

IN THE COURT OF APPEALS OF THE
STATE OF OREGON

STATE OF OREGON,
Plaintiff-Respondent,

v.

JOSHUAH SHAILEN BURNHAM,
Defendant-Appellant.

Lincoln County Circuit Court
130104; A155709

Mary Mertens James, Judge.

Argued and submitted April 13, 2016.

Jesse Wm. Barton argued the cause and filed the brief for appellant.

David B. Thompson, Assistant Attorney General, argued the cause for respondent. With him on the brief were Ellen F. Rosenblum, Attorney General, and Paul L. Smith, Deputy Solicitor General.

Before Ortega, Presiding Judge, and Lagesen, Judge, and Garrett, Judge.

GARRETT, J.

Reversed and remanded.

GARRETT, J.

Defendant appeals a judgment of conviction for two counts of hunting upon the cultivated or enclosed land of another without permission, ORS 498.120; two counts of second-degree criminal trespass, ORS 164.245; one count of violating a provision of the wildlife laws or rules with a culpable mental state, ORS 496.992(1); and two counts of third-degree theft, ORS 164.043. On appeal, defendant assigns error to the trial court's denial of his motion to suppress evidence that was obtained as a result of the execution of a search warrant. Defendant argues, among other things, that the search warrant was overbroad in violation of Article I, section 9, of the Oregon Constitution. We agree with defendant that the search warrant was impermissibly overbroad for reasons articulated in our recent decisions in *State v. Friddle*, 281 Or App 130, 381 P3d 979 (2016), and *State v. Mansor*, 279 Or App 778, 381 P3d 930 (2016), *rev allowed*, 360 Or 752 (2017). Accordingly, we reverse the judgment on all counts.¹

We review a challenge to the validity of a search warrant for legal error. *State v. Castilleja*, 345 Or 255, 264, 192 P3d 1283, *adh'd to on recons*, 345 Or 473, 198 P3d 937 (2008). We state the uncontroverted facts as recited in the search-warrant affidavit. *Friddle*, 281 Or App at 131.

Oregon State Police received information that, in August 2012, defendant had trespassed on land owned by Plum Creek Timber Company and killed an elk while hunting there without permission. In December 2012, officers in the Fish and Wildlife Division of the Oregon State Police made contact with a person named Martin, who informed them that he and defendant had entered Plum Creek's property through a closed gate on August 26 and hunted there. Martin also said that, on August 27, defendant contacted him to ask for help in tracking an elk that he had shot and could not locate, and, on August 28, Martin and defendant again entered Plum Creek's property to search for the dead elk. Martin told the police that defendant had pointed out

¹ Because we conclude that the trial court erred in denying defendant's motion to suppress evidence and that the error was not harmless, we do not reach defendant's other assignments of error.

where he had been standing when he shot the elk and where the elk was standing when it had been shot. According to Martin, the two followed tracks and a blood trail to locate the elk, and Martin used defendant's cellular phone to take photos of defendant with the elk at the location where the elk had died. Martin also told the police that defendant had posted the photos on his Facebook page.

Martin subsequently accompanied two officers onto Plum Creek's property, pointing out the locations where defendant said he had been standing when he shot the elk, where the elk had been standing, and where the elk had died. One of the officers recorded GPS coordinates for each of the locations, and he determined that, if Martin's description was accurate, defendant had shot the elk while both he and the elk were located on Plum Creek's property. The officer also determined that the elk had died on a different landowner's property.

Based on that information, Kehr, a fish and wildlife officer, obtained a search warrant for defendant's residence. The warrant authorized officers to seize and search the contents of "any and all" of defendant's "computer equipment" and "electronic data devices," including "any data processing hardware and storage devices, cell phones, computers, laptops, notebooks, computer systems," and "any other computer storage media that contains information of illegally obtained or possessed wildlife or parts thereof."

In a supporting affidavit, Kehr averred that, based on his "training and experience as a fish and wildlife officer," it is "customary and traditional" for a hunter to retain photographs of harvested wildlife and to store those photos in "various formats," including in "computer media devices" and "laptops." Kehr further averred that, based on his training and experience, when a cellular phone is used to take photos, "often times the phone will store the date, time, and a geographical location when the function was performed," and that information "can be stored on, but not limited to, internal memories, and Internet databases."

In executing the search warrant, officers seized a number of incriminating items. Officers also seized a laptop owned by defendant, performed forensic analysis on its

digital contents, and obtained incriminating GPS data from photos discovered on the laptop.

Defendant moved to suppress all evidence derived from the execution of the search warrant, arguing, among other things, that the warrant was overbroad and that the affidavit was insufficient to establish probable cause for the seizure and analysis of defendant's laptop. The trial court denied defendant's motion. On appeal, defendant argues that the trial court erred in denying his motion to suppress, reprising his argument that the warrant was impermissibly overbroad.

Article I, section 9, provides, in relevant part: “[N]o 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.” When a warrant authorizes the seizure and examination of the contents of multiple personal electronic devices—which are, for purposes of the particularity requirement of Article I, section 9, more akin to “‘place[s]’ to be searched” than “‘thing[s]’ to be seized and examined”—the affidavit must substantiate probable cause for the forensic examination of the contents of *each* of the electronic devices included in the warrant. *Friddle*, 281 Or App at 138 (quoting *Mansor*, 279 Or App at 801). If it does not, such a warrant authorizes invasions of privacy that are not supported by probable cause and, as such, is overbroad in violation of Article I, section 9. *Id.* at 137-38.

Our recent decision in *Friddle* is closely analogous to this case. In *Friddle*, the defendant was suspected of assaulting his then-girlfriend. *Id.* at 131. Police knew that the defendant had a security system that may have recorded the assault, and a police officer had personally observed the defendant accessing an audio recording of the assault on his cellular phone. *Id.* at 132. Based on that information, the police applied for a warrant to seize and analyze the contents of a broad array of the defendant's personal electronic devices. *Id.* at 133-34. The affiant alleged that, based on his “training and experience,” individuals involved in “criminal activity regularly use” cellular phones to “record and store photos, audio recordings, and video recordings of their

crimes.” *Id.* at 133. The affiant stated that it was his belief that a search of the defendant’s cell phones and computer “will show recordings” of the alleged assault. *Id.*

On appeal, we concluded that, for two reasons, the affidavit was insufficient to support probable cause to forensically examine all of the electronic devices included in the warrant. First, we concluded that the affiant’s description of his training and experience was “generic,” and nothing in the affidavit indicated that the affiant had professional training or experience specifically related to personal electronic devices and their contents as evidence in criminal investigations. *Id.* at 139. Second, even assuming that the affidavit demonstrated the requisite training and experience, and, assuming that the facts alleged could support the possibility of “multiple access or retention” of the incriminating data, the affidavit failed to substantiate a probability that evidence of the alleged assault would be found on all of the defendant’s personal electronic devices. *Id.* at 141.

Applying that reasoning here, we conclude that the warrant was facially overbroad. As in *Friddle*, the fish and wildlife officers in this case had reliable information that, on one occasion, defendant’s cellular phone was used to create and store potentially incriminating digital photographs. And, as in *Friddle*, the crime under investigation (illegal hunting) was not one that depended upon or was committed through the use of electronic devices. Thus, in both cases, the only concrete factual link between the crimes under investigation and the multiple electronic devices covered by the warrant was the likely presence of incriminating digital data on specifically identified devices—here, a single cellular phone. As in *Friddle*, the search-warrant affidavit in this case relies on the evidence potentially contained in the phone to justify the search of other electronic devices based on the invocation of the affiant’s “training and experience.”

Yet, as in *Friddle*, the affiant in this case alleged no specialized training or experience actually bearing on the transmission of data between electronic devices, nor is there any experience inherent in that of a fish and wildlife officer from which a magistrate could infer such knowledge. See *id.* at 140 (“The phrase ‘training and experience’ ***

is not a magical incantation with the power to imbue speculation, stereotype, or pseudoscience with an impenetrable armor of veracity.” (Internal quotation marks omitted.)). From the affidavit, a magistrate could infer that, because defendant’s cellular phone was used to take incriminating photographs—and defendant posted those photos on his Facebook page—there was a *possibility* that the photos had been transmitted to at least some of his other electronic devices. Yet, the contents of the affidavit failed to establish that it was *more likely than not* that such transmission had occurred with respect to all of his devices. *See id.* at 138 (“[T]he 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.*” (Quoting [State v. Williams](#), 270 Or App 721, 725, 349 P3d 616 (2015) (emphasis in *Friddle*))). Thus, as in *Friddle*, because the affidavit contains no specific information to support an inference that data existing on one device would have been transmitted to other devices belonging to defendant, the affidavit was insufficient to support probable cause to examine those other devices. Accordingly, the warrant was impermissibly overbroad in violation of Article I, section 9, and the trial court erred in denying defendant’s motion to suppress.²

The state does not argue that any error was harmless. Nor can we conclude, in light of the centrality of the evidence obtained pursuant to the warrant to the state’s prosecution of defendant, that there was little likelihood that the error affected the verdict as to any of the counts of conviction. *See State v. Davis*, 336 Or 19, 32-33, 77 P3d 1111 (2003).

Reversed and remanded.

² In light of our disposition, we do not address the remainder of defendant’s arguments bearing on the validity of the search warrant and its execution, including whether the warrant was invalid under the Fourth Amendment to the United States Constitution. *See State v. Barnthouse*, 360 Or 403, 413, 380 P3d 952 (2016) (“In keeping with our customary practice, we *** turn to the Fourth Amendment only if we conclude that no state constitutional violation occurred.”).