

IN THE COURT OF APPEALS OF THE
STATE OF OREGON

STATE OF OREGON,
Plaintiff-Respondent,

v.

RONALD WESLEY FRIDDLE,
Defendant-Appellant.

Josephine County Circuit Court
13CR0160; A155347

Michael Newman, Judge.

Submitted August 27, 2015.

Peter Gartlan, Chief Defender, and Sarah Laidlaw, Deputy Public Defender, Office of Public Defense Services, filed the brief for appellant.

Ellen F. Rosenblum, Attorney General, Anna M. Joyce, Solicitor General, and Susan G. Howe, Assistant Attorney General, filed the brief for respondent.

Before Lagesen, Presiding Judge, and Garrett, Judge, and Haselton, Senior Judge.

HASELTON, S. J.

Reversed and remanded.

HASELTON, S. J.

Defendant appeals an amended judgment of conviction for unlawful possession of more than one ounce of marijuana, ORS 475.864(2), assigning error to the denial of a motion to suppress (marijuana) evidence discovered during the execution of a warrant authorizing the seizure and forensic examination of the contents of personal electronic devices. Specifically, defendant contends that, because the warrant application established probable cause to examine the contents of only a single cell phone and the home security system at his residence, the predicate warrant was overbroad—and, hence, invalid—as authorizing the search of defendant’s residence for other electronic devices and the seizure and examination of such devices; thus the consequent search of a gun safe, which yielded the marijuana, was unlawful. For the reasons that follow, we agree with defendant, and we decline to consider the state’s alternative basis for affirmance proffered for the first time on appeal. Accordingly, we reverse and remand.

Because defendant’s appellate challenge pertains solely to the purported overbreadth of the warrant, our review focuses on the relationship between the content of the affidavit submitted in support of the warrant application and the content of the warrant, specifically the electronic devices to be seized and searched (including here, forensic examination of their electronic contents). *See generally* [State v. Mansor](#), 279 Or App 778, 791-803, ___ P3d ___ (2016). Accordingly, the facts material to our review of the denial of suppression in this case are those recited, without controversy, in the supporting affidavit. *Id.*

Around midnight on December 16, 2012, defendant and his then-girlfriend, W, had an altercation at defendant’s home in Grants Pass. Oregon State Police Trooper McClendon responded to a call about the altercation and spoke to W, who was no longer at defendant’s home, about the incident. W told McClendon that she and defendant had had a heated argument and that, as she tried to leave the home with her belongings, defendant had punched her in the face—“[j]ust clocked me.”

W also told McClendon that, at some point during the altercation, before defendant punched her, he “probably hit record.” In a follow-up interview, W elaborated on that comment. As recounted in McClendon’s affidavit in support of the warrant application, W told him that

“[defendant] kept a security system at his residence ***. [W] said the system allows [defendant] to access his cameras from his cell phone and see a live feed of the house. [W] explained to me one time while [defendant] was working, [W] turned one of the cameras to face the wall. [W] said when [defendant] found out about this he was angry. [W] told me there was a camera facing the area in which the assault took place and believed there was a possibility the assault was captured on the security system.”

McClendon subsequently spoke with defendant, who acknowledged that he had struck W but said that he had done so only in self-defense, as he was trying to block one of W’s punches. Defendant told McClendon that he “had recorded the whole conversation” with W, and, when asked, allowed McClendon to listen to “the audio” on a cell phone. That recording captured a screaming argument, laced with profanities, as well as sounds of glass breaking, “a struggle,” and “a loud thud,” which McClendon believed was a punch.¹

Nearly three months later, on March 9, 2013, McClendon applied for a warrant to seize and search the contents of, *inter alia*, various personal electronic devices and the security system at defendant’s home.² After recounting the facts just described, McClendon made the following representations:

¹ In the suppression hearing, McClendon testified that, after defendant had allowed him to listen to the audio recording of the altercation, defendant had offered to “download [that recording] through his computer onto a disk” for McClendon—and that defendant had, in fact, done so, “us[ing] that recording and that phone on his computer.” However, that information, including the specific reference to defendant’s computer, was not recounted in McClendon’s warrant application affidavit. Accordingly, it was, and is, inapposite to the determination of defendant’s overbreadth challenge.

² The warrant application affidavit also described the type and content of “digital evidence” subject to forensic examination. Here, defendant does not contend (as in *Mansor*, 279 Or App at 801-03) that the warrant was overbroad because of inadequate substantive or temporal limitations with respect to the forensic examinations of the content of individual devices. Rather, defendant contends solely that the warrant was overbroad because it encompassed some devices for which there was no probable cause to seize or conduct *any* examination.

“The make and model number of the phone in question are at this point unknown. The number to the phone is [phone number specified]. The make, model number and type of the computer are also unknown.

“It is my opinion based on my experience and training that subjects involved in criminal activity regularly use cellular telephones and cellular telephone features, *i.e.*, text-messaging, photos, recordings (audio and video) etc., to record and store photos, audio recordings and video recordings of their crimes. It is my belief that a search of the above noted cell phone *** (and other phones in [defendant’s] possession) and computer will show recordings (audio and video), of [defendant] and [W], and their interactions on the date and time in question.”³

Accordingly, McClendon averred that he had “probable cause to believe *** that evidence of the crime of Assault II will be present on the cellular phone(s), possibly [phone number specified] belonging to [defendant] or computer system located inside [defendant’s] residence.”

The warrant application sought authorization to seize and examine, as evidence of crimes “including but not limited to Assault,” “[a]ll cell phones, computers, recorders and security systems owned or operated by [defendant].” The application further sought authorization to examine such items for digital evidence, including “[g]raphic and movie files ***, which may be, or are, used to visually depict an assault taking place,” as well as text files and “[c]orrespondence” “pertaining to the crime of assault.”⁴

³ The affidavit also included generalized “training and experience”-based representations by McClendon regarding the functionality and capacity of personal electronic devices, including that “cellular phones and computers are capable of being used to send and receive text/email messages, photographs, short videos, other electronic data and voice communication” and that “cellular telephones typically have cameras that can record still images and video” and “can be used to store and disseminate those images and videos to other people.”

⁴ The warrant application also sought “authorization to search and seize all digital evidence recognizable as the fruits or instrumentalities pertaining to Assault” stored remotely on servers at third-party electronic service providers. Although the affidavit includes extensive representations about the dynamics of such remote storage and the potential for the deletion of such evidence via electronic devices, the warrant, as ultimately issued, *see* 281 Or App at ____, did not include such authorization.

The trial court issued a warrant authorizing the seizure from defendant's residence of "[a]ny" "cell phones," "[c]omputers," "[s]ecurity system," "recorders," or "[t]ablets (Ipad, Kindle, etc.)" owned or operated by defendant and the examination of such items "for evidence of the crime of Assault II."

McClendon and other officers executed the warrant at defendant's residence. Before doing so, however, McClendon had taken defendant into custody at the Oregon State Police patrol office in Grants Pass and, at that time, had seized from defendant's person the same cell phone on which defendant, in December, had played the audio recording of the incident with W.⁵ In the living and office areas of defendant's house, the officers found and seized "a couple cell phones," two cameras from the security system, and defendant's computer and hard drive. Thereafter, in defendant's garage, the officers found a gun safe large enough to hold cell phones, recording devices, cameras, and computer hardware. Inside the safe was the marijuana (93 grams) that was the subject of the criminal drug possession charge on which defendant was convicted—and the object of the motion to suppress.

In moving to suppress, defendant argued, alternatively, that the search of the safe was unlawful because (a) the search warrant was facially overbroad, and (b) in all events, the opening of the safe, after McClendon and the other officers had recovered the other items from defendant's person and home, exceeded the scope of the warrant, because, at that point, there was no reasonable likelihood that items described in the warrant would be found in the safe.

With respect to the first contention—which is the only challenge that defendant raises on appeal—defense counsel asserted that the combination of W's statements to McClendon about the security system, including defendant's ability to access that system via his cell phone, and defendant's playing of the audio recording of the altercation

⁵ The record does not disclose why McClendon had taken defendant into custody.

on his cell phone did not substantiate probable cause that any recording, or any other evidence of the alleged assault, would be found on any of defendant's electronic devices other than that particular cell phone and the security system:

"There's nothing in the affidavit *** there's no[t] even [any] allegation by Trooper McClendon that there's any reason to believe that there's any other recording than what's on the phone.

"[T]here's no factual basis in the [affidavit] to believe that there was anything other than these two things. No I-pads, no other cameras, nothing else. There was an isolated incident that was, that happened over a period of a few minutes. There were these two systems that perhaps had evidence."

The state countered that the warrant was not overbroad, because it related solely to "electronic evidence that the defendant already made Officer McClendon aware of that existed"—which, in turn, "leads an officer to know that there might be additional evidence related to this crime on X, Y, and Z piece of evidence or on other electronic means."

The trial court denied the motion to suppress. In so ruling, the court began by observing, "Trooper McClendon's affidavit could in part be described as something of a generic assertion of the relevance of cell phones to criminal activity and persons who engage in criminal activity." The trial court further noted that, although an officer's "training and experience"-related representations could certainly be material to the assessment of probable cause, the parties had not "cited to any case that specifically reviews the language of the current warrant or anything close to the substance and extent of the affidavit presented in this case." The court reasoned that, although McClendon's generalized representations regarding criminal suspects' use of electronic devices might be insufficient to substantiate probable cause, the circumstance that defendant had, in fact, used his cell phone to access and store a recording of the altercation was decisive: "Here, the police had concrete proof that the defendant had a cell phone and that he had used it in the manner that the trooper's training and experience had taught him to be the case." Consequently, and concomitantly, the trial court

reasoned that the “same or similar may be applied to *** the kinds of recording devices or storage devices, and the number of computers or storage devices that computers may have or are related to computers,” as well as to “multiple cell phones.” Accordingly, the court concluded that the warrant was not invalid as overbroad.

Thereafter, defendant entered a conditional guilty plea, and this appeal from the consequent judgment of conviction ensued.

On appeal, defendant assigns error only to the denial of the motion to suppress. His sole appellate contention is that the predicate warrant was invalid as unconstitutionally overbroad, because, defendant asserts,

“it permitted a wholesale search of defendant’s home for *any* cellular phones, computers, security systems, recorders, or tablets when the affidavit in support of the search warrant provided probable cause for the search of only two items: defendant’s cellular phone and defendant’s home surveillance system.”⁶

(Emphasis in original.) Accordingly, defendant asserts, the search of the gun safe, which yielded the marijuana, was unlawful, as undertaken during the execution of an invalid warrant.

The state remonstrates that the warrant application affidavit established that “defendant was capable of remotely accessing his security video footage from a smart phone or other internet-connected electronic device.” That, in turn, the state posits, established probable cause to seize and examine the contents of all of the electronic devices described in the warrant “both in order to obtain a copy of the recording and to prevent defendant from destroying

⁶ In support of that challenge, defendant invokes on appeal both Article I, section 9, of the Oregon Constitution and the Fourth Amendment to the United States Constitution. However, as the state notes, defendant did not develop any independent federal constitutional analysis before the trial court and does not do so on appeal.

Article I, section 9, provides, in part, that “no warrant shall issue but upon probable cause, supported by oath, or affirmation, and particularly describing the place to be searched, and the person or thing to be seized.”

it.” In that regard, the state contends that, because the evidence sought “was the non-tangible, digital video recording of defendant’s physical altercation with [W]” and because the affidavit substantiated defendant’s ability to remotely access that data, the seizure of the security system and of the cell phone defendant used to play the audio recording for McClendon did not “necessarily guarante[e] access to the sought-after video recording.”

In *Mansor*, we observed that “[t]he fundamental purpose of the constitutional particularity requirement is ‘to protect the citizen’s interest in freedom from governmental intrusion through the invasion of his privacy.’” 279 Or App at 791 (quoting *State v. Blackburn/Barber*, 266 Or 28, 34, 511 P2d 381 (1973)). In summarizing the requisites of the particularity requirement, we noted that that requirement

“implicates two analytically distinct, but frequently practically intertwined, concepts. First, the warrant, as supplemented by any attached or incorporated supporting documents, must so clearly describe the place to be searched and the items to be seized and examined that officers can, with reasonable effort, ascertain that place and those items to a reasonable degree of certainty. Second, the warrant must, to the extent reasonably possible, be drawn in such a way as to preclude seizures and searches not supported by probable cause.”

Mansor, 279 Or App at 792-93 (internal quotations and citation omitted).

Here, defendant’s challenge pertains only to the second, overbreadth component. The gravamen of such a challenge is an asserted lack of probable cause for the invasion of interests in privacy in premises or items. See *Blackburn/Barber*, 266 Or at 34 (“If the search warrant describes premises in such a way that it makes possible the invasion of [the] interest in privacy without the foundation of probable cause for the search, the warrant is too broad and therefore constitutionally defective.”); see also *State v. Ingram*, 313 Or 139, 144-46, 831 P2d 674 (1992) (summarizing particularity requirement and concluding that warrant authorizing search of “all vehicles *** associated with the occupants of said premises” was invalid as overbroad, in that executing

officers “could invade privacy interests not intended by the magistrate to be invaded and *could conduct searches not supported by probable cause.*” (emphasis added)).

That probable cause assessment is, in turn, circumscribed by the contents of the warrant application affidavit(s). See *State v. Reid*, 319 Or 65, 71, 872 P2d 416 (1994) (“[A] warrant may not authorize a search that is broader than the supporting affidavit supplies probable cause to justify.”); see also *Mansor*, 279 Or App at 801-03 (applying that construct). Here, because the warrant authorized the seizure and forensic examination of the contents of personal electronic devices, those devices are deemed, for purposes of the particularity requirement, to be “more akin to the ‘place’ to be searched than to the ‘thing’ to be seized and examined.” *Mansor*, 279 Or App at 801. Concomitantly, “that requires that the search of that ‘place’ to be limited to the ‘thing(s)’—the digital data—for which there is probable cause to search.” *Id.* Thus, our review reduces, ultimately, to whether the warrant application affidavit substantiated probable cause for the forensic examination of the contents of each of those “places”—that is, of “any” cell phones, computers, and electronic tablets owned or operated by defendant located at his residence (emphasis added).

In *State v. Williams*, 270 Or App 721, 349 P3d 616 (2015), we summarized the controlling standard of probable cause:

“When evaluating the sufficiency of a search warrant affidavit, our task is to determine whether the affidavit alleged sufficient facts to permit a neutral and detached magistrate to determine that seizable evidence probably would be found at the place to be searched. That standard requires an affidavit to do more than allege facts that support a mere suspicion that evidence will be found; even a well-warranted suspicion does not suffice. Rather, the standard of probability requires the conclusion that *it is more likely than not that the objects of the search will be found at the specified location.*”

Id. at 725 (internal citations and quotations omitted) (emphasis added); see also *State v. Verdine*, 290 Or 553, 557, 624 P2d 580 (1981) (“[A] suspicion, no matter how well founded, does not rise to the level of probable cause.”).

Applying that standard here, we conclude, as amplified below, that the warrant application affidavit did not substantiate probable cause that evidence of the alleged assault—specifically, recordings of the altercation—would be found by way of forensic examination of various devices included in the warrant, including all computers and electronic tablet devices at defendant’s residence that he owned or operated. We further conclude that the state’s alternative contention—*viz.*, that the seizure of all such devices was necessary to forestall potential “remote” deletion of recordings of the altercation stored on other electronic devices—is not cognizable on this record as an alternative basis for affirmation. Accordingly, the warrant was invalid, and the search of the gun safe, which yielded the marijuana, was unlawful.

We return to the content of the affidavit. We note at the outset—and defendant does not dispute—that the affidavit does establish probable cause with respect to the seizure and forensic examination of defendant’s home security system, based on W’s statements to McClendon, *see* 281 Or App at ____, and of the cell phone, with the specifically identified phone number, on which defendant played for McClendon the audio recording of the altercation. The critical, disputed nexus, however, is between the content of the affidavit and the other electronic devices included in the warrant. Specifically, does the affidavit substantiate not merely a “well-warranted suspicion,” *Verdine*, 290 Or at 557, but a *probability*—that is, that it was “*more likely than not*,” *Williams*, 270 Or App at 725 (emphasis added)—that an examination of the contents of those devices would disclose evidence of the alleged assault?

The warrant application affidavit discloses only two possible bases for such a circumstantial inference. The first is McClendon’s general “training and experience”-based representation that “subjects involved in criminal activity regularly use cellular telephones and cellular telephone features, *i.e.*, text-messaging, photos, recordings (audio and video) etc., to record and store photos, audio recordings and video recordings of their crimes.” *See* 281 Or App at ____. The second is the uncontroverted circumstance that defendant did, in fact, access and store an audio recording of the altercation on a cell phone identifiable by a specific phone number. That

representation and that circumstance are insufficient, individually and collectively, to establish probable cause to seize and examine the contents of the other personal electronic devices.

We begin by seconding the trial court’s characterization of McClendon’s “training and experience”-based representations as “generic.” In that regard, we note that the affidavit’s only description of McClendon’s professional training and experience was that he had served as a state police trooper for three years and had participated in “no less than 50 investigations” involving “person-to-person” crimes. Nothing in the affidavit describes any training relating to personal electronic devices and their contents as evidence in criminal investigations or any specific personal professional experience pertaining to such matters. In this context, and given the proliferation of applications for warrants authorizing the forensic examination of the contents of electronic devices, an admonition bears reiteration:

“In the context of statements regarding training and experience, *** we must not only ensure that the officer’s knowledge is connected to the facts of a particular case; we must also examine the knowledge itself. The phrase ‘training and experience,’ in other words, is not a magical incantation with the power to imbue speculation, stereotype, or pseudoscience with an impenetrable armor of veracity.”

State v. Daniels, 234 Or App 533, 541, 228 P3d 695, *rev den*, 349 Or 171 (2010); *accord State v. Holdorf*, 355 Or 812, 829, 333 P3d 982 (2014) (“We emphasize that a police officer’s training and experience, as relevant to proving particular circumstances, is not presumed based solely upon a police officer’s employment status.”).⁷

⁷ See also *State v. Farrar*, 252 Or App 256, 261-62, 287 P3d 1124 (2012) (concluding that officer’s testimony failed to substantiate reasonable suspicion of possession of methamphetamine, justifying extension of initial traffic stop, where “there was no testimony establishing the number of years that [the officer] had served as a patrol trooper ***, much less providing any indication of [the officer’s] ‘training and experience’ relating to investigating methamphetamine possession” (emphasis added)).

We appreciate that, in some circumstances, exigencies may restrict a police officer affiant’s ability to recount with particularity the officer’s pertinent training and experience. Here, however (as noted), the warrant application was submitted months after the December altercation, and the record discloses no exigency, such as the imminent destruction of evidence.

In all events—even assuming, for present purposes, the affiant’s asserted competence with respect to criminal suspects’ purported “regular” behavior in recording and storing “audio recordings and video recordings of their crimes”—nothing in the affidavit addresses the pertinent and pivotal circumstance here. Specifically, the affidavit does not address whether a suspect who has accessed and stored a recording of an event on one personal electronic device (as defendant did here) will do so on all other devices that she or he owns or operates—or on even some of those devices. Further, because the affidavit does not even refer to such a scenario, it does not (of course) address its putative likelihood. Consequently, even if the warrant affidavit could somehow support an inference of the possibility of such multiple access or retention, the affidavit does not substantiate a *probability* that defendant’s other personal electronic devices contained evidence of the alleged assault. See [*State v. Huff*](#), 253 Or App 480, 492-93, 291 P3d 751 (2012) (concluding that warranted search was unlawful because “stacking of inferences” from the content of the warrant application affidavit was too speculative to “permit a magistrate reasonably to conclude that it is more likely than not that additional evidence of criminal drug activity would be found on defendant’s property”); accord [*State v. Wilson*](#), 178 Or App 163, 172, 35 P3d 1111 (2001) (“[A]lthough the facts suggest a possibility that criminal evidence might be found at defendant’s residence, that is not the standard to be met here.”).

We turn, finally to the state’s alternative rationale—*viz.*, that seizure of defendant’s other personal electronic devices was justified as essential to preclude potential “remote” deletion of any evidence stored in the surveillance system or the cell phone on which defendant had played the audio recording for McClendon. That contention is raised for the first time on appeal: The state did not advance such a contention in opposing suppression before the trial court—which is unsurprising, given that the only references in the warrant application affidavit to such potential “tampering” or deletion were in the context of seeking authorization to seize and search data stored on

remote servers to forestall destruction of *that* evidence. See 281 Or App at ___ n 4.⁸

We decline to consider the state’s belated contention. That contention is legally and factually problematic in that it implicates matters not addressed (again, unsurprisingly) in the warrant application affidavit. For example, can suspects engage in “remote” destruction of evidence on one or more of their personal electronic devices (or stored on servers) by using a device other than their own? Or, even assuming the state’s premise that *seizure* of all of a suspect’s electronic devices is necessary to forestall such “remote” destruction of evidence on other devices (or servers), how does that justify *forensic examination* of the contents of all of the devices? Even putting aside those aspects, however, the state’s novel proposition has potentially profound systemic implications that have been completely unexplored on this record. Accordingly, we decline to review that contention. See [State v. Kolb](#), 251 Or App 303, 311-12, 283 P3d 423 (2012) (emphasizing that appellate court’s consideration of an alternative basis for affirmance “is a matter of prudential discretion and not compulsion” and declining to address the state’s “belated and still-cursory” alternative basis for affirmance of denial of suppression because, regardless of whether the trial court record might have been affected if that contention had been raised in opposing suppression, “the fact remains that to address that contention meaningfully would require us, in the first instance—without legal record development or any real assistance from the parties—to decide difficult, nuanced, and systemically significant issues”).⁹

The search warrant was invalid, rendering the search of the gun safe unlawful. Accordingly, the trial court erred in denying the motion to suppress.

Reversed and remanded.

⁸ As noted in footnote 4 above, the warrant did not include such authorization. Cf. [State v. Rose](#), 264 Or App 95, 96-106, 330 P3d 680, *rev den*, 356 Or 400 (2014) (rejecting contention that there was no statutory authority to issue an “out-of-state search warrant” to internet service provider).

⁹ See also [Biggerstaff v. Board of County Commissioners](#), 240 Or App 46, 56, 245 P3d 688 (2010) (declining to exercise “prudential discretion” to consider various alternative bases for affirmance that were not raised, “much less developed,” in the proceedings under review and “present[ed] substantial issues of statutory and constitutional law”).