IN THE COURT OF APPEALS OF THE
STATE OF OREGON

STATE OF OREGON,
Plaintiff-Respondent,
v.
RANDALL DE WITT SIMONS,
Defendant-Appellant.

Lane County Circuit Court
19CR43543; A177032

Karrie K. McIntyre, Judge.

Argued and submitted September 26, 2023.

Kyle Krohn, Deputy Public Defender, argued the cause for appellant. Also on the briefs was Ernest G. Lannet, Chief Defender, Criminal Appellate Section, Office of Public Defense Services.

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

Before Aoyagi, Presiding Judge, and Joyce, Judge, and Jacquot, Judge.

AOYAGI, P. J.

Reversed and remanded.

AOYAGI, P. J.

Defendant was convicted of 15 counts of first-degree encouraging child sexual abuse, ORS 163.684, for downloading child pornography. He was caught as a result of his activities in accessing and downloading child pornography while using a free wireless internet (Wi-Fi) network that a fast-food restaurant near his home provided for its customers, subject to a user agreement.

Defendant raises two assignments of error. First, he argues that police monitoring of his internet browsing activity on the restaurant's Wi-Fi network constituted an unlawful warrantless search under Article I, section 9, of the Oregon Constitution, and the Fourth Amendment to the United States Constitution, such that the evidence obtained from the restaurant (and all derivative evidence) should have been suppressed. On that issue, we agree with the trial court that defendant did not have a constitutionally protected privacy interest under the circumstances, so no "search" occurred. Second, with respect to a later warranted search of his home, defendant argues that the trial court applied the wrong legal standard to decide whether the evidence from the home should be suppressed, after it concluded that some information in the warrant application was unlawfully obtained. We accept the state's concession on that point, and we agree with the state that the proper remedy is to remand for reconsideration of that ruling under the correct legal standard. Accordingly, we reverse and remand.

I. FACTS

"We review a trial court's denial of a motion to suppress for errors of law and are bound by the court's factual findings if there is constitutionally sufficient evidence to support them." *State v. DeJong*, 368 Or 640, 643, 497 P3d 710 (2021). We state the facts in accordance with the standard of review.

In 2018, the A&W restaurant in Oakridge provided free Wi-Fi for its customers. A&W did not require a password, but it did require users to agree to A&W's "Acceptable Use Policy" (user agreement), which entailed scrolling through the user agreement and checking a box to "agree"

to the terms. Among other things, the user agreement notified potential users that A&W did not ensure "the security of any data you send through the Wi-Fi System and it is your responsibility to secure such data." It stated that A&W "does not actively monitor the use of the Wi-Fi System under normal circumstances," but that A&W "may remove, block, filter or restrict by any other means any materials that *** may be illegal, may subject [A&W] to liability or may violate the [user agreement.]" Also, A&W "may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong." Examples of activities that would violate the user agreement were provided, including transmitting "unlawful," "obscene," or "otherwise objectionable" material (by uploading, posting, email or otherwise) or "intentionally or unintentionally" violating any local, state, national, or international law or regulation. Additionally, A&W "may disclose your communications and activities using the Wi-Fi System in response to lawful requests by governmental authorities, including Patriot Act requests and judicial orders."

The user agreement had to be accepted each time that a user logged onto A&W's guest Wi-Fi network. A user who stayed on the network for a long time would have to re-accept the terms every two to four hours. The Wi-Fi signal extended beyond A&W's property, so it was possible for noncustomers to access the guest Wi-Fi network, if they were close enough to the restaurant to be within signal range.

Porteous, the owner of A&W, employed Sanders, a private consultant, to install and maintain the guest Wi-Fi network, which included installing a firewall. The firewall automatically captured and logged unencrypted web traffic on the network. As a result, A&W knew the device names and Media Access Control (MAC) addresses of devices that used the network, the times that devices were logged onto the network, and the unencrypted websites and webpages that those devices visited. The firewall listed the visited websites by category, and one category was "Child Abuse Images." A&W's free firewall software did not allow for blocking websites; A&W would have had to buy the paid version to get that feature.

On July 2, 2018, while performing routine maintenance, Sanders displayed the firewall logs to Porteous, who asked about the "Child Abuse Images" category. That conversation led to their calling 9-1-1 to report that someone using a device called "IanAnderson-PC" had used the A&W network to access child pornography. Officer Larsen responded and began an investigation.

From July 2018 to June 2019, Sanders worked with Larsen to identify when "IanAnderson-PC" visited child pornography websites while on A&W's guest Wi-Fi network, which happened frequently during that time period. Sanders sent Larsen the firewall logs, as well as spreadsheets that Sanders created. Sanders added Larsen to an existing firewall feature, so that Larsen would receive an email alert whenever a user accessed a child-abuse website. Sanders also sent Larsen "packet capture" or "PCAP" data for IanAnderson-PC, which is a type of data that can be used to reconstruct someone's internet activity on a particular network, although only unencrypted activity can be viewed. Using the information provided by Sanders, the police were able to see all of IanAnderson-PC's unencrypted internet activity while logged onto A&W's network, including both illegal activities—accessing child pornography websites and downloading images—and benign activities such as book shopping on Amazon.

The police eventually determined that a man named Thomas (who used "Ian Anderson" as an alias) was the original purchaser of the "IanAnderson-PC" device, and that Thomas had given the laptop to defendant about two years earlier. The police also determined that defendant lived across the street from the A&W restaurant and that his home was within range of A&W's network.

At that point, the lead investigator, Detective Weaver, believed that he "absolutely had probable cause" to obtain a search warrant for defendant's home. However, he wanted to be able to say with "100 percent" certainty that the IanAnderson-PC signal was coming from defendant's home, so he walked around the triplex in which defendant lived while using Kismet software and a directional antenna (a combination known as a "packet sniffer"), which

successfully located where the signal was strongest when "IanAnderson-PC" logged onto A&W's guest Wi-Fi network. Weaver took that extra step before applying for a warrant because he "wanted to prove the case beyond a reasonable doubt." He testified that he would have applied for a warrant even without the Kismet information though.

Using all of the foregoing information, Weaver obtained a warrant to search defendant's home. The police seized a laptop from the home that was later confirmed to be "IanAnderson-PC." A search of that laptop found child pornography.

Defendant was indicted on 15 counts of first-degree encouraging child sexual abuse. Before trial, he moved to suppress evidence obtained in violation of Article I, section 9, and the Fourth Amendment. As relevant here, defendant argued that, with respect to the evidence gathered from A&W's guest Wi-Fi network (first motion), Sanders had acted as a state agent and effectuated an unlawful warrantless search of his internet activity. As for the warranted search of his home (second motion), defendant challenged the warrant on the basis that the warrant application included the Kismet information, which was acquired in an unlawful search. The state opposed both motions.[1] On the second motion, the state argued that, even if the Kismet information was improperly obtained and should not have been included in the warrant application, the record showed that the police would have applied for and successfully obtained a warrant without that information, so the "inevitable discovery" doctrine applied.

The court held a hearing on defendant's motions to suppress, during which Sanders, Weaver, and Larsen testified, and the A&W user agreement was admitted into evidence. The court then issued a written opinion denying the motions (which it later supplemented at defendant's request). With respect to the evidence from A&W's guest Wi-Fi

[1] Technically, defendant filed a single motion to suppress that he later amended, then supplemented, and there was briefing at each stage. As defendant acknowledges, his motion to suppress "encompassed multiple distinct legal issues." For ease of reference and clarity, we discuss defendant's motion as two motions, tracking defendant's two assignments of error on appeal.

network, the court agreed with defendant that Sanders acted as a state agent, but it concluded that no "search" had occurred for constitutional purposes, because defendant did not have a constitutionally protected privacy interest in the information that Sanders turned over to the police. As for the warranted search of defendant's home, the court agreed with defendant that Weaver conducted an unlawful warrantless search when he used the Kismet software to identify the signal's strength and location while outside defendant's home. However, it denied the motion to suppress evidence from defendant's home, because it concluded that, upon excising the Kismet information, the warrant application was still sufficient to establish probable cause. The court did not reach the state's inevitable discovery argument.

Defendant waived jury, and the charges were tried to the court on stipulated facts. The court found defendant guilty on all counts. This appeal followed.

II. DEFENDANT'S INTERNET BROWSING HISTORY ON A&W'S GUEST WI-FI NETWORK

Defendant's first assignment of error pertains to his motion to suppress evidence that the police obtained, via Sanders, from A&W's guest Wi-Fi network. As previously described, the trial court agreed with defendant that Sanders acted as a state agent,[2] but it decided that no "search" had occurred for constitutional purposes, because defendant did not have a constitutionally protected privacy interest in the information that Sanders turned over to the police. Defendant assigns error to the denial of his motion, arguing that he had a constitutionally protected privacy interest in his internet browsing history. We conclude that the court did not err.

A. *Article I, Section 9*

Article I, section 9, prohibits unreasonable searches by the government. Or Const, Art I, § 9 ("No law shall violate the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search,

[2] To the extent that the state challenges the trial court's determination that Sanders acted as a state agent, we need not reach that issue in light of our disposition. That includes not needing to address whether the issue is procedurally properly before us.

or seizure."). In deciding whether an unreasonable search occurred, the threshold question is whether the government conducted a "search" at all. *State v. Meredith*, 337 Or 299, 303, 96 P3d 342 (2004). "If the government conduct did not amount to a 'search' within the meaning of Article I, section 9, then the protections of that constitutional provision do not apply, and [the court's] inquiry ends." *Id.*

Whereas federal courts frame the "search" issue in terms of reasonable expectations of privacy, Oregon frames it differently: "[T]he privacy protected by Article I, section 9, is not the privacy that one reasonably *expects* but the privacy to which one has a *right*." *State v. Campbell*, 306 Or 157, 164, 759 P2d 1040 (1988) (emphases in original). The Oregon Supreme Court has rejected the "reasonable expectation of privacy" formulation for purposes of Article I, section 9, because that phrase "becomes a formula for expressing a conclusion rather than a starting point for analysis, masking the various substantive considerations that are the real bases on which Fourth Amendment searches are defined." *Id.*

A "search" occurs for purposes of Article I, section 9, when the government invades a "protected privacy interest." *Meredith*, 337 Or at 303. As described in *Campbell*, in the specific context of technological advances:

> "A privacy interest, as that phrase is used in this court's Article I, section 9, opinions, is an interest in freedom from particular forms of scrutiny. The interest is not one of freedom from scrutiny in general, because, if that were the case, any form of scrutiny would infringe a privacy interest and thereby be considered a search. ***
>
> "Government scrutiny aside, individual freedom from scrutiny is determined by social and legal norms of behavior, such as trespass laws and conventions against eavesdropping. [Examples provided.] ***
>
> "Our intention is not to set forth a definition of search based upon social and legal norms of behavior but to clarify the nature of the interest protected by Article I, section 9. Social and legal norms cannot govern the scope of the constitutional provision, which itself plays a substantial role in shaping those norms. But since 1859, when Article I, section 9, was adopted, the government's ability to scrutinize the

> affairs of 'the people' has been enhanced by technological and organizational developments that could not have been foreseen then. *** In deciding whether government practices that make use of these developments are searches, we must decide whether the practice, if engaged in wholly at the discretion of the government, will significantly impair 'the people's' freedom from scrutiny, for the protection of that freedom is the principle that underlies the prohibition on 'unreasonable searches' set forth in Article I, section 9."

306 Or at 170-71 (internal citations omitted; footnote omitted); *see also State v. Wacker*, 317 Or 419, 425, 856 P2d 1029 (1993) (requiring the court to make an objective inquiry into whether "the government's conduct would significantly impair an individual's interest in freedom from scrutiny, *i.e.*, his privacy" (internal quotation marks omitted)).

Ultimately, the question is whether the defendant "had a protected privacy interest in light of the particular context in which the government conduct occurred." *Meredith*, 337 Or at 306. "Whether a constitutionally protected privacy interest exists is a question of law." *State v. Hawthorne*, 316 Or App 487, 495, 504 P3d 1185 (2021), *rev den*, 369 Or 856 (2022).

Here, defendant contends that "[a] person has a protected privacy interest in their internet use, which includes nonpublic, noncriminal information that can reveal many sensitive facts about their private life." Relying on *Campbell* and *Hawthorne*, he argues that the police violated his right to privacy by surreptitiously monitoring his internet use over the A&W guest Wi-Fi network for a year, which revealed both his illegal activities (child pornography) and lawful activities (such as book shopping).

The state counters that a person who uses a Wi-Fi network owned by a private business does not have a constitutionally protected privacy interest in information about their activities on the network. Further, the state argues, defendant received access to A&W's network only after accepting the user agreement, which prohibited use of the network to transmit obscene material or engage in illegal activity, and which notified users that, although A&W did not "actively" monitor use of the network "under normal

circumstances," it could remove, block, filter, or restrict materials that were illegal or that violated the user agreement and that A&W "may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong."[3]

We begin our analysis with *Campbell*, *Meredith*, and *Hawthorne*, which are the cases on which the parties principally rely.

In *Campbell*, decided in 1988, the police suspected the defendant in a series of burglaries. 306 Or at 159. After unsuccessfully trying to follow him by traditional means, they surreptitiously attached a radio transmitter to his car while it was parked in a public lot. *Id.* at 159-60. That allowed them to determine the car's approximate location by tracking the transmitter from an airplane. *Id.* at 160-61. One day, the police located the car in that manner (40 miles away), went to the location, and observed the defendant commit a burglary. *Id.* On review, the Supreme Court held that using the transmitter to locate the car was a "search" under Article I, section 9. *Id.* at 172. It explained that the use of a "device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom from scrutiny" and that the limitation was "made more substantial by the fact that the radio transmitter is much more difficult to detect than would-be observers who must rely upon the sense of sight." *Id.* at 172. The court concluded,

> "Conversations in public may be overheard, but it is relatively easy to avoid eavesdroppers by lowering the voice or moving away. Moreover, one can be reasonably sure of whether one will be overheard. But if the state's position in this case is correct, no movement, no location and no

[3] We do not understand the state to rely on the "third-party doctrine," although some of its arguments touch on that doctrine's principles. *See Hawthorne*, 316 Or App at 498-99 ("Under Article I, section 9, Oregon courts have held that, in some instances, a person does not have a protected privacy interest in information that the person voluntarily allows a third party to access and maintain for its own legitimate business purposes."); *see also Carpenter v. United States*, 585 US ___, ___, 138 S Ct 2206, 2219-220, 201 L Ed 2d 507 (2018) (describing the third-party doctrine, for purposes of the Fourth Amendment, as essentially recognizing that a person who voluntarily exposes information to a third party assumes the risk that the third party will share it). In any event, we need not apply the third-party doctrine to resolve this case, so we do not address it.

> conversation in a 'public place' would in any measure be secure from the prying of the government. There would in addition be no ready means for individuals to ascertain when they were being scrutinized and when they were not. That is nothing short of a staggering limitation upon personal freedom. We could not be faithful to the principles underlying Article I, section 9, and conclude that such forms of surveillance were not searches."

Id.

Sixteen years later, in 2004, the Supreme Court decided *Meredith*, which involved "the same technology and the same type of monitoring by a government agent," but reached a different result. 337 Or at 302-03. In that case, the defendant was employed as a fire prevention technician with the United States Forest Service (USFS). *Id.* at 301. A USFS district ranger authorized law enforcement agents to attach a radio transmitter to one of its trucks while it was parked on USFS property. *Id.* at 301-02. The agents then tracked the truck from an airplane while the defendant drove it for work, and eventually observed the defendant committing arson. *Id.* at 302. The court held that no "search" took place for purposes of Article I, section 9, because the agents did not violate any protected privacy interest of the defendant. *Id.* at 307.

In reaching that conclusion, the court explained that *Campbell* did not stand for the proposition that a person has "the right to be free from the government's surreptitious use of a transmitter to monitor a person's location and movements under *any* circumstances." *Id.* at 304 (emphasis in original). The court also rejected reading *Campbell* to mean that the court "looks to only the government conduct asserted to be a search and evaluates how that conduct, if engaged in wholly at the discretion of the government, would impact the general privacy interests of 'the people.'" *Id.* at 305. Rather, the court had always taken a circumstance-specific approach, assessing "whether the defendant had had a protected privacy interest in light of the particular context in which the government conduct occurred." *Id.* at 305-06 (discussing prior case law).

Thus, properly framed, the interest at issue in *Meredith* "boil[ed] down to defendant's claim to an interest in

keeping her location and work-related activities free from this type of electronic surveillance by her employer while she used employer-owned property on work time." *Id.* at 306. The court concluded that the "defendant did not have a protected privacy interest in keeping her location and work-related activities concealed from the type of observation by her employer that the transmitter revealed." *Id.* at 307. Given the specific facts of the case, "neither the attachment of the transmitter to the truck nor the subsequent monitoring of that transmitter's location invaded a privacy interest of defendant, and, it follows, no search implicating Article I, section 9, occurred." *Id.*

Nearly two decades later, in 2022, we decided *Hawthorne*. In that case, the police were investigating a murder that had just occurred, and they wanted to find the defendant, who was their prime suspect. 316 Or App at 489. "Before they obtained a search warrant, detectives asked that defendant's cell phone service provider 'ping' defendant's phone's location to help locate the fleeing suspect." *Id.* The service provider did so and gave the police the resulting cell-site location information (CSLI), which showed the phone's general location as close to a certain motel. *Id.* at 492. Looking to *Campbell* and *Meredith*, as well as the description of the nature of cell phone tracking in *Carpenter v. United States*, 585 US ___, 138 S Ct 2206, 201 L Ed 2d 507 (2018), we concluded that a "search" had occurred under Article I, section 9. *Id.* at 496-98.

We explained that cell phones "continuously" tap into cell sites to search for a signal and that "[a]s technology improves and cell sites increase, cell phones generate 'increasingly vast amounts of increasingly precise CSLI.'" *Id.* at 496 (quoting *Carpenter*, 585 US at ___, 138 S Ct at 2212). Thus, a cell phone "'tracks nearly exactly the movements of its owner.'" *Id.* at 497 (quoting *Carpenter*, 585 US at ___, 138 S Ct at 2218). At the same time, cell phones have become "necessary for participation in modern life" and are "'almost a feature of human anatomy'" at this point. *Id.* (quoting *Carpenter*, 585 US at ___, 138 S Ct at 2218). Given that combination of facts, "[t]he intrusion caused by pinging a cell phone is even greater than that posed by a tracking device attached to a car." *Id.* Tracking the location

of a person's cell phone "'achieves near perfect surveillance'" of that person and "has the potential to reveal where a person spends time," which in turn "could reflect a person's religious, political, social, or professional associations." *Id.* (quoting *Carpenter*, 585 US at ___, 138 S Ct at 2218).

That led us to conclude that pinging the defendant's cell phone qualified as a "search" for purposes of Article I, section 9. We summarized our reasoning:

> "As ubiquitous as cell phones are, they could become tracking devices that the authorities could tap into at will. That potential would 'significantly impair the people's freedom from scrutiny.' *Campbell*, 306 Or at 171 (internal quotation marks omitted). Without a warrant to assure judicial oversight, such clandestine, technological intervention would be susceptible to abuse. Mindful of *Campbell*, we conclude that pinging defendant's phone to reveal its real-time location was a sufficiently intrusive action to be a search under Article I, section 9."

Id. at 497. We then distinguished *Meredith*, explaining that the defendant's service agreement with his cell phone service provider was "not equivalent to the employment relationship in *Meredith*" and was "not an agreement to have the government use his or her phone as a real-time tracking device." *Id.* at 498.[4]

Returning to the facts of the present case, defendant contends that the state's monitoring of his internet browsing history is "a more severe intrusion" into privacy than the searches in *Campbell* and *Hawthorne*. In his view, unrestrained government monitoring of public Wi-Fi networks raises the same concerns as unrestrained access to cell phone location data (as discussed in *Hawthorne*), because public Wi-Fi networks are "ubiquitous" and have the potential to surreptitiously track people "anytime they access[] the internet via an open Wi-Fi network."

Whatever concerns may exist about public Wi-Fi networks becoming state tracking devices as a result of people

[4] We ultimately affirmed the denial of the motion to suppress in *Hawthorne*, on the basis that the state had established exigent circumstances. 316 Or App at 489. However, only the "search" holding from *Hawthorne* is pertinent to the present discussion.

involuntarily and unknowingly connecting to them, that is not the issue before us. Like the defendant in *Meredith*, defendant misframes the privacy right at issue by stating it too broadly. What is at issue is not a person's right to privacy in internet browsing history in general terms. Rather, what we must assess is whether defendant "had a protected privacy interest *in light of the particular context in which the government conduct occurred*." *Meredith*, 337 Or at 306 (emphasis added).

Here, we conclude that he did not. Specifically, defendant did not have a constitutionally protected right to keep private his internet browsing activities—including illegal activities—that occurred over A&Ws guest Wi-Fi network, to which he had been granted access only after entering into a user agreement that prohibited using the network to transmit obscene material or engage in illegal activity, and which notified defendant that A&W had the ability to monitor users' activities on the network (even if it did not "actively" do so "under normal circumstances"), as well as that A&W "may cooperate with legal authorities *** in the investigation of any suspected or alleged crime[.]"

We disagree with defendant that the user agreement was unclear or confusing as to whether A&W might cooperate in a criminal investigation without a warrant. To the contrary, it was quite clear that A&W might do exactly what it did in this case: notice that someone was using the guest Wi-Fi network to transmit obscene material and engage in criminal activity in violation of the user agreement, alert the police, monitor the network more closely due to the abnormal circumstances, and cooperate with the police in investigating the suspected crimes. That is precisely the type of scenario that the user agreement contemplates.

Defendant accepted the terms of the user agreement every time that he used A&W's guest Wi-Fi network, including re-accepting them every two to four hours when he stayed on the network for longer periods of time.[5] Nonetheless,

[5] It appears that defendant regularly used A&W's guest Wi-Fi network to access the internet. The record shows that, between July 2018 and June 2019,

defendant repeatedly violated the user agreement by accessing and downloading child pornography, which brought him to A&W's attention. None of defendant's internet browsing data was encrypted, so it was readily available to A&W as the network provider, and A&W accessed that data in a manner consistent with its user agreement.

Although defendant's relationship with A&W may not be comparable to the employment relationship in *Meredith*, his situation also is not comparable to those of the defendants in *Campbell* and *Hawthorne*. Defendant repeatedly logged onto A&W's guest Wi-Fi network and accepted A&W's user agreement, then violated that user agreement by transmitting obscene material and engaging in illegal activity, while on notice that A&W had the ability to monitor his activity and might cooperate with the police in investigating criminal activity on its network. Moreover, we disagree with defendant that A&W's user agreement is analogous to the cell phone service agreement in *Hawthorne*. Unlike having a cell phone, having access to private businesses' guest Wi-Fi networks, while convenient, is not "'necessary for participation in modern life.'" *Hawthorne*, 316 Or App at 497 (citing *Carpenter*, 585 US at ___, 138 S Ct at 2218). Also, our discussion of the cell phone service agreement in *Hawthorne* was primarily tied to the state's arguments regarding the third-party doctrine, and there is no indication that any arguments were made regarding the actual terms of the agreement. *See id.* at 496-99. We expressed no opinion in *Hawthorne*—and we continue to express no opinion—on the effect of specific terms of a cell phone service agreement. Nor do we understand *Hawthorne* to hold that no agreement is ever relevant to whether a person has a protected privacy interest in particular circumstances.

We agree with the trial court that defendant did not have a right to privacy in his internet browsing history on A&W's guest Wi-Fi network under these circumstances and that, consequently, no "search" occurred under Article I, section 9.

---

defendant visited 255,723 webpages while logged onto A&W's network. According to numbers provided by defendant, approximately 63 percent of defendant's internet usage while on A&W's network involved "legal" activities.

B. *Fourth Amendment*

We next consider the same argument under the Fourth Amendment, as defendant relied on both the state and federal constitutions in his suppression motion.

The Fourth Amendment prohibits "unreasonable searches and seizures."

US Const, Amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."). The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter*, 585 US at ___, 138 S Ct at 2213 (internal quotation marks omitted). A "search" occurs for Fourth Amendment purposes when the government invades a person's "reasonable expectation of privacy." *Wacker*, 317 Or at 427 (internal quotation marks omitted). A "reasonable expectation of privacy" is "one that society is prepared to recognize as reasonable." *Carpenter*, 585 US at ___, 138 S Ct at 2213 (internal quotation marks omitted). Thus, there are "two questions: first, whether the individual has shown that he or she seeks to preserve something as private; second, whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable." *Wacker*, 317 Or at 427 (internal quotation marks omitted).

Defendant contends that he had a reasonable expectation of privacy in his internet browsing history. He recognizes that, while "reasonable expectation of privacy" is a different formulation than the standard under Article I, section 9, many of the underlying concerns are similar, and his arguments under the Fourth Amendment are similar to his arguments under Article I, section 9, except that he relies entirely on *Carpenter* for his Fourth Amendment argument.

In *Carpenter*, while investigating a string of armed robberies, law enforcement officers obtained historical CSLI data from the defendant's cell phone service provider and used it to reconstruct his physical movements for four months. 585 US at ___, 138 S Ct at 2212-213. Cell phones generate CSLI data "without any affirmative act on the part

of the user beyond powering up," and CSLI data can be used to create "a detailed chronicle of a person's physical presence compiled every day, every moment." *Id.* at ___, 138 S Ct at 2220. The Court held that the government conduct constituted a "search" because it invaded the defendant's reasonable expectation of privacy in his physical movements. *Id.* at ___, 138 S Ct at 2219. The Court's reasoning was similar to ours in *Hawthorne*, in which we cited heavily to *Carpenter*. *Compare id.* at 2217-220, *with Hawthorne*, 316 Or App at 496-98 (deciding the case under Article I, section 9, but citing heavily to *Carpenter*). The Court expressly limited its holding to the particular circumstances, stating that its decision was "narrow" and that it was not expressing views on matters not before it. *Carpenter*, 585 US at ___, 138 S Ct at 2220.

The present case is materially distinguishable from *Carpenter* on its facts. *Carpenter* involved surreptitious tracking of a person's physical movements at all times without their knowledge. By contrast, this case involves monitoring of a person's internet browsing activity on a particular network owned by a private business, only while the person was on that network, and to which the person had access only because he agreed to the terms of a user agreement that prohibited illegal activity and warned users that the network owner could monitor their activity and might cooperate in police investigations of illegal conduct on the network. Defendant has not cited any federal case law other than *Carpenter* to support his Fourth Amendment argument.

We are unpersuaded that defendant had a reasonable expectation of privacy in his internet browsing activities on A&W's guest Wi-Fi network and therefore agree with the trial court that no "search" occurred for purposes of the Fourth Amendment. It follows that the trial court did not err in denying defendant's first motion to suppress.

III. EVIDENCE FOUND IN DEFENDANT'S HOME

In his second assignment of error, defendant contends that the trial court erred in denying his motion to suppress evidence obtained from the warranted search of

his home. He argues that the court applied the wrong legal standard to determine whether that evidence should be suppressed, after it ruled that the Kismet information included in the warrant application was unlawfully obtained.

It is undisputed that the trial court applied the standard described in *State v. Binner*, 128 Or App 639, 646, 877 P2d 642, *rev den*, 320 Or 325 (1994): "When an application includes constitutionally tainted information, the correct action is for the magistrate and reviewing court to excise from the application all such information and to determine whether the remaining information is sufficient to establish probable cause." Defendant maintains that *Binner* is no longer good law in light of *DeJong*, a case decided two months after defendant's trial.[6] *See DeJong*, 368 Or at 654 (explaining that, to determine whether a prior illegality requires suppression of evidence from a warranted search, the correct approach is not to excise the illegally obtained information from the warrant application and decide whether probable cause still exists; rather, the focus of the inquiry is on "the effect that the prior illegality may have had on the authorized search"). The state agrees that *Binner*'s approach is "incomplete" in light of *DeJong*.

DeJong implicitly overruled *Binner*. *See State v. Yaeger*, 321 Or App 543, 548, 517 P3d 1029 (2022), *rev den*, 371 Or 477 (2023) (concluding that *DeJong* implicitly overruled *State v. Gardner*, 263 Or App 309, 327 P3d 1169, *rev den*, 356 Or 400 (2014)); *Gardner*, 263 Or App at 313 (stating that when a warrant "application includes constitutionally tainted information, the proper remedy is for the reviewing court to excise all the tainted information from the application and determine whether the remaining information in the affidavit is sufficient to establish probable cause," citing *State v. Hitesman/Page*, 113 Or App 356, 359, 833 P2d 306, *rev den*, 314 Or 574 (1992)); *Binner*, 128 Or App at 646 (also relying on *Hitesman/Page* as authority for the same procedure described in *Gardner*).

We therefore agree with the parties that the trial court erred in applying *Binner* to determine whether the

[6] On appeal, we apply the current law, not the law in effect at the time that the trial court ruled. *State v. Cannon*, 328 Or App 29, 41-43, 537 P3d 182 (2023).

evidence from the warranted search of defendant's home should be suppressed in light of the inclusion of unlawfully obtained Kismet information in the affidavit.[7]

As for the remedy, we agree with the state that the proper course is to remand for the trial court to reconsider defendant's second motion under *DeJong*. Under *DeJong*, 368 Or at 642, "the defendant has the initial burden to establish a minimal factual nexus between the illegality and the challenged evidence," and "[i]f the defendant does so, the burden shifts to the state to establish that the challenged evidence was untainted by the illegality." The state does not dispute that the evidence is sufficient for defendant to meet his initial burden. Defendant contests that the evidence is sufficient for the state to meet its burden; he argues that the record fails "to show that police could and would have secured a warrant without the [Kismet] information." Having reviewed the record, however, we agree with the state that remand is appropriate. *See DeJong*, 368 Or at 657, 659 (where the evidence is legally sufficient to allow a ruling in the state's favor, the case should be remanded to the trial court to make findings and conclusions under the correct legal standard). Accordingly, we reverse and remand for the court to reconsider its ruling on the second motion, applying *DeJong*, including making factual findings relevant to whether the warranted search was tainted by the unlawful Kismet information.

IV. CONCLUSION

In sum, we affirm the trial court's denial of defendant's first motion to suppress, because, under the circumstances, defendant did not have a constitutionally protected privacy interest in his internet browsing history on A&W's guest Wi-Fi network. However, we reverse and remand on defendant's second motion to suppress, because the trial court applied the wrong legal standard after concluding that some information in the warrant application was unlawfully

[7] We treat the second claim of error as preserved. We disagree with defendant that preservation is excused because the law changed after trial, *see State v. Horton*, 327 Or App 256, 258-61, 535 P3d 338 (2023), but we agree with the state that the purposes of preservation were adequately served under the particular circumstances.

obtained. The trial court is to reconsider the second motion under the *DeJong* standard.

Reversed and remanded.