2016) (same).

The text of section 2516(2) authorizes only certain officials to seek court-authorized wiretaps. Specifically, that statute provides that “[t]he principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof,” may apply “to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications,” if also authorized to do so “by a statute of that State.”

² The parties do not appear to dispute that ORS 133.724(1) permits Oregon district attorneys to delegate their authority to submit wiretap applications. The state recognizes, however, that the dispositive question is whether federal law prohibits that delegation of authority. *See, e.g., Villa v. Maricopa Cty.*, 865 F3d 1224, 1230 (9th Cir 2017), *cert den*, ___ US ___, 138 S Ct 1696 (2018) (citing numerous cases recognizing proposition that federal wiretapping law “sets forth minimum procedural requirements for state and federal orders authorizing wiretapping” and preempts less restrictive state requirements).

The state does not dispute that, in Oregon, the “principal prosecuting attorney” of a county is the district attorney and not deputy district attorneys. The state nevertheless asserts that, despite textual use of the term “principal prosecuting attorney,” the statute is “silent” on whether that officer may delegate authority to apply for a wiretap warrant. The state urges us to understand that “silence” as implicit authorization for the delegation.

We are not convinced. Section 2516(2) sets specific limitations on the officials who are authorized to apply for wiretaps. It does not allow *any* prosecuting attorney to apply, but only a “principal prosecuting attorney.” *Id.* Even then, applications by that person must also be expressly authorized by state statute. *See id.* (application must be made by an “attorney *** authorized by a statute of that State to make [that] application”). Although the statute may not prohibit delegation in express terms, its specificity implies that prohibition.

Moreover, important context for the meaning of section 2516(2) can be found in the related provision that specifies the *federal* officials who are authorized to make application for wiretaps, section 2516(1), which the Supreme Court has construed as precluding the kind of delegation that the state proposes here. *See United States v. Giordano*, 416 US 505, 94 S Ct 1820, 40 L Ed 2d 341 (1974). Like section 2516(2), section 2516(1) identifies specific officers who are authorized to apply for a wiretap:

“The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General ***.”

(Footnote omitted.) Both provisions were adopted as part of the Omnibus Crime Control and Safe Streets Act of 1968. *See Giordano*, 416 US at 507 (so noting). The Court in *Giordano* concluded that Congress intended section 2516(1) to be a limitation on the power to authorize federal wiretap applications. *Giordano*, 416 US at 514.

The United States in *Giordano* had argued that the Attorney General could permissibly delegate authority to an executive assistant to approve wiretap applications. *Id.* at 512-13. It noted that there were federal statutes expressly vesting all functions of the Department with the Attorney General, who was then authorized to delegate that authority to others. *Id.* at 513.³

But the Court rejected that argument. *Id.* at 523. Although acknowledging that section 2516(1) did not expressly prohibit delegation, the Court held that the provision, “fairly read, was intended to limit the power to authorize wiretap applications to the Attorney General himself and to any Assistant Attorney General he might designate.” *Giordano*, 416 US at 514.

The Court explained that the overall structure of the act showed a congressional intent to limit when wiretaps would be permitted at all. *Id.* at 514-15. Conceding that the statute “is not as clear in some respects as it might be,” the Court concluded that it was “at once apparent” that Congress intended to “impose[] important preconditions to obtaining any intercept authority at all.” *Id.* at 515. “[T]he clear intent [was] to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications.” *Id.* As regards the officers authorized to apply, the Court explained that “[t]he mature judgment of a *particular, responsible* Department of Justice official is interposed as a *critical precondition* to any judicial order.” *Id.* at 515-16 (emphases added).

The Court also examined the extensive legislative history behind the act, which dated back to an original proposal in 1961 that would have allowed the United States Attorney General, as well as the Executive Assistant and any United States Attorney, to apply for a wiretap. *Id.* at

³ The Court cited 28 USC sections 509 (“All functions of other officers of the Department of Justice and all functions of agencies and employees of the Department of Justice are vested in the Attorney General [subject to identified exceptions].”) and 510 (“The Attorney General may from time to time make such provisions as he considers appropriate authorizing the performance by any other officer, employee, or agency of the Department of Justice of any function of the Attorney General.”). *Giordano*, 416 US at 513.

516-22. At that time, the Department of Justice had itself requested “that the authority to approve applications be substantially narrowed so that the Attorney General could delegate his authority only to an Assistant Attorney General.” *Id.* at 516. The drafter of the operative text later testified that “I would not want this equipment used without high level responsible officials passing on it.” *Id.* at 518 (quoting Hearings on Anti-Crime Program before Subcommittee No. 5 of the House Committee on the Judiciary, 90th Cong, 1st Sess, 1379 (1967) (testimony of Professor G. Robert Blakey)).

The Court also reviewed the relevant sections of the Senate report regarding the act that created section 2516(1). *Giordano*, 416 US at 520 (discussing S Rep 90-1097, 90th Cong, 2d Sess, 96-97, to which we will turn shortly). The Court concluded that that report was “particularly significant in that it not only recognizes that the authority to apply for court orders is to be narrowly confined but also declares that it is to be limited to those responsive to the political process.” *Id.*

The Court’s conclusion—that Congress intended section 2516(1) to circumscribe the particular federal officials who have the authority to apply for wiretaps—provides significant context for what the same Congress intended to convey by specifying particular state officials in section 2516(2). It supports our conclusion, based on the text of section 2516(2), that Congress intended paragraph (2) to circumscribe the particular state officials who have the authority to apply for wiretaps.

The state contends, however, that a later congressional enactment provides context pointing to a different interpretation of section 2516(2). The provision that the state identifies was added by the 1970 Congress to the Code for the District of Columbia, the codification of general and permanent laws relating to the District. The state understands that 1970 law to expressly permit the United States Attorney for the District of Columbia to delegate authority to apply for a wiretap to assistants and to “investigative or law enforcement officer[s].” *See* Pub L 91-358, § 210(a), 84 Stat 473, 616-17, 620 (1970) (codified at DC Code §§ 23-541(11),

23-546(a)). Notably, the District of Columbia is defined as a “state” for purposes of 18 USC section 2516(2). 18 USC § 2510(3). Thus, according to the state, the 1970 Congress’ decision to allow delegation of the United States Attorney’s wiretapping authority in the District of Columbia suggests that the 1968 Congress intended to permit similar delegation of the wiretapping authority by principal prosecuting attorneys in the 50 states.

The state’s proposal, however, extends beyond the inferences that reasonably may be drawn from the District of Columbia statute. At least with respect to the wiretapping provisions, there is no basis for inferring that the intent of the 1970 Congress can be imputed to the 1968 Congress. As defendant emphasizes, the composition of the two Congresses was different. Moreover, the drafters of the 1970 law identified the delegation provision as one that would “supersede” provisions of the 1968 wiretapping law “in cases of irreconcilable conflict.” Pub L 91-358, § 210(a), 84 Stat 627 (DC Code § 23-556(b)). At least one member of Congress described the 1970 legislation as containing “broad and general wiretap authority going far beyond the limited authority of Title III of the 1968 Omnibus Crime Bill[.]” *Crime in the National Capital: Hearings on S. 2601 Before the S Comm on the District of Columbia*, 91st Cong 2077 (Mar 23 and Apr 2, 1970) (statement of Sen Ervin).

The state also points to one sentence in the senate report for the 1968 Act, which refers to “[t]he issue of delegation” being “a question of State law.” S Rep 90-1097, 90th Cong, 2d Sess, *reprinted in* 1968 USCCAN 2112, 2187. The broader context of the report’s discussion of section 2516(2), however, significantly undermines the weight that the state ascribes to the isolated sentence. The report’s discussion of section 2516(2) repeatedly emphasizes that the intent of the proposed provision was to centralize authority and restrict who among state officials may apply for wiretaps. The relevant paragraph of the report explains that “[t]he intent of the proposed provision is to provide for the centralization of policy relating to statewide law enforcement in the area of the use of electronic surveillance in the chief prosecuting

officer of the State.” *Id.* In those states where the absence of an attorney general (or equivalent) makes it necessary for “policymaking” to “move down to the next level of government,” “[t]he intent of the proposed provision is to centralize areawide law enforcement policy in [that officer].” *Id.* And the paragraph concludes that, “[w]here there are both an attorney general and a district attorney, either could authorize applications,” but that “[t]he proposed provision does not envision a further breakdown.” *Id.*

Those statements of intent to centralize and limit the authority of state officials to pursue wiretaps are similar to the statements of intent to centralize and limit the authority of federal officials that the Court in *Giordano* considered to be so persuasive. *See Giordano*, 416 US at 520 (discussing S Rep 90-1097, 90th Cong, 2d Sess, 96-97). The statements of intent persuaded the Court in *Giordano* that section 2516(1) prohibits the delegation of wiretapping authority beyond the specific officials identified in that section, despite a federal statute that authorized the Attorney General to delegate various other duties. *Id.* at 514, 520. The Court’s reasoning persuades us that—just as Congress did not intend that section 2516(1) would permit delegation beyond the specified federal officers—Congress did not intend that section 2516(2) would permit delegation beyond the specified state officials. Consistent with that restriction, Oregon law can authorize “the principal prosecuting attorney” of a political subdivision of the state “to make application,” but that is the only delegation of authority that Congress has permitted.

That conclusion should mean that the applications by a deputy district attorney here were not authorized applications for wiretaps. But the state urges us to follow the holdings of some courts from other states and federal districts that have upheld wiretaps despite something less than literal compliance with the application limits of section 2516(2). *See, e.g., State v. Verdugo*, 180 Ariz 180, 183, 883 P2d 417, 420 (Ariz Ct App 1993) (upholding state authorization statute that court concluded “substantially complies” with federal wiretapping statute). The state acknowledges that those decisions are not binding on this court and that the issue is one on which jurisdictions “have not reached

a uniform interpretation of section 2516(2).⁴ Nevertheless, the state similarly urges us to allow wiretap applications that comply with the purpose of section 2516(2).

What the state misses in proposing a focus on congressional intent is that, as we have already explained, Congress' purpose in narrowly circumscribing the state and federal officials who may apply for wiretaps was to centralize and limit the exercise of that authority. Even the purpose-driven decisions most favorable to the state do not stray as far from the requirements of section 2516(2) as the state would have us stray; those courts still have required some active involvement on the part of the "principal prosecuting attorney"—by authorizing the particular application, reviewing the merits of the particular application, or both. See *Verdugo*, 180 Ariz at 182-84, 883 P2d at 419-21 (upholding statute that permitted applications by "such prosecuting attorneys as [the attorney general or the county attorney] may designate in writing;" and noting that applications had been supported by affidavit of the county attorney); *State v. Marine*, 464 A2d 872, 877-78 (Del 1983) (wiretapping application that was personally authorized by state Attorney General by phone—but signed by a deputy—satisfied the legislative purpose, "the centralization of authorization authority in the Attorney General"); *Commonwealth v. Vitello*, 367 Mass 224, 231-32, 257-58, 327 NE2d 819, 825-26, 839 (1975) (concluding that special designation under state statute comported with section 2516(2) as long as

⁴ Some courts have interpreted section 2516(2) as strictly limiting authority to apply for wiretaps to the "principal prosecuting attorney." See, e.g., *State v. Bruce*, 295 Kan 1036, 1044, 287 P3d 919, 924-25 (2012) (holding that section 2516(2) "allows no such delegation of wiretap order applications by 'the principal prosecuting attorney of any State'"); *State v. Frink*, 296 Minn 57, 75, 206 NW2d 664, 674 (1973) (rejecting conclusion that assistant county attorney could apply for wiretap, despite state statute generally authorizing assistant county attorney to exercise authority of county attorney; neither state or federal statute "intends that at the county level anyone other than the 'principal prosecuting attorney' *** shall have the power to initiate an electronic surveillance"). Others employ a "substantial compliance" standard that permits only slight deviation from the federal requirements. See *Villa*, 865 F3d at 1233-34 (wiretap application failed to satisfy Arizona's "substantial compliance" standard, although application had been expressly authorized by the Maricopa County Attorney, because the application was made by a deputy and did not state that the County Attorney "was personally familiar with any evidence providing probable cause that would justify a wiretap on any of those numbers or persons").

“the district attorney *** [gave] full and fair review of the grounds asserted for seeking a wiretap warrant,” did so “on a case by case basis only,” and the authority was “specifically granted in writing”); *State v. Peterson*, 841 P2d 21, 22, 24 n 1 (Utah Ct App 1992) (“Here, the Utah County Attorney prepared a document specifically authorizing Deputy County Attorney Taylor to apply for the wiretap order [of a particular phone], thus fulfilling the requirements of both the federal and state acts”).⁵

In this case, we need not decide whether to reject the reasoning that has motivated other courts to conclude that “substantial compliance” with the application requirements of the federal wiretap act is enough, because the wiretap applications in this case fall below even the standards set in the decisions that the state views as persuasive. The most that is shown here regarding involvement of the “principal prosecuting attorney” in the wiretap applications at issue is a generic claim that the Washington County District Attorney had delegated his authority to file wiretap applications. As far as the applications show, the district attorney could have given a blanket oral authorization to all assistant district attorneys to file wiretap applications in any case where they see fit. Indeed, the state affirmatively argues that “it is irrelevant whether the district attorney was specifically aware of any particular wiretap application.” That is far too similar to the blanket delegation that the Court in *Giordano* refused to authorize. See *United States v. Giordano*, 469 F2d 522, 524 (4th Cir 1972), *aff’d*, 416 US 505, 94 S Ct 1820, 40 L Ed 2d 341 (1974) (referring to “the ‘Alice in Wonderland’ world of [United States] Justice Department wiretap applications,” in which “neither [Attorney General] Mitchell nor [Assistant Attorney General] Wilson had heard of the *Giordano* application or signed the letters

⁵ The state also cites *People v. Vespucci*, 75 NY2d 434, 554 NYS2d 417, 553 NE2d 965 (1990), in which the court took a slightly different approach. There, the state statute had authorized wiretap applications by “the deputy attorney general in charge of the organized crime task force,” and the court reasoned that the nature of the state’s Organized Crime Task Force made the director a “principal prosecuting attorney” for purposes of section 2516(2). *Vespucci*, 75 NY2d at 438-40, 554 NYS2d at 419-20, 553 NE2d at 967-68 (citation and emphasis omitted). Here, the state has not contended that a deputy district attorney can be considered a “principal prosecuting attorney,” and the state identifies no court that has interpreted the term that broadly.

bearing their respective initials and signature”).⁶ None of the cases identified by the state appears to have approved such open-ended delegation, and it is beyond what even a “substantial compliance” standard would support. The trial court correctly held that the wiretaps in this case were unlawful.

3. *Whether there is a “good faith” exception to suppression*

The state argues that, regardless of whether the wiretaps were lawful, the trial court erred in suppressing the evidence that the state obtained through those wiretaps. It asks us to conclude that law enforcement had obtained the evidence in good faith reliance on the wiretap warrants and, on that basis, that the evidence should not be suppressed. We reject that argument.

The “good faith” principle on which the state relies is a court-created exception to the court-created rule that evidence obtained in violation of the Fourth Amendment should be excluded. The “good faith” doctrine was first recognized in *United States v. Leon*, 468 US 897, 104 S Ct 3405, 82 L Ed 2d 677 (1984), regarding an invalid search warrant. The Court there held “that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion.” *Id.* at 922. The Court premised its creation of a good faith exception on the fact that “[t]he Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands.” *Id.* at 906. It reasoned that “[t]he wrong condemned by the [Fourth] Amendment is fully accomplished by the unlawful search or seizure itself, and the exclusionary rule is neither intended

⁶ As the First Circuit stated in *United States v. Smith*, 726 F2d 852, 858 (1st Cir 1984), *cert den*, 469 US 841 (1984), such a blanket delegation would “frustrat[e] the twin congressional objectives of policy uniformity and political accountability, and would constitute an abdication of responsibility.” See also *Bruce*, 295 Kan at 1036-37, 1043, 287 P3d at 920, 924 (state attorney general had given assistant attorney general blanket delegation of all authority to make wiretap applications in all cases; court could not “perceive Congress intended that at any given time the number of persons in Kansas who may obtain a wiretap order is limited only by the number of assistant attorneys general and county attorneys in existence at the particular time” (internal quotation marks and citation omitted)).

nor able to cure the invasion of the defendant's rights which he has already suffered." *Id.* (internal quotation marks and citations omitted).

There is no basis for applying the doctrine in the context of a statute that specifically provides for the suppression and exclusion of evidence intercepted through an unlawful wiretap. As noted above, suppression is required by two different provisions of the federal wiretap act. The first is section 2515, which provides, in part:

"Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court *** of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter."

The second is section 2518(10)(a), which provides, in part:

"Any aggrieved person in any trial, hearing, or proceeding in or before any court *** of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted[.]"

In addition to those suppression provisions, the law prohibits the intentional disclosure or use of the content of intercepted communications, if the person knows or has reason to know that they were unlawfully intercepted. 18 USC § 2511(1)(c), (d).

The Court in *Giordano* emphasized that "unlawfully intercepted" is "not limited to constitutional violations," and it concluded that "Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device." 416 US at 527 (quoting 18 USC § 2518(10)(a)(i)).

The Court also held that, where there is a failure to satisfy the requirement that only the named officials have authority to apply for a wiretap, that failure requires suppression:

“We are confident that the provision for pre-application approval was intended to play a central role in the statutory scheme and that suppression must follow when it is shown that this statutory requirement has been ignored.”

Id. at 528.

Although *Giordano* predates the Court’s adoption of a “good faith” exception to the Fourth Amendment exclusionary rule, *Giordano* remains controlling precedent on the question of whether evidence intercepted through an unlawful wiretap must be suppressed. Moreover, the Court has since reiterated *Giordano*’s holding, albeit in a different context. *Dahda v. United States*, ___ US ___, ___, 138 S Ct 1491, 1499, 200 L Ed 2d 842 (2018). Whereas *Giordano* had involved suppression due to a defective wiretap *application* under section 2518(10)(a)(i), in *Dahda*, the Court addressed suppression under section 2518(10)(a)(ii), which provides for suppression of evidence intercepted through a wiretap *order* that is “insufficient on its face.” *Dahda*, ___ US at ___, 138 S Ct at 1499-1500. Despite recognizing that the suppression requirement under subparagraph (ii) was less rigid than that required for an unlawful application under subparagraph (i), the Court reiterated *Giordano*’s holding that suppression under section 2518(10)(a)(i) was required when “the Government’s use of a wiretap *** violates a statutory provision that reflects Congress’ core concerns.” *Dahda*, ___ US at ___, 138 S Ct at 1498-99.

In summary: We agree with the trial court that the wiretap applications here were not made by an authorized applicant under section 2516(2), and the wiretap orders were, thus, invalid. Given that proper authorization was a core concern of Congress in enacting the federal act and that Congress expressly provided for exclusion of evidence intercepted through an unauthorized application, the trial court correctly granted defendant’s motion to suppress the evidence as “unlawfully intercepted” under section 2518(10)(a)(i).

B. *Search Warrants*

1. *Motions to suppress and trial court order*

The state's second assignment of error challenges the court's consolidated ruling that granted "Defense Motions 104, 107-129," all of which sought suppression of evidence obtained from the search warrants for cell phone records. Defendant's motions separately challenged the validity of 24 different search warrants but raised arguments that were common to all.

The earliest warrant that defendant challenged was the September 22 warrant for records related to the -2494 phone number (Defense Motion 104).⁷ He argued that the affidavit in support of that warrant failed to establish probable cause and, alternatively, that the warrant lacked specificity and was overbroad. Because of those defects, defendant contended, evidence obtained through the warrant must be excluded from trial and must be stricken from all subsequent warrant applications before the court analyzed defendant's challenges to those later warrants. In his separate motions challenging the later warrants, defendant argued that the affidavits in support failed to establish probable cause, especially once the court struck the evidence that had been unlawfully obtained through the prior warrants. He also argued that the later warrants themselves lacked specificity and were overbroad.

The state filed a consolidated response to defendant's motions to suppress the evidence obtained through the cell phone search warrants ("Omnibus Consolidated Responses to Defense Motions #104-129"). The response did not specifically address defendant's motion 104 regarding the September 22 warrant; it instead asserted generically that all of the search warrants were based on probable cause and were sufficiently specific and not overbroad.

The trial court agreed with defendant and granted the motions to suppress cell phone records. In its written order, the court addressed defendant's "Motions 104,

⁷ The earliest warrant that the state obtained was for the records related to RBH's cell phone. Defendant has not challenged that warrant.

107-129” under a single heading in which it both described one warrant specifically and ruled on the challenges that were common to all warrants.⁸ The court specifically quoted text from the September 22 warrant but noted that the information requested in the other warrants was “substantively the same throughout.” The court concluded that each of the warrants amounted to a “general warrant,” was “overbroad,” and was not supported by “particular facts to support anything more than a suspicion that evidence of the suspected crime(s) would result.” The court also specified that its probable cause rulings with respect to later warrants had been based on an evaluation of the affidavits after striking evidence obtained from earlier invalid warrants:

“Finally, to the extent that affidavits rely on evidence obtained from earlier search warrants that have been suppressed, the court struck that evidence from subsequent affidavits and concludes there is no probable cause to support the warrant.”

On appeal, the state argues that all of the warrants were supported by probable cause and were sufficiently specific and that none of the warrants was overbroad.

2. *September 22 warrant*

We begin with the trial court’s ruling that the September 22 warrant for records related to the -2494 phone number was invalid and that the evidence obtained must be suppressed and stricken from all later affidavits. Because the trial court struck that information from later search warrant applications and then concluded that the resulting warrants lacked probable cause, and because the later warrants all relied to some extent on evidence obtained from the September 22 warrant, the fall of that warrant was effectively the domino that caused the rest of the chain to fall.⁹

⁸ The trial court also granted defendant’s motions to suppress number 105 and 106, but on a different basis, and that ruling is not before us on appeal.

⁹ The state asserts in its reply brief that it “does not understand the trial court to have suppressed any evidence obtained from” the September 22 warrant. The state points to a comment in a different trial court ruling that, “after striking the information suppressed from prior search warrants what remains is the evidence from the 1st search warrant,” but the “1st search warrant” in this case was the unchallenged warrant for records of RBH’s cell phone. Although the “1st search warrant” reference might have been ambiguous in the abstract, the

As described above, the affidavit in support of that warrant described the two cell phones on the victim's body and recited that one of those phones had been called repeatedly by phone number -2494 over a period of eight minutes close to the time of the murder: four calls that did not connect, four calls that went to voicemail, and a final call that connected and lasted for four minutes. The final call from phone number -2494 had connected to the victim's phone at approximately the same time that a witness had reported hearing "popping sounds" near where the victim's body was found. The affidavit asserted that those facts showed probable cause to believe that records for phone number -2494 "will help identify people who may be able to provide witness information or details about what was happening or have information about the murder." And the affiant asked the court to issue a search warrant to obtain the records for that phone number.

The first part of the resulting search warrant was consistent with the stated probable cause: that is, it directed T-Mobile to provide information relevant to who owned the phone (*e.g.*, subscriber's name, address, date of birth). The warrant went on, however, to request the production of an extensive amount of additional information regarding the -2494 number. For a 60-hour period surrounding the estimated time of the murder—"from 8:00 a.m. (Pacific Coast Time) September 19th, 2017 through 8:00 p.m. (Pacific Coast Time) September 21[st], 2017"—the warrant directed T-Mobile to produce "complete call detail records" of every phone call and text message sent or received by -2494, "including, but not limited to, dates and times of use, duration of use, and the destination and origination numbers"; details of all "data usages" by -2494 (including the addresses for every website visited); and all "location data including any and all cell site data and GPS location information." As particularly relevant here, the warrant required T-Mobile to produce the content of defendant's communications:

court's written order expressly grants defendant's motion 104, and defendant's motion 104 was directed solely at suppressing the evidence obtained through the September 22 warrant. Indeed, the court's explanation in that ruling for why the warrants were defective quotes the text of the September 22 warrant and simply describes the later warrants as comparable. Thus, it is clear to us that the court suppressed the evidence obtained from the September 22 warrant.

“Any and all incoming and/or outgoing SMS and/or MMS messages and related records from 8:00 a.m. (Pacific Coast Time) September 19th, 2017 through 8:00 p.m. (Pacific Coast Time) September 21[st], 2017; including all meta-data such as date, time, destination phone (or IP) number and origination phone (or IP) number, and geotags (or geographical coordinates)[.]”

The trial court granted suppression of the material obtained through the September 22 warrant under Article I, section 9, of the Oregon Constitution. That section provides:

“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.”

This court recently explained that Article I, section 9, imposes an “objective test of whether the government’s conduct would significantly impair an individual’s interest in freedom from scrutiny, *i.e.*, his privacy.” *State v. Mansor*, 363 Or 185, 206-07, 421 P3d 323 (2018) (internal quotation marks omitted). The obligations imposed by 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,” and accordingly it “applies to every possible form of invasion—physical, electronic, technological, and the like.” *Id.* at 207 (internal quotation marks omitted).

The standard for whether a warrant is issued “upon probable cause,” Or Const, Art I, § 9, is whether the state has established “an objectively reasonable belief that seizable things will probably be found in the location to be searched,” *State v. Foster*, 350 Or 161, 172, 252 P3d 292 (2011). “The test is one of probability, which requires more than mere suspicion or a mere possibility.” *Id.* In evaluating probable cause on appeal, we ask whether a neutral magistrate could conclude, based on the facts in the supporting affidavit and the reasonable inferences from those facts, whether there was probable cause. *State v. Castilleja*, 345 Or 255, 265, 192 P3d 1283 (2008).

Although the trial court granted defendant's motion with respect to the September 22 warrant on multiple, alternative bases, the state has never contended that suppression remedy would be different if only one of those bases invalidated the warrant. Thus, it is enough for purposes of this appeal to address only one: the ruling that the warrant was "overbroad." Overbreadth is an aspect of the requirement in Article I, section 9, that warrants issue only "upon probable cause, *** and particularly describing the place to be searched, and the person or thing to be seized." *See Mansor*, 363 Or at 212 (emphasizing that the particularity requirement is informed by the "related, but distinct, concepts" of specificity and overbreadth). The constitutional requirement means that, "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." *Id.* (internal quotation marks omitted); *see Wayne R. LaFave*, 2 *Search and Seizure* § 4.6(a), 752 (6th ed 2020) ("[A]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based."). The probable cause shown by the supporting affidavits, thus, constrains the scope of the lawful search. *See State v. Blackburn/Barber*, 266 Or 28, 34, 511 P2d 381 (1973) (explaining that, if the warrant "makes possible the invasion of [an] interest in privacy without the foundation of probable cause for the search, the warrant is too broad and therefore constitutionally defective").

In this case, the affidavit in support of the September 22 warrant set out precisely the state's asserted probable cause: that the caller was a witness whom the state needed to identify:

"The records are going to provide evidence of the crime of murder because the records will help identify people who may be able to provide witness information or details about what was happening or have information about the murder because the calls were so close in time to reports of 'pops' by neighbors."

The asserted probable cause—that the person (or people) who called from phone number -2494, at approximately the time that shots might have been fired, "may

be able to provide” information or details relevant to the murder—might support a search of records that would identify the person who made those calls. But the state offers no explanation for how the asserted probable cause justifies a search of the account holder’s entire record of cell phone calls, text messages, internet usage, and locations for a period of 60 hours. Nor can we identify a basis to conclude that the invasion of the account-holder’s privacy interest in that information is supported by “the foundation of probable cause for the search.” See *Blackburn/Barber*, 266 Or at 34. Thus, we agree with the trial court that the search authorized by the September 22 warrant was “broader than the supporting affidavit supplies probable cause to justify.” See *Mansor*, 363 Or at 212 (internal quotation marks omitted).

The state also asserts on appeal that the affidavit in support of the September 22 warrant showed probable cause for a reasonable magistrate to conclude that the user of phone -2494 was “involved in the homicide.” Among the multiple impediments to that argument is that the premise is not sound. The fact that someone repeatedly tried to reach the victim, and ultimately connected for a short phone conversation, shortly before the victim was shot does not make it probable that the caller was involved in the shooting. And the state does not explain how that evidence establishes an objectively reasonable probability that the caller was *involved* in the murder. At best, that might be a possible explanation for the calls; but possibility is not enough. See *Foster*, 350 Or at 173 (observing that “probable cause is harder to establish based on observations” that would be “equally or more consistent with innocent circumstances”); *State v. Carter/Grant*, 316 Or 6, 13, 848 P2d 599 (1993) (“Probable cause is necessary to support a warrant, not merely one possibility, among many.”).

We therefore agree with the trial court: The September 22 warrant was overbroad.

3. *Partial suppression as remedy for September 22 warrant*

As a form of alternative argument, the state contends that some of the evidence obtained through the unlawful search warrant should not have been suppressed

because defendant lacked a protected privacy interest in at least some of the “third-party” records that the state obtained. According to the state, defendant had a protected privacy interest only in some location data and in the contents of messages on his account. Under that theory, the remaining records could have been lawfully obtained from the cell phone service without a warrant and, thus, should not have been suppressed. As pertinent to our analysis of the September 22 warrant, the state’s theory of partial suppression—limited to the evidence in which defendant had a protected privacy interest—would require the trial court to reevaluate which facts must be excised from the later warrant affidavits and reevaluate whether the affidavits, as modified, establish probable cause to support the warrants.

Defendant disagrees with the state’s “third-party” reasoning. According to defendant, the principles that govern a person’s privacy interest in information contained on a cell phone apply equally when that information is maintained by a cell phone service.

We need not resolve in this case the parties’ dispute over the extent of defendant’s protected privacy interest, because the state’s alternative argument for partial suppression is unpreserved. And we decline to undertake in the first instance the kind of parsing of information obtained through the warrant that the state now seeks with its alternative argument. As indicated above, the state filed a consolidated response to all defendant’s motions to suppress the warrants at issue here. In it, the state asserted that the supporting affidavits for the warrants established probable cause; that the warrants themselves described with sufficient particularity the items to be seized; and that the warrants were narrowly tailored so as not to exceed the probable cause shown. The state did not separately address defendant’s motion to suppress evidence obtained through the September 22 warrant—either to explain why the breadth of the warrant was supported by probable cause or to identify the records that the state believed it could have obtained without a warrant.

To the extent that the state addressed the scope of protected privacy interests with respect to any of the search

warrants, it made a generic statement that the *enhanced* privacy interests that apply to the data stored on personal electronic devices do not extend to “records and data stored with third-parties,” but it acknowledged that this court has “suggested” that “a customer has a constitutionally protected privacy right in the contents of his or her past communications,” even if “stored and kept with a service provider.” Those arguments did not address which of the individual categories of evidence sought by the September 22 warrant—or by any of the other search warrants—was information in which defendant lacked a protected privacy interest. Nor did the state identify which pieces of information it believed it could have obtained without the September 22 warrant. And it did not explain how the analysis of probable cause for the later warrants would be different if some of the information obtained through the September 22 warrant could have been lawfully obtained without a warrant.

In other words, the state litigated the motions to suppress on an all-or-nothing basis. It did not argue that the court should deny the motion to suppress only in part even if the court agreed with defendant’s challenge to the warrant. Under the circumstances, the state did not preserve its argument that the trial court should have suppressed only some—but not all—of the evidence obtained unlawfully. *See State v. Jones*, 339 Or 438, 441, 121 P3d 657 (2005) (when “the state did not argue to the trial court that differing circumstances surrounding each interview provided separate grounds for admitting the evidence pertaining to each interview,” state had failed “to preserve for appeal any alternative argument supporting the admissibility of any part of the evidence”); *see also State v. Sarich*, 352 Or 601, 618, 291 P3d 647 (2012) (explaining that, “when a party offers evidence as a whole and the evidence is rejected by the trial court, the appellate court will affirm the trial court’s ruling if any part of the evidence is inadmissible”). Before us, the state does not dispute that it obtained at least some information in which defendant had a protected privacy interest through the overbroad September 22 warrant. *See State v. Johnson*, 340 Or 319, 336, 131 P3d 173 (2006) (“Defendant clearly had a cognizable privacy interest in the *content* of his telephone calls.” (Emphasis in original.)). Thus, the trial court

correctly granted defendant's motion to suppress evidence obtained through the overbroad September 22 warrant, and we decline to consider whether the state might have been entitled to have the motion denied in part. Accordingly, we conclude that the trial court did not err in suppressing the entirety of the evidence obtained from the September 22 warrant.

4. *Later warrants*

Our conclusion that we must affirm the trial court's suppression of all evidence obtained through the overbroad September 22 warrant cascades into our analysis of the rest of the search warrants at issue here. The state relied on evidence obtained through the September 22 warrant to obtain the next round of warrants a few days later, and then continued to rely on the evidence derived from the September 22 warrant to obtain each subsequent warrant that defendant challenged. In its ruling, the trial court expressly found that,

“to the extent that affidavits [for later search warrants] rely on evidence obtained from earlier search warrants that have been suppressed, the court struck that evidence from subsequent affidavits and concludes there is no probable cause to support the warrant.”

The state has not challenged that conclusion, except in challenging the court's underlying conclusion that the evidence obtained with the earlier warrants must be suppressed. The state, for example, did not (and does not) argue that the affidavits for any of the later suppressed search warrant established probable cause *even after* excising the evidence that the state unlawfully obtained from the overbroad September 22 warrant and those warrants that relied on that evidence to establish probable cause. And the state did not (and does not) make an argument of that type with respect to any of the subsequent affidavits that the state relied on to obtain the subsequent search warrants. Thus, the court did not err in concluding that the 23 subsequent search warrants were not supported by probable cause, after excising from the supporting affidavits evidence that the state derived from the unlawful September 22 search.

In summary: We conclude that the trial court did not err in determining the September 22 T-Mobile warrant to be overly broad. Because the state now concedes that at least some of the information it obtained required a valid warrant, and because the state did not preserve its alternative argument that that evidence should have been suppressed only in part, we conclude that the trial court did not err in suppressing all of the evidence obtained with the warrant. We also conclude that the trial court did not err in granting defendant's motions to suppress evidence obtained through the remaining 23 search warrants, which lacked probable cause once the information derived from the September 22 warrant had been excised.

III. CONCLUSION

For the foregoing reasons, we affirm the challenged rulings by the trial court.

The order of the circuit court is affirmed.