IN THE SUPREME COURT OF THE
STATE OF OREGON

STATE OF OREGON,
Respondent on Review,
v.
RANDALL DE WITT SIMONS,
Petitioner on Review.
(CC 19CR43543) (CA A177032) (SC S070787)

En Banc

On review from the Court of Appeals.*

Argued and submitted September 12, 2024.

Kyle Krohn, Senior Deputy Public Defender, Oregon Public Defense Commission, Salem, argued the cause and filed the briefs for petitioner on review. Also on the briefs was Ernest G. Lannet, Chief Defender, Criminal Appellate Section.

Joanna Hershey, Senior Assistant Attorney General, Salem, argued the cause and filed the brief for respondent on review. Also on the brief were Ellen Rosenblum, Attorney General, and Benjamin Gutman, Solicitor General.

Kelly Simon, ACLU Foundation of Oregon, Portland, filed the brief for *amici curiae* The National Association of Criminal Defense Lawyers, Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Oregon.

Rosalind M. Lee, Eugene, filed the brief for *amicus curiae* Oregon Criminal Defense Lawyers Association. Also on the brief were Amy Potter and Daniel C. Silberman. Aliza B. Kaplan, Portland, filed the brief for *amicus curiae* Criminal Justice Reform Clinic at Lewis & Clark Law School.

---

*Appeal from Lane County Circuit Court, Karrie K. McIntyre, Judge. 329 Or App 506, 540 P3d 1130 (2023).

JAMES, J.

The decision of the Court of Appeals is reversed in part. The judgment of the circuit court is reversed, and the case is remanded to the circuit court for further proceedings.

Bushong, J., concurred in part and dissented in part and filed an opinion.

JAMES, J.

This case requires us to decide whether Article I, section 9, of the Oregon Constitution recognizes a person's right to privacy in their internet browsing activities, even when they are accessing the internet via a public access point that they neither operate nor control.

Defendant accessed the internet via a publicly accessible wireless (Wi-Fi) network operated by a local business, A&W, for the benefit of its visitors. To connect to that network, visitors were required to acknowledge a terms-of-service provision that included statements that, although A&W did not "actively monitor" the network, users could be suspended from the network for improper activity, and that A&W "may cooperate with legal authorities," including "disclosing communications and activities *** in response to lawful requests by governmental authorities, including *** judicial orders." Alerted to suspicious activity by A&W, the police used the business to monitor defendant's internet traffic. Over the course of a year, without a warrant, the state tracked 255,723 of defendant's webpage visits. Defendant was eventually arrested for and later convicted on charges of encouraging child sexual abuse.

On defendant's appeal, the Court of Appeals held that "defendant did not have a constitutionally protected privacy interest under the circumstances, so no 'search' occurred." *State v. De Witt Simons*, 329 Or App 506, 508, 540 P3d 1130 (2023). We allowed defendant's petition for review and now hold that the mere fact that a person accesses the internet through a public network does not eliminate the Article I, section 9, right to privacy that exists for one's internet browsing activities. Nor do terms-of-service provisions such as were present here eliminate that right to privacy. Finally, we hold that the trial court was correct to conclude that the coordinated effort between A&W and law enforcement to monitor defendant for a year constituted state action. Accordingly, the state's year-long surveillance of defendant's internet activities was a search under Article I, section 9. The state did not secure a warrant, and, on this record, the state failed to establish that an exception to the warrant requirement applied. The decision of the

Court of Appeals is reversed in part. The judgment of the circuit court is reversed, and the case is remanded to the circuit court for further proceedings.

I. BACKGROUND

This case stems from the trial court's denial of defendant's combined motion to controvert and suppress evidence at trial. Defendant moved to suppress the alleged search by A&W. Defendant also moved to controvert the later warrant to search his home, the affidavit in support of which was, in part, based on information obtained by the year-long activities of A&W. The Court of Appeals noted that "[f]or ease of reference and clarity, we discuss defendant's motion as two motions, tracking defendant's two assignments of error on appeal." *Simons*, 329 Or App at 511 n 1. We follow suit. "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).

During 2018 and 2019, defendant accessed the internet from a public Wi-Fi network operated by an A&W restaurant in Lane County, Oregon. A&W's Wi-Fi signal reached beyond the restaurant's premises, and people could access the network if they were close enough to the restaurant to be within signal range. Defendant's home was within signal range of the A&W Wi-Fi.

The A&W network did not require a password, but it did require users to click a button to accept its terms of service every two to four hours. A&W's owner, Porteous (hereinafter "the owner"), had copied the terms of service from sources on the internet. Not all of the language in the terms of service had been modified to fit A&W's circumstances—for example, it described the business as a hospital and customers as "patients," and it directed any inquiries to a Harvard University email address and an unidentified phone number. The terms of service included the following provisions:

- The network is free for "patients, visitors, and business partners."

- Users must comply with local, state, federal, and international laws.
- Users must not transmit material that is "unlawful, threatening, abusive, harassing, tortious, defamatory, obscene, libelous, invasive of another's privacy, hateful or racially, ethnically, or otherwise objectionable."
- Users must not transmit material that violates any "contractual or fiduciary relationships" or intellectual property rights; may not transmit spam or malicious computer code; and may not use the network "for high volume data transfers" or resell access to the network.
- A&W "does not undertake the security of any data you send through the Wi-Fi System and it is your responsibility to secure such data."
- A&W "does not screen or restrict access to any content placed on or accessible through the Internet," including "improper," "obscene," or "otherwise offensive" content.
- Users may encounter "improper, inaccurate, misleading, defamatory, obscene or otherwise offensive" content, and A&W "is not liable for any action or inaction" with respect to such content.
- A&W "does not actively monitor the use of the Wi-Fi System under normal circumstances" or "review the content of any Web site, electronic mail transmission, newsgroup or other material created or accessible over or through the Wi-Fi System."
- A&W "may remove, block, filter or restrict by any other means any materials" that A&W determines may be illegal, violate the terms of service, or subject A&W to liability.
- Violations of the terms of service "may result in the suspension or termination of your access to the Wi-Fi System."

- A&W may also "cancel your access to the Wi-Fi System at any time, without notice and for any reason."
- A&W "may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong."
- 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."

A firewall secured the network but did not restrict internet access to specific websites. The firewall did monitor and log any unencrypted websites its users visited, including websites that the firewall tagged as containing images of child pornography or child abuse. A&W's Wi-Fi and internet access was serviced by a private internet technology consultant, Ken Sanders (hereinafter "the consultant"). Neither the owner nor the consultant regularly monitored the website logs prior to becoming aware of the charged conduct in this case.

In July 2018, the owner and the consultant noticed that the log included entries that the firewall had tagged as "child abuse images" from a user whose computer was named "IanAnderson-PC." They contacted law enforcement, and Officer Larsen responded and began an investigation. The consultant asked Larsen whether A&W should block Wi-Fi access by IanAnderson-PC. Larsen instructed the consultant not to block the user but, instead, to track the user to find his location. The consultant informed the officer about the firewall logs, and he volunteered to collect and provide specific logs for IanAnderson-PC for the benefit of law enforcement. Because the consultant had not configured the firewall to monitor the activity of a single user, and the firewall did not create logs for single users, he manually prepared IanAnderson-PC logs for Larsen using a separate application. The consultant also established a firewall account for the officer so that the officer received email notifications each time that IanAnderson-PC accessed a flagged website.

Following Larsen's directives over the course of the following year, A&W gave the officer logs of all the websites visited by IanAnderson-PC on its network. Altogether, the logs contained 255,723 entries, and covered defendant's internet activity from July 1, 2018 through June 29, 2019. Each entry displayed the exact URL (uniform resource locator) that the computer had visited, including file names. A few months into the investigation, A&W, again in coordination with law enforcement, began collecting PCAP (packet capture) data from IanAnderson-PC. PCAP data can be used to reconstruct a person's unencrypted internet usage. For example, A&W could have used PCAP data to identify specific items that IanAnderson-PC had searched for and purchased on Amazon.com. In this case, the PCAP data included 44 images matching children in a database of the National Center for Missing & Exploited Children. A&W provided that information to Larsen.

Ultimately, A&W provided the officer with logs of all the unencrypted traffic that it had collected from IanAnderson-PC, which included, as the consultant later explained, "the content of the communication that the computer was having with the internet." At no point during A&W's monitoring and collection of IanAnderson-PC's activity did A&W receive a subpoena for that information, nor did the state secure a search warrant for the information.

Law enforcement eventually identified defendant, who lived near the A&W restaurant, as the current owner of IanAnderson-PC. Detective Weaver testified that during this time he would "go up to Oakridge at the times when this person was normally logging in to the Wi-Fi and just sat there and waited until the person did log in." Based on the logs produced by A&W, the detective employed a "packet sniffer," a tracking device with a directional antenna, to identify radio traffic associated with the Media Access Control (MAC) address assigned to IanAnderson-PC. The detective determined that IanAnderson-PC was broadcasting a signal and, using the packet sniffer, the detective was able to narrow the location from which the broadcast was occurring to defendant's home. The detective then applied for and was granted a warrant to search defendant's home.

In the ensuing search, detectives seized a laptop that was later confirmed to be the IanAnderson-PC device. A search of that laptop revealed child pornography. Defendant was subsequently charged with 15 counts of encouraging child sexual abuse in the first degree.

Before trial, defendant moved to suppress the evidence obtained from the investigation. In support of that motion, defendant argued, among other things, that A&W had acted as a state agent and that monitoring and documenting his internet activity was an unlawful search under the state and federal constitutions. The state responded that A&W had not been acting as a state agent. Further, the state argued, even if state action were involved, a search had not occurred, because defendant had no protected privacy rights under either Article I, section 9, of the Oregon Constitution or the Fourth Amendment to the United States Constitution.

The trial court ruled for the state. Despite agreeing with defendant that A&W's owner and consultant had acted as state agents when they provided the logs documenting his internet browsing activity to the police, the trial court held that defendant lacked a privacy right in his use of the A&W network. After a stipulated facts trial, the trial court convicted defendant of 15 counts of first-degree encouraging child sexual abuse, ORS 163.684.

On appeal, the Court of Appeals agreed with the state that the warrantless surveillance of defendant's internet activity did not offend either Article I, section 9, or the Fourth Amendment, because defendant did not have a right to privacy or a reasonable expectation of privacy in his internet browsing activities conducted on A&W's guest Wi-Fi network under the circumstances. *De Witt Simons*, 329 Or App at 520, 522. That was so, the court explained, because defendant had been granted access to A&W's guest Wi-Fi network only after acknowledging the terms of service that prohibited the transmission of obscene materials or illegal activity and, further, placed defendant on notice 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[.]'" *Id.* at 519 (omission and brackets in *De Witt Simons*). The court noted that "[n]one 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." *Id.* at 520. Thus, the court concluded that defendant did not have a constitutionally protected right to keep private his internet browsing activities that occurred over the network. That decision obviated the court's need to address the trial court's ruling that A&W's owner and consultant had acted as state agents. *Id.* at 512 n 2.

The Court of Appeals nevertheless reversed the trial court on a separate ground because the state had conceded error. *See id.* at 508 (so noting). That aspect of the Court of Appeals' decision is not presented here.

II. ANALYSIS

On review, defendant argues that both Article I, section 9, and the Fourth Amendment to the United States Constitution grant him a right to privacy in his internet browsing activity that was not extinguished by the fact that he used a public Wi-Fi network. As we will explain, we agree with defendant's argument that the police conduct in this case violated the Oregon Constitution. For that reason, we do not consider whether defendant's Fourth Amendment rights also were violated.

A. *Overview of Article I, Section 9.*

The Oregon Constitution recognizes a right to privacy in, among other provisions, Article I, section 9, which states, in relevant part, that "[n]o law shall violate the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure." Article I, section 9, begins with the words "no law shall." It addresses not only executive action, but legislative action as well as all governmental action regardless of source. *State v. Davis,* 313 Or 246, 253, 834 P2d 1008 (1992) ("The introductory phrase, '[n]o law shall violate,' is not limited to provisions of legislation. It defines the limits of permissible governmental conduct generally."). Accordingly, Article I, section 9, protects Oregonians by focusing on, and prohibiting, "*acts* of

the government." *State v. Campbell*, 306 Or 157, 164, 759 P2d 1040 (1988) (emphasis in original).

In an inquiry under Article I, section 9, the threshold question is whether the conduct at issue constituted a "seizure" or a "search." *See State v. Juarez-Godinez,* 326 Or 1, 5-6, 942 P2d 772 (1997) (outlining methodology for addressing Article I, section 9, questions). Where, as here, seizure has not been challenged, 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 our inquiry ends. *See State v. Smith,* 327 Or 366, 374, 963 P2d 642 (1998) (stating that, because dog sniff conducted in public place was not a search, protections of Article I, section 9, did not apply). For purposes of Article I, section 9, a search occurs if governmental action invades "a protected privacy interest." *State v. Wacker*, 317 Or 419, 426, 856 P2d 1029 (1993). As can be seen, whether there is a protected privacy interest and whether the conduct constituted a "search" are often two sides of the same analytical coin.

What constitutes a search under Article I, section 9, differs from what constitutes a search under the Fourth Amendment to the United States Constitution. Under the Fourth Amendment, a search occurs when police invade a person's reasonable expectation of privacy. *Carpenter v. United States*, 585 US 296, 304, 138 S Ct 2206, 201 L Ed 2d 507 (2018). By contrast, the privacy protected by Article I, section 9, "is not the privacy that one reasonably *expects* but the privacy to which one has a *right*." *Campbell*, 306 Or at 164 (emphases in original; citation omitted).

In *Campbell*, we criticized the federal reasonable "expectation of privacy" test as a "formula for expressing a conclusion rather than a starting point for analysis." *Id.* That criticism drew upon our earlier observation in *State v. Tanner*, 304 Or 312, 321 n 7, 745 P2d 757 (1987):

> "One difficulty with analyzing privacy interests in terms of 'expectations' is that the issue is one of right, not expectation. Rights under section 9 are defined not by the privacy one expects but by the privacy one has a right to expect *from the government*."

(Emphasis in original.)

The framing of Article I, section 9, in terms of rights, not expectations, is not simply a difference of expression; it is a difference in constitutional focus. The Fourth Amendment focuses on the expectation of privacy of the individual against whom the government has acted, and the objective reasonableness of that expectation. *See, e.g., Oliver v. United States*, 466 US 170, 177, 104 S Ct 1735, 80 L Ed 2d 214 (1984) ("Since *Katz v. United States*, [389 US 347, 88 S Ct 507, 19 L Ed 2d 576 (1967),] the touchstone of Fourth Amendment analysis has been whether a person has a constitutionally protected reasonable expectation of privacy." (Internal quotation marks omitted.)). Article I, section 9, on the other hand, does not focus on the expectation of privacy of the individual; rather, it focuses on the expectations that society sets for the conduct of our government.

We have explained that the right to privacy protected by Article I, section 9, "is the freedom from scrutiny as 'determined by social and legal norms of behavior, such as trespass laws and conventions against eavesdropping.'" *State v. Newcomb*, 359 Or 756, 764, 375 P3d 434 (2016) (citing *Campbell*, 306 Or at 170). Critically, those references in *Campbell* and *Newcomb* to trespass laws, for example, are not directed at whether the *individual* asserting a protected privacy interest is either lawfully present or a trespasser in a place; they are directed at the actions of the *government*—that is, whether the *government* has behaved like a trespasser.

By defining protected privacy interests as rights, Article I, section 9 places the primary focus on governmental conduct. This focus on governmental conduct means that expectations implied by contract or agreement are not controlling. As we have said, Article I, section 9, is not "defined by private property or contractual rights, although such rights may inform the analysis in a given case." *State v. Lien/Wilverding*, 364 Or 750, 759-60, 441 P3d 185 (2019). This focus enables us to frame the fundamental question underlying an Article I, section 9, challenge as follows: whether the government's conduct, "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." *Campbell*, 306 Or at 171. Focusing on the governmental conduct, on the expectations that society sets for the conduct of our government, permits and, in fact, *requires* Article I, section 9, to be "read in light of the ever-expanding capacity of individuals and the government to gather information by technological means *** [and to] speak to every possible form of invasion—physical, electronic, technological, and the like." *Smith*, 327 Or at 373.[1]

B. *As a general proposition, Oregonians have a right to privacy while accessing the internet through a third party.*

The Court of Appeals held that the police had not conducted a "search" in this case, reasoning:

> "Whatever concerns may exist about public Wi-Fi networks becoming state tracking devices as a result of people involuntarily and unknowingly connecting to them, that is not the issue before us. ***
>
> "[D]efendant did not have a constitutionally protected right to keep private his internet browsing activities—including illegal activities—that occurred over A&W's 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

[1] This focus on governmental action, as opposed to some aspect of the individual upon whom government action is brought to bear, is not a discrete feature of Oregon search and seizure law. Rather, it is an oft-occurring aspect of our independent state constitutional methodology that we see echoed in other jurisprudential contexts.

As an example, First Amendment analysis is generally built upon the categorization of individual expression based upon its nature. Accordingly, commercial speech gets less federal constitutional protection than political speech. *Compare Boos v. Barry*, 485 US 312, 321, 108 S Ct 1157, 99 L Ed 2d 333 (1988) (political speech), *with Central Hudson Gas & Elec. Corp. v. Public Service Comm'n of New York*, 447 US 557, 562-63, 100 S Ct 2343, 65 L Ed 2d 341 (1980) (commercial speech).

Article I, section 8, in contrast, focuses not upon the nature of the individual speech, but upon the nature of the governmental interference with speech—what we recognize as the *Robertson* categories. *See, e.g.*, *State v. Plowman*, 314 Or 157, 163-64, 838 P2d 558 (1992) (discussing *State v. Robertson*, 293 Or 402, 649 P2d 569 (1982)).

> circumstances'), as well as that A&W 'may cooperate with legal authorities *** in the investigation of any suspected or alleged crime[.]'"

De Witt Simons, 329 Or App at 518-19 (first omission added; second omission and brackets in original).

We understand the state to propose, and the Court of Appeals to have based its decision on, two possible rationales. The first is that, generally, there is no privacy right under Article I, section 9, when using public Wi-Fi. The second is that, even if there is some privacy right generally, there is no privacy right under Article I, section 9, when the terms of service required for use of that public Wi-Fi inform the user of the possibility that the provider may monitor network activity and report it to law enforcement. We disagree with both those rationales because they place insufficient focus on the governmental action involved and fail to locate that action within the broader social norms of behavior to determine whether, "if engaged in wholly at the discretion of the government," said action would "significantly impair 'the people's' freedom from scrutiny." *Campbell*, 306 Or at 171.

We turn to the state's first rationale—that "it is not the *location* of defendant's internet usage, or the fact that he accessed a network for free, that extinguishes his right to privacy. It is defendant's use of a third party's property, knowing that the third party could monitor and share his activity, that extinguished his right to privacy." (Emphasis in briefing.) As we will explain, that argument sweeps too broadly—it ignores the fact that, as a practical matter, *every* decision to access the internet carries with it the risk of third-party monitoring. If adopted, the state's rationale would render privacy a historical footnote.

1. *Merely communicating over public Wi-Fi does not eliminate an Oregonian's Article I, section 9, right to privacy.*

Participation in the modern world virtually requires access to the internet. The United States Supreme Court has observed that internet-enabled smartphones are "'such a pervasive and insistent part of daily life' that carrying [them] is indispensable to participation in modern society." *Carpenter*,

585 US at 315 (quoting *Riley v. California*, 573 US 373, 385, 134 S Ct 2473, 189 L Ed 2d 430 (2014)). Our physical and virtual lives are lived simultaneously. Indeed, *Riley* noted survey evidence suggesting that, among smartphone users, 12 percent of us are so connected to our virtual lives that we use our "phones in the shower," 573 US at 395—a figure that dates from 2013, and so likely understates the level of use today.

Nearly every member of society, young or old, rich or poor, housed or unhoused, will use the internet to conduct what they intend to be private business—indeed, in many cases they must do so. In our age of paperless billing and cloud-based storage, health records are accessed and finances are managed online. On most days, many—if not most—Oregonians will find themselves in a location serviced by a Wi-Fi network, and there are legitimate reasons, both financial and technological, to use those networks.

As *amici* point out, multiple studies show that lower-income Americans are significantly less likely to have access to home broadband and, thus, are more likely to rely on public Wi-Fi options. One such study found a 75 percent correlation between median household income and broadband access across all U.S. counties.[2] Rural communities face a disproportionate lack of high-speed home internet access, resulting in increased use of publicly available Wi-Fi.[3]

Even without economic incentives to connect to Wi-Fi, users may nevertheless elect to connect to various public Wi-Fi hotspots throughout their day because of the pragmatic advantages of doing so. Connecting to available Wi-Fi can provide higher speed for internet browsing. It can provide a more stable internet connection. It can compensate for poor cell phone reception. Wi-Fi can also improve the accuracy of location data, which can be useful when a user regularly uses mapping applications or wants to locate a device using another connected device. Further, in many instances, our

[2] Jeremy Nevy, Internet Access and Inequality, Social Policy Lab (Sept. 30, 2021), https://www.socialpolicylab.org/post/Internet-access-and-inequality (accessed Mar 19, 2026).

[3] Darrell M. West & Jack Karsten, Rural and Urban America Divided by Broadband Access, Brookings (July 18, 2016), https://www.brookings.edu/article (accessed Mar 19, 2026).

devices connect to available Wi-Fi networks automatically, without the user even realizing it: for example, when a device recognizes a previously accessed Wi-Fi hotspot.

Simply put, the use of the internet is a modern necessity, and wireless access is part and parcel of that.

Any access to the internet, whether through Wi-Fi or not, carries a degree of risk of public exposure because internet access *must be* provided by a third-party internet service provider (ISP). No one accesses the internet entirely on their own. Modern internet life necessarily involves interaction with at least one party, and, typically, many parties. Even Wi-Fi provided by an individual's "home network" requires the services of a third-party—the ISP. Using Wi-Fi while visiting a friend's home involves the homeowner and that homeowner's ISP. Wi-Fi provided by an apartment complex, bundled as part of the rent or utilities, may involve the property management company, the building's owner(s), and an ISP. Wi-Fi provided as an amenity, such as Wi-Fi provided by a hotel for its guests, may involve a company managing the hotel, the owner of the hotel, a separate company that services the equipment, and an ISP. And all of that is before the user accesses a website that itself may also monitor traffic.

The state argues that "knowing that the third party could monitor and share his activity *** extinguished [defendant's] right to privacy," but the proposition that a privacy right is extinguished by a mere possibility of monitoring and disclosure by a third party is an argument that we have already rejected in multiple contexts.

In *Lien/Wilverding*, 364 Or 750, we considered whether law enforcement's inspection of the defendants' garbage *after* it had been set out on the curb for disposal invaded the defendants' protected privacy interests. We noted that—generally—when one puts opaque and closed garbage bins out for collection, the sanitation company "would pick up their garbage, commingle it with the garbage of hundreds of other households on the garbage truck route, and take it to the landfill." *Lien/Wilverding*, 364 Or at 760. Based on the way that process ordinarily transpires, we noted that general social norms indicated it would be "highly improper

for others—curious neighbors, ex-spouses, employers, opponents in a lawsuit, journalists, and government officials, to name a few—to take away [one's] garbage bin and scrutinize its contents." *Id.* at 761. Our point was not that it would be illegal or even unheard of for some private citizen to take away someone else's garbage to inspect it; our point was that it would be considered contrary to social norms.

In light of those prevailing societal norms, we concluded in *Lien/Wilverding* that giving the government wholly unfettered discretion to take away a person's garbage to inspect it, even after it had been left on the curb for pickup, would violate a person's privacy interest under Article I, section 9. *Id.* at 763. In other words, it would "significantly impair 'the people's' freedom from scrutiny." *Campbell*, 306 Or at 170. We concluded that this constitutionally protected privacy interest existed even though some risk of "public" exposure had occurred:

> "[W]e recognize, given the realities of living in modern society and technological changes, that privacy norms exist notwithstanding some limited public exposure of information, in this case, putting out garbage in a closed bin for pickup by the sanitation company at curbside, an area accessible to members of the public other than the sanitation company."

Lien/Wilverding, 364 Or at 764.

Notably, in *Lien/Wilverding*, we measured the impropriety of the governmental conduct, in part, by considering whether the act, if done in a non-law- enforcement setting, would violate social norms or general civil law. To illustrate, the court explained:

> "In *McLain v. Boise Cascade Corp.*, 271 Or 549, 554, 533 P2d 343 (1975), the court described the general rule permitting recovery for invading someone's seclusion—a species of tortious violation of privacy—by reference to the *Restatement (Second) of Torts* section 652B (1961), which provided:
>
> > "'One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another, or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable man.'

> "This court later explained that the tort protecting one's seclusion and private affairs 'protects the right of a plaintiff to be let alone.' *Mauri v. Smith*, 324 Or 476, 482, 929 P2d 307 (1996) (internal quotation marks omitted). And, '[i]t is now well established in Oregon that damages may be recovered for violation of privacy.' *McLain*, 271 Or at 554. Tortious invasion of privacy is one of the limited number of torts in Oregon in which a plaintiff may be awarded damages consisting solely of mental suffering caused by the violation. *Hinish* [*v. Meier & Frank Co.*, 166 Or 482, 506, 113 P2d 438 (1941)]."

Lien/Wilverding, 364 Or at 763 (footnote omitted). Thus, the court concluded, "[b]ased on social and legal norms, *** for purposes of Article I, section 9, [the] defendants in [that] case had privacy interests in their garbage that had been placed within a closed, opaque container and put out at curbside for collection by the sanitation company." *Id.* at 763-64.

The state's argument in this case, that "knowing that the third party could monitor and share his activity *** extinguished [defendant's] right to privacy," was rejected by us, in another context, in *Gollersrud v. LPMC, LLC,* 371 Or 739, 750-51, 541 P3d 864 (2023). In *Gollersrud*, the plaintiff and his mother brought suit against LPMC, LLC, among others. LPMC subpoenaed emails between Gollersrud and his mother that were located on three of Gollersrud's former employers' email servers after Gollersrud had left employment with each of the respective companies. Gollersrud objected to the scope of the subpoenas because some of those emails on each server included emails to his attorney seeking legal advice.

The issue in that case was one of statutory interpretation. OEC 503(2) describes the attorney-client privilege and is codified at ORS 40.225:

> "A client has a privilege to refuse to disclose and to prevent any other person from disclosing *confidential communications* made for the purpose of facilitating the rendition of professional legal services to the client[.]"

(Emphasis added.) OEC 503(1)(b), in turn, defines "confidential communication" as:

> "a communication *not intended to be disclosed* to third persons other than those to whom disclosure is in furtherance of the rendition of professional legal services to the client or those *reasonably necessary for the transmission of the communication*."

(Emphases added.)

LPMC argued that the communications could not be confidential because Gollersrud's employer had the ability, and the right, to monitor employee emails. We rejected that argument as "ignor[ing] the practicalities of modern life." *Gollersrud*, 371 Or at 749-50. We reasoned:

> "LPMC's argument, which, as noted, is grounded in a risk of possible disclosure, presupposes that personal email contains no such risk. That assumption does not bear weight. Though an employer may have a comparatively broad right to monitor the email messages flowing through its systems, they are not the only party with a qualified right to do so. Most personal email is hosted by 'free' email service providers (Gmail, Yahoo! Mail, AOL Mail, etc.) who themselves reserve the right to monitor the contents. As an example, Google's current terms of service provide that when a user sends or receives 'content,' including emails, they provide Google with a 'worldwide,' 'non-exclusive,' and 'royalty-free' license to 'host, reproduce, distribute, communicate, and use'; 'publish, publicly perform, or publicly display'; or 'modify and create derivative works based on' that content.'"

Id. at 750-51 (internal quotation marks and citation omitted).

Reasoning similarly here, we conclude that it is a necessary concession of modern life that, to use the internet, one must access it through channels controlled by others, which make one's browsing activity potentially viewable by third parties. That does not change the societal norm that a person's internet searches and browsing activities are reasonably considered to be private. In this case, had another A&W network user monitored the communications of other patrons for over a year, we would have little difficulty concluding that that behavior would universally be viewed as socially offensive and unacceptable, and it might well generate a suit by one patron against another for invasion of privacy.

To summarize, then, the mere fact that, to access the internet, society has accepted that multiple private entities along the path of a communication may, in theory, monitor the traffic does not equate to social acceptance that the government would use Wi-Fi networks to surveil its citizenry. For Article I, section 9, Oregonians have a *right* to freedom from governmental scrutiny, even if they may not have an *expectation* to freedom from potential third-party scrutiny. It follows, then, that the mere fact that a person browses the internet over a Wi-Fi network or an internet connection operated by the third party does not extinguish that individual's Article I, section 9, privacy interest in that browsing activity.[4]

2. *The terms of service here did not eliminate defendant's right to privacy under Article I, section 9.*

Having concluded that Oregonians enjoy a right to privacy in their internet communications, even when accessing the internet via a third-party provider, including a Wi-Fi operator, we further conclude that acknowledging a terms-of-service provision that includes a notice to the user that the proprietor may monitor activities and cooperate with law enforcement does not extinguish that privacy right.

We reiterate that, in considering issues such as these, we will not "ignore[] the practicalities of modern life." *Gollersrud*, 371 Or at 749-50. As we have explained, one does not access the internet on one's own. For those same reasons, no one accesses the internet without encountering at least one terms-of-service provision. The terms of service that A&W utilized for access to its Wi-Fi are not materially distinguishable from the terms of service always present when one accesses the internet, including when using the internet in one's own home, under a contract with one's own ISP. As *amici* point out, the vast majority of ISPs reserve the right to monitor internet activity and share information

[4] We are not called upon to decide, and do not decide, whether the Article I, section 9, privacy right that we recognize today extends beyond this factual context to include internet activities conducted by an individual who is unlawfully present from the start—*i.e.*, a hacker—on a private, secured, network, or internet activities conducted by an individual on a public network who has been previously banned or ejected from that network.

with law enforcement.[5] Verizon, for example, prohibits subscribers from using its internet access service "in ways that *** violate any law" and "reserve[s] the right to provide information about your account and your use of the [internet access] Service to third parties, including law enforcement."[6] Similarly, Xfinity requires users to agree to "not use the Web Services for any unlawful purpose," and reserves the right to disclose information about users "to enforce our rights under our terms of service."[7]

Given the ubiquity of terms-of-service provisions when accessing the internet, if such terms were to eliminate Article I, section 9, privacy rights, there functionally would be no privacy in one's internet activities, ever. Wi-Fi hotspots and ISPs would become access points for governmental mass surveillance without limitation.[8] Beyond ren-

---

[5] *See, e.g.*, Pew Research Center, *Internet, Broadband Fact Sheet* (Nov 20, 2025), https://www.pewresearch.org/Internet/fact-sheet/Internet-broadband; *see also* Xfinity, "Web Services Terms of Service" (2024), https://www.xfinity.com/terms/web (citing Xfinity, "Our Privacy Policy," https://www.xfinity.com/privacy/policy#privacy-who); Spectrum, "Spectrum Residential Internet Services Agreement," https://www.spectrum.com/policies/residential-Internet-services-agreement (citing Spectrum, "Spectrum Subscriber Annual Privacy Notice (2023)," https://www.spectrum.com/policies/spectrum-customer-privacy-policy); Verizon, "Verizon Online Terms of Service for Verizon Internet and Value Added Services," https://www.verizon.com/about/terms-conditions/verizon-online-terms-serviceverizon-business-Internet-and-value-added-services (all accessed Mar 20, 2026).

[6] *See* Verizon, "Verizon Online Terms of Service for Verizon Internet and Value Added Services," https://www.verizon.com/about/terms-conditions/verizon-online-terms-service-verizon-business-Internet-and-value-added-services (accessed Mar 20, 2026).

[7] See Xfinity, "Web Services Terms of Service," https://www.xfinity.com/terms/web (accessed Mar 20, 2026).

[8] Even under the Fourth Amendment—which has been construed as less protective of privacy than Article I, section 9—such arguments have been rejected. As the Sixth Circuit reasoned,

> "[a]n ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception."

United States v. Warshak, 631 F3d 266, 286 (6th Cir 2010) (citation omitted).

dering constitutional privacy a relic, such a holding would be at odds with our treatment of similar provisions in other contexts. There are terms-of-service equivalents that govern automobile and hotel room rentals, for example, yet we have never held that violating such terms eliminates one's privacy interest in that hotel room or vehicle while it is being used.

Terms-of-service provisions are best understood as agreements between private individuals—*i.e.*, the service provider and the end-user.[9] In that vein, they are akin to private contracts. However, as we noted in *Lien/Wilverding*, "[i]n Oregon, the right to privacy—the individual freedom from government scrutiny—protected by Article I, section 9, is not defined by private property or contractual rights, although such rights may inform the analysis in a given case." *Lien/Wilverding*, 364 Or at 759-60; *see Hinish*, 166 Or at 502-03 ("[W]e deem it unnecessary to search for a right of property, or a contract, or a relation of confidence. The question is whether a right of privacy, distinct in and of itself and not incidental to some other long recognized right, is to be accepted by the courts and a violation of the right held actionable.").

To whatever degree terms-of-service provisions may inform the obligations of the parties to the agreement—the service provider and the end-user—they are not reflective of the general societal and legal norms for government conduct, nor do they dispositively set the standard by which governmental conduct will be judged.[10] We emphasize again that Article I, section 9, focuses on the conduct of the government, and in our analysis, we consider, among other things, whether that conduct is inconsistent with the "general social norms of behavior." *Lien/Wilverding*, 364 Or at 760. Accordingly, to the extent that the terms of service bear

[9] We are not called upon here to decide whether they are true "agreements," rather than contracts of adhesion.

[10] A&W's terms of service here did not reference consent, but we note that some "terms of service" provisions inform the network user that use of the network constitutes consent to disclosure and monitoring by law enforcement. Such language would not alter the privacy right under Article I, section 9, that we recognize here today. However, whether such language establishes an exception to the warrant requirement—for example, consent—is a question not presented here.

on whether an Article I, section 9, right to privacy exists, they only do so by, in part, contextualizing the broader social norm of behavior for everyone, and, thus, in part, the reasonable expectations society sets for the conduct of our government.[11]

Our decision in *State v. Dixson*, 307 Or 195, 766 P2d 1015 (1988), is illustrative. There, officers were investigating a suspected marijuana grow operation on what they understood to be land belonging to a lumber company. They sought and obtained the lumber company's permission to search for the marijuana plants. However, they ultimately discovered the plants on what turned out to be property belonging to the defendants. The issue in *Dixson* was whether the officers were conducting a warrantless search when they entered the defendants' property. We recounted the facts leading to the officers' entrance onto the defendants' property as follows:

> "The officers drove onto the property by way of a public road until they reached a dirt logging road the informant had described as leading to the marijuana. Unknown to the officers, this road extended onto property being purchased by defendants Lorin and Theresa Dixson, and on which they lived. The dirt road had fallen into disuse and no longer was passable by car. The trunk of a large tree lay across the road and, a little further on, a wire cable with a 'No Hunting' sign on it stretched across the road. The officers left their car and walked past the fallen tree and wire cable. Just past the cable was another dirt road running along a fence line. This road also had a wire cable and 'No Hunting' sign stretched across it. The officers continued walking down this second road. At a bend in the road, they encountered another 'No Hunting' sign. The area was rural and covered with thick brush."

Dixson, 307 Or at 198.

In an argument derived from Fourth Amendment jurisprudence, the state had contended that the police had not conducted a search, because the constitutional protections against warrantless searches did not apply to "open

[11] Even behavior that might be socially acceptable amongst the populace can nevertheless still exceed the bounds of Article I, section 9, when engaged in by the government. Social norms are an important, but not singularly controlling, consideration.

fields" outside the "curtilage" of a home. This court rejected that argument but held in the state's favor on a different ground. Employing the "social norm" test under Article I, section 9, that we previously described, the court concluded that the police officers had not conducted a search because, in the circumstances, no one would have known the land was closed to the public. *Id.* at 211-12. Accordingly, in the court's view, the officers had behaved exactly as any reasonable member of the public would have under the circumstances. We noted that, "[i]n this society, signs, such as 'No Trespassing' signs, the erection of high, sturdy fences and other, similar measures are all indications that the possessor wishes to have his privacy respected." *Id.* at 211. None of those were present. We concluded:

> "[O]n this record there was no objective reason for the officers to believe that, in addition to the restriction on hunting, other uses such as hiking were forbidden. In this state, with its expanses of rough and open country, hiking, camping and the like commonly occur on land that is owned by large companies and individuals. Unless they intended to hunt, neither the officers nor anyone else would have understood the posted signs to be intended to exclude them from the property entirely."

Id. at 212 (citation omitted). Importantly, in holding that the police conduct in *Dixson* was not an unconstitutional search, we reiterated:

> "Allowing the police to intrude into private land, regardless of the steps taken by its occupant to keep it private, would be a significant limitation on the occupant's freedom from governmental scrutiny. Article I, section 9, does not permit such freewheeling official conduct."

Id. at 211.

Applying those principles here, we conclude that, although the terms of service made it clear that A&W might monitor network traffic, nothing in the terms of service in this case suggests that it was generally socially acceptable for anyone on the A&W network to be monitoring and reading the traffic of other users. Stated another way, nothing in the terms of service supports an argument that it was generally socially acceptable for anyone other than the provider,

much less the government, to surveil users of the network. In fact, at least one of those terms implied exactly the opposite: that A&W would only "disclose *** communications and activities using the Wi-Fi System in response to *lawful requests by governmental authorities, including Patriot Act requests and judicial orders*." (Emphasis added.)

In sum, we conclude that defendant had an Article I, section 9, right to privacy in his internet activities, and the fact that he accessed the internet from A&W's Wi-Fi network, or that he acknowledged A&W's terms-of-service provision to do so, did not eliminate that right to privacy.[12]

3. *Our decision in State v. Meredith does not require a different conclusion.*

The state relies heavily on our decision in *State v. Meredith*, 337 Or 299, 306, 96 P3d 342 (2004) in arguing that the warrantless surveillance of defendant's internet activities was not a search under Article I, section 9. The state contends that "[d]efendant's situation here is legally indistinguishable from that of the defendant in *Meredith*." We disagree.

Meredith followed and effectively flowed from our decision in *Campbell*, and, therefore, we briefly describe our decision in *Campbell* before turning to our analysis of *Meredith*. In *Campbell*, 306 Or 157, the government—without first securing a warrant—surreptitiously attached a radio transmitter to the defendant's privately owned car while it was parked in a public lot. That transmitter "broadcast[ed] a signal that enable[d] the police to locate [it], with little delay," when the car was up to 40 miles away. 306 Or at 166. Using that technology, law enforcement officers used an airplane to locate defendant's car visually, saw defendant exit his car and commit a residential burglary, and proceeded to charge him with that offense.

[12] The dissent posits a fundamental deconstruction and reworking of Article I, section 9's approach to what constitutes a "search," which would involve modifying decades of precedent. It is the prerogative of any member of this court to express their thoughts in separate opinions. Those separate opinions should not be taken as any indication of how the court, as a whole, would address an issue in a future case, nor as an invitation by the court for litigants to undertake such arguments. Here, the dissent's proposed reworking was not argued by the parties, and we have no need to address it on the merits.

On review of the defendant's convictions, we held that prevailing societal and legal norms compelled us to conclude that the government's clandestine attachment of a radio transmitter to a private car—which enabled it to monitor defendant's movements from a significant distance—significantly impaired the defendant's right to be free from governmental scrutiny. *Id.* at 171-72. The surveillance required the government to engage in a trespass to affix the transmitter to the defendant's car. Once it was affixed, the government's surveillance (and the transmitter itself) became "much more difficult to detect" than traditional forms of surveillance would have been. *Id.* at 172. For example, the transmitter enabled the government to "observe a range of conduct that normally would have been inaccessible to the general public or to government officials." *Meredith,* 337 Or at 306 (describing the import of the transmitter in *Campbell*). We concluded that, if that type of conduct were permitted wholly at the discretion of the government, then "no movement, no location and no conversation in a 'public place' would in any measure be secure from the prying of the government. *** That is nothing short of a staggering limitation on personal freedom." *Campbell,* 306 Or at 172.

Years later, in *Meredith*, we concluded that the United States Forest Service's (USFS) use of the same technology on a truck owned by USFS did *not* implicate Article I, section 9. In that case, the USFS employed the defendant as a fire prevention technician in the Tiller District of the Umpqua National Forest. *Meredith*, 337 Or at 301. The USFS supplied technicians with trucks to use while working in the Tiller District. The trucks were required to remain on the job site, and employees checked the keys out and back in at the beginning and end of a shift. Although the defendant customarily used the truck at issue, that truck was not assigned to her and, if it was unavailable, she used a different truck. *Id.*

The USFS district manager authorized a USFS law enforcement agent to affix a transmitter to the USFS-owned truck that the defendant customarily used during work in the Tiller District. *Id.* The transmitter did not enable law enforcement to see or hear the defendant in the cab of the truck. *Id.* at 306 n 2. It did, however, allow law

enforcement to locate the truck within the Tiller District during the defendant's shift. Law enforcement surveilled the truck from an aircraft and saw the defendant exit the truck and start a fire. *Id.* at 302. The defendant was charged with first-degree arson for that conduct.

We concluded that the societal context at play in *Meredith* was different in constitutionally significant ways from the context in *Campbell*. *Id.* at 305. It bears repeating that *Meredith* involved the USFS authorizing USFS law enforcement—its own agents—to place a transmitter on a USFS vehicle. We held that the defendant "had no right to privacy with respect to that truck's location, and the transmitter never disclosed anything other than that location." *Id.* at 307. Consequently, "neither the attachment of the transmitter to the truck nor the subsequent monitoring of that transmitter's location invaded a privacy interest enjoyed by the defendant." *Id.* at 307.

Meredith is therefore contextually inapposite from this case. A&W did not provide the computer to defendant, and defendant was not using his computer at the direction of, or in the employment of, A&W. Here, A&W can best be understood to provide a means of access, like a roadway. To bring *Meredith* closer to these circumstances, it would be akin to USFS providing public access to a USFS owned and maintained road. Certainly, *Meredith* would have involved a different analysis had the USFS purported to authorize government tracking of employees' private vehicles (as in *Campbell*) or authorize surveillance of any vehicle traversing and using a USFS road.

C. *A&W's actions are attributable to the State.*

Having concluded that defendant had an Article I, section 9, privacy right in his internet activities conducted on the A&W network, we turn to the issue not reached by the Court of Appeals—whether A&W's year-long surveillance of defendant's internet activity amounted to governmental action. First, however, we clarify what is, and what is not, at issue. As noted, A&W voluntarily disclosed defendant's activities to the police, who thereafter instructed the business to continue monitoring defendant's activities. In his

written motion to suppress before the trial court, defendant acknowledged that, "[w]hen [the consultant] first noticed evidence that someone was accessing child pornography using the A&W WiFi, he may not have been working for the police." We do not understand defendant to have ever challenged the initial disclosure from A&W to the police, nor to move to suppress any information provided in that initial disclosure. Rather, defendant has consistently argued that, once police responded to A&W's disclosure, only then did they begin to direct A&W's actions in a manner sufficient to render A&W a state actor.

As we have discussed, Article I, section 9, is focused on actions of the government. However, we have recognized that "situations can and do arise in which a private citizen's conduct in pursuing his or her own search and seizure may become so intertwined with the conduct of a state actor that the private citizen's actions are essentially those of the state and should be subject to constitutional restrictions on state searches and seizures." *State v. Sines*, 359 Or 41, 50, 379 P3d 502 (2016).[13] In assessing when private action has become so intertwined as to amount to state action, we look to the objective conduct of law enforcement and those involved to evaluate whether that conduct "communicated to the [informants] that they were authorized to act as agents of the state." *Id.* at 59. Common-law agency principles can be helpful in our evaluation, although those principles are not controlling. *State v. Benton*, 371 Or 311, 322-23, 534 P3d 724 (2023). The critical component is that the evaluation is based on objective statements and conduct, and not on the "subjective motives and understandings" of the state official and the private citizen. *Id.* at 322.

We look to objective statements and conduct and ask whether those statements or that conduct constituted

[13] Our discussions concerning when private actions are attributable to the state for constitutional purposes relevant to criminal investigation have arisen in the context of both Article I, section 9, and Article I, section 11 (guaranteeing, among other things, the accused's right to be heard by himself and by counsel in a criminal prosecution). We have previously indicated that the analysis in those areas "overlap." *State v. Benton*, 371 Or 311, 320 n 3, 534 P3d 724 (2023). However, we note again, as we did in *Benton*, that we do not "conclude that those two constitutional provisions will necessarily be interpreted in the same way in other factual settings." *Id.*

direct or indirect initiation, planning, control, or support for the informant's activities. *State v. Smith*, 310 Or 1, 13, 791 P2d 836 (1990). We have emphasized that there is "no single metric" for evaluating the state's involvement. *Benton*, 371 Or at 324. However, the level of the state's involvement in, or direction of, private action is meaningful. For example, we consider whether there was an agreement between the informant and the state, or, if there was no formal agreement, whether the state encouraged the informant. Even if the state did not actively encourage the informant, the informant nonetheless may, in some circumstances, be considered a state actor if the state did not actively discourage the informant. *Id.* at 325 ("[T]he failure to discourage is likely relevant to the court's broad inquiry into the parties' conduct."). We also consider the informant's motive in gathering evidence, *State v. Acremant*, 338 Or 302, 327-29, 108 P3d 1139 (2005), but, we have explained, motive "is generally insufficient by itself to determine whether an informant acted on the state's behalf." *Benton*, 371 Or at 325. As we explained in *Benton*,

> "[i]n the end, although the precise nature of the state's involvement may vary from case to case, the ultimate inquiry is whether the state was involved enough in guiding, encouraging, or supporting the informant's activities that the informant's conduct is fairly attributable to the state."

Id.

As noted, in this case, the trial court concluded that A&W's consultant was "an agent of the state." Specifically, the trial court found as follows:

> "From July 2018 until June 2019, [the consultant] and [the investigating officer] worked collaboratively to identify when the 'Ian Anderson PC' was logging into child abuse/pornography websites. [The consultant] indicated that he established an alert system that would send an email to [the officer] (at an email provided by [the officer]) any time a child abuse/pornography site was accessed. [The consultant] indicated that he offered this service to [the officer] to assist with the investigation. [The officer] indicated he felt he and [the consultant] were working together to get the information for the investigation. During this period

> of time, A&W network continued to log all websites visited by all users including those catalogued as child abuse/pornography.
>
> "* * * * *
>
> "The court finds that [the consultant] and [the owner] contacted law enforcement and that together with law enforcement, they developed a plan to exchange information such that [the officer] would receive instantaneous email alerts when someone was accessing a child abuse and pornography site on the A&W restaurant network. I find that [the consultant] was an agent of the state, acting on behalf of the state in gathering information for a criminal investigation for child abuse and child pornography viewers."

Based on this record, we agree with the trial court. Nothing in the record suggests that anyone associated with A&W intended to monitor or track defendant or otherwise take any action to surveil defendant's internet activity before law enforcement intervened. Rather, A&W's initial reaction upon learning that its firewall had flagged certain activity by IanAnderson-PC was to notify police. In addition, we note that A&W's consultant testified that he only began monitoring defendant's internet activity in response to law enforcement's express direction, and that his initial reaction was to ask if they should terminate the person's network access.

It is true that the record does not establish that law enforcement demanded A&W's assistance in its investigation of defendant. But, as we have indicated, that is not the standard for determining whether an informant is a state agent. Rather, we ask whether law enforcement was "involved *enough* in guiding, encouraging, or supporting the informant's activities that the informant's conduct is fairly attributable to the state." *Benton*, 371 Or at 325 (emphasis added). A&W's consultant testified that the investigating officer made multiple, specific requests for A&W to gather information with which he complied. A&W also modified its firewall in order to send direct alerts to the officer, and the investigating officer testified that he would call A&W when he failed to receive those alerts. Further, the consultant described his role in law enforcement's work as "participation," and he testified that A&W was "working with [the

police department]." The investigating officer also described law enforcement and A&W as "working together."

On this record, therefore, we conclude, as did the trial court, that the actions of A&W's owner and consultant, from July 2018 until June 2019, were attributable to the state such that they were "subject to constitutional restrictions on state searches and seizures." *Sines*, 359 Or at 50.

III. CONCLUSION

A&W's owner and consultant were state agents for purposes of our Article I, section 9, analysis, and, thus, their actions in assisting law enforcement were governmental conduct. That conduct invaded a protected privacy interest recognized under Article I, section 9, and, therefore, it was a "search." That search occurred without a warrant, and the state has not argued that any applicable exception to the warrant requirement justified a warrantless search. Accordingly, the trial court erred in denying defendant's motion to suppress, and the Court of Appeals erred in affirming that ruling. We remand the case to the trial court for further consideration of the combined motion to controvert and suppress in light our decision.

The decision of the Court of Appeals is reversed in part. The judgment of the circuit court is reversed, and the case is remanded to the circuit court for further proceedings.

BUSHONG, J., concurring in part and dissenting in part.

Defendant lived across the street from an A&W restaurant. He used A&W's free wireless internet (Wi-Fi) network to access and download child pornography onto his laptop computer. A&W discovered what defendant was doing and notified the police. The police obtained the pertinent information from A&W, continued to monitor defendant's use of A&W's Wi-Fi network, used a tracking device to locate defendant, and ultimately used all that information to obtain a warrant to search defendant's home and laptop computer. The state sought to use the evidence obtained in that search to prosecute him. The trial court denied defendant's motion to suppress that evidence, concluding that he

did not have a constitutionally protected privacy interest in using A&W's Wi-Fi network. After a stipulated facts trial, the trial court found defendant guilty of 15 counts of first-degree encouraging child sexual abuse.

The Court of Appeals agreed with the trial court that the police did not unlawfully invade a privacy interest that is protected by Article I, section 9, of the Oregon Constitution or the Fourth Amendment to the United States Constitution when they obtained information about defendant's use of A&W's Wi-Fi network without a warrant. *State v. De Witt Simons*, 329 Or App 506, 540 P3d 1130 (2023). The majority opinion disagrees and reverses the decisions of the trial court and the Court of Appeals, concluding that the police did violate a privacy interest that is protected by Article I, section 9, of the Oregon Constitution. I agree with the trial court and the Court of Appeals on that point and disagree with the majority opinion.

The majority opinion concludes that "the state's year-long surveillance of defendant's internet activities" without a warrant violated Article I, section 9, of the Oregon Constitution. 375 Or at 72. I agree with that conclusion, but not for the reasons explained in the majority opinion. In my view, that surveillance should be treated as a "search" under Article I, section 9, and the police were required to get a warrant before conducting that surveillance. But, as I will explain, I disagree with the majority opinion that defendant had a constitutionally protected privacy right to use A&W's Wi-Fi network.

My conclusion that the year-long surveillance of defendant's use of A&W's Wi-Fi network was a "search" for purposes of Article I, section 9, strays from our traditional approach in deciding whether police activities amounted to a "search." But, as I will explain, I believe that our traditional approach is fundamentally flawed. I would urge this court to reconsider that approach in an appropriate case. Because no party has asked us to reconsider our approach to Article I, section 9, I am not suggesting that we should do so in this case. Rather, I take this opportunity to explain a flaw in our traditional approach and urge litigants to raise

the issue in a future case, so that we may reconsider that approach with the benefit of briefing by the parties.[1]

I begin with our traditional approach, before turning to why, in my view, we should reconsider that approach.

A. *The Traditional Approach for Deciding What Constitutes a "Search"*

Our traditional analytical approach begins with the text of Article I, section 9, which protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure[.]" If the government conduct was not a "search" or a "seizure" within the meaning of Article I, section 9, then we have determined that "the protections of that constitutional provision do not apply[.]" *State v. Meredith*, 337 Or 299, 303, 96 P3d 342 (2004). Under our traditional test, we have concluded that a "search" occurs for purposes of Article I, section 9, when the government invades "a protected privacy interest." *Id.*; *see also State v. Lien/Wilverding*, 364 Or 750, 759, 441 P3d 185 (2019) ("For purposes of Article I, section 9, a 'search' occurs when governmental action invades a protected privacy interest." (Internal quotation marks omitted.)). The privacy interest that is 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).

In deciding whether the government has conducted a "search" within the meaning of Article I, section 9, when it works with a private party to discover and obtain information, we have examined "whether the practice, if engaged in wholly at the discretion of the government, will significantly impair the people's freedom from scrutiny[.]" *Id.* at 171 (internal quotation marks omitted). We do so because "the protection of that freedom is the principle that underlies the

[1] As I will explain, this opinion sets forth the reasons why I think that we should reconsider our approach to interpreting Article I, section 9, in a future case. In general, justices may express in a separate opinion ideas that a justice thinks the court should consider in a later case. The fact that I am doing so here, and no justice has written separately to expressly disagree, does not mean that the court agrees with me that we should reconsider our approach to interpreting Article I, section 9. Rather, whether we reconsider that approach in a future case remains to be decided.

prohibition on 'unreasonable searches' set forth in Article I, section 9." *Id.* We have observed that, "whether a person has a constitutionally protected privacy interest in information that a third party collects and maintains" is a question that "has arisen with increasing frequency, driven in large part by the ability that computers provide to store, aggregate, and analyze vast amounts of data." *State v. Ghim*, 360 Or 425, 436, 381 P3d 789 (2016). We have further noted that the answer to the privacy question "can vary, *** depending on contractual and other restrictions that apply to the third-party's use and dissemination of the information, general societal norms, and the level of generality with which the government analyzes the data." *Id.* at 437.

In this case, the relevant "contractual and other restrictions" that applied to defendant's use of A&W's Wi-Fi network appeared on defendant's computer screen when he logged into the network. Among other things, a user logging into A&W's W-Fi network was informed that, by doing so, the user accepted and agreed to the terms and conditions of A&W's user agreement. The user agreement informed users that they "bear all risks and consequences" for communications that they send or receive via the Wi-Fi network. It also informed users that A&W did not "undertake the security" of data sent through the Wi-Fi network and required users to comply with A&W's acceptable-use policy. That policy prohibited users from transmitting or uploading any "unlawful" or "obscene" material, informed users that A&W could restrict any unlawful internet activity, and informed users that A&W "may disclose" a user's activities using A&W's Wi-Fi network "in response to lawful requests by governmental authorities."

Defendant accepted and agreed to those terms every time that he used A&W's Wi-Fi network, and he re-accepted those terms every two to four hours when he used the network for longer periods.[2] Law enforcement's collection, analysis, and use of the information regarding defendant's

[2] As the Court of Appeals noted, it appears from the record that defendant regularly used A&W's Wi-Fi network. Between July 2018 and June 2019, defendant visited 255,723 webpages while logged into A&W's network; 63 percent of that internet usage involved "legal" activities. *De Witt Simons*, 329 Or App at 519 n 5.

Wi-Fi use was specific to defendant and limited to his use of A&W's Wi-Fi network to access child pornography; the government was not generally searching third-party internet service providers for evidence of criminal activity. Although I share the majority opinion's concerns about police activities that unreasonably intrude upon the people's freedom from governmental scrutiny, I am not convinced that this limited collection of information by law enforcement violated any societal norms.

Under the circumstances, I would conclude, applying our traditional test, that defendant did not have a constitutionally protected privacy right to use A&W's Wi-Fi network, for all the reasons set out in the Court of Appeals' opinion, *De Witt Simons*, 329 Or App at 512-20. That means that, under our traditional approach, the police did not conduct a "search" within the meaning of Article I, section 9, when it obtained evidence from A&W regarding defendant's use of its Wi-Fi network.

B. *Why We Should Reconsider Our Approach to Interpreting Article I, section 9*

The problem with our traditional approach is that it can yield results that are counterintuitive. For example, while I do not think that defendant had a constitutionally protected privacy right to use A&W's Wi-Fi network, I also do not think that the police should be free to conduct a year-long surveillance of defendant's internet usage without obtaining a warrant. That leads me to suggest a reconsideration of our approach to Article I, section 9, especially our traditional analysis of what constitutes a "search" in the first instance.

I am not the first to express dissatisfaction with this court's approach to interpreting Article I, section 9. Former Justice Jack Landau has described this court's approach as "a bit of a muddle." Jack L. Landau, *The Search for the Meaning of Oregon's Search and Seizure Clause*, 87 Or L Rev 819, 859 (2008). According to him, our approach "has developed by fits and starts, with no real analysis and a surprising tendency to rely on federal search and seizure law." *Id.* at 820-21.

In *Priest v. Pearce*, 314 Or 411, 840 P2d 65 (1992), this court adopted a three-part analysis for interpreting the provisions of the original state constitution. Under that approach, we examine (1) the text of the provision, (2) the historical circumstances surrounding its adoption, and (3) case law interpreting the provision. *Id.* at 415-16. We engage in that analysis "to determine the meaning of the provision at issue most likely understood by those who adopted it[.]" *Couey v. Atkins*, 357 Or 460, 490-91, 355 P3d 866 (2015); *see also State v. Davis*, 350 Or 440, 446, 256 P3d 1075 (2011) (stating that our goal in applying that three-part analysis "is to ascertain the meaning most likely understood by those who adopted the provision").

The ultimate objective is "to identify, in light of the meaning understood by the framers, relevant underlying principles that may inform our application of the constitutional text to modern circumstances." *Id.*; *see also Couey*, 357 Or at 490 (stating that our purpose "is not to freeze the meaning of the state constitution to the time of its adoption, but is instead to identify, in light of the meaning understood by the framers, relevant underlying principles that may inform our application of the constitutional text to modern circumstances" (internal quotation marks omitted)); *State v. Rogers*, 330 Or 282, 297, 4 P3d 1261 (2000) (stating that courts seek to "apply faithfully the principles embodied in the Oregon Constitution to modern circumstances as those circumstances arise").

We have not previously engaged in a *Priest* analytical inquiry in determining what constitutes a "search" under Article I, section 9. In *State v. Carter*, 342 Or 39, 42-44, 147 P3d 1151 (2006), this court used the *Priest* methodology for "the first time" in interpreting Article I, section 9. Landau, 87 Or L Rev at 859. We did so in *Carter* in deciding whether a warrant that authorized the police to search for specific items—but did not authorize them to seize those items—complied with Article I, section 9. We have not applied that analytical framework in determining what constitutes a "search" in the first instance.

If we were to do so, we would begin with the text of Article I, section 9:

> "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 person or thing to be seized."

The text "consists of two clauses—a reasonableness clause and a warrants clause—separated by a conjunction and a semicolon." Landau, 87 Or L Rev at 837-38. The "reasonableness" clause itself describes two related, but distinct, concepts: (1) the people's right to be "secure" in their persons, houses, papers, and effects;[3] and (2) what the people are secure from, that is, from unreasonable searches and seizures.[4]

Our traditional approach to determining when police conduct amounts to a "search" went astray, in my view, when we used the people's right to be "secure" in their persons, houses, papers, and effects—often referred to as a "protected privacy interest"—to help us define what constitutes a "search" in the first instance.[5] Conflating those two concepts seems to have been influenced by the "reasonable expectation of privacy" test that the United States Supreme Court adopted in *Katz v. United States*, 389 US 347, 88 S Ct 507, 19 L Ed 2d 576 (1967), in determining whether police conduct amounted to a "search" within the meaning of the Fourth Amendment. *See State v. Holt*, 291 Or 343, 347, 630 P2d 854 (1981) (applying *Katz*'s "reasonable expectation of privacy" test in concluding that a police officer's observation of the defendant masturbating in a doorless toilet stall in a public restroom was not a "search" under Article I, section 9); *State v. Louis*, 296 Or 57, 60-61, 672 P2d 708 (1983)

---

[3] We have traditionally referred to the people's right to be "secure in their persons, houses, papers, and effects" as their right to "privacy."

[4] Former Justice Landau also noted that the reasonableness clause, unlike the Fourth Amendment, "is not phrased in the passive voice." Landau, 87 Or L Rev at 838. That phrasing—declaring that "no law shall violate" the people's right to be secure in their persons, houses, papers, and effects—was "very interesting" to former Justice Landau, "for it suggests that the focus of the framers was on limiting the power of the legislature, not on abuses by executive branch law enforcement officials." *Id.*

[5] The majority opinion notes that, under our traditional approach, "whether there is a protected privacy interest and whether the conduct constituted a 'search' are often two sides of the same analytical coin." 375 Or at 79.

(citing *Katz* in holding that that the police did not conduct a "search" within the meaning of Article I, section 9, when they used a camera with a telephoto lens to photograph the defendant through his living room window). But extrapolating from *Katz* to use a right to privacy—which, as noted, is based on the right to "be secure" provision of Article I, section 9—to define a "search" was, in my view, a mistake.

As we have stated, we are free "to interpret our own constitutional provision regarding search and seizures and to impose higher standards on searches and seizures under our own constitution than are required by the federal constitution." *State v. Caraher*, 293 Or 741, 750, 653 P2d 942 (1982). Doing so is "part of a state court's duty of independent constitutional analysis." *Id.* As we noted in *Caraher*, "we began to build our own state body of law governing searches and seizures" as early as 1901. *Id.* at 752 (citing *State v. McDaniel*, 39 Or 161, 65 P 520 (1901)).

Thus, we should not attempt to define a "search" for purposes of Article I, section 9, by examining whether the police conduct invades a person's "reasonable expectation of privacy," as in *Katz*. Nor should we attempt to define "search" by examining whether police conduct invades "a protected privacy interest." *Meredith*, 337 Or at 303. That approach was based on our rejection of *Katz*'s "reasonable expectation of privacy" test to define a protected privacy interest for purposes of Article I, section 9, as "not the privacy that one reasonably *expects* but the privacy to which one has a *right*." *Campbell*, 306 Or at 164 (emphases in original); *see also State v. Dixson/Digby*, 307 Or 195, 206, 766 P2d 1015 (1988) (noting that, in *Campbell*, this court "expressly rejected the federal 'reasonable expectation of privacy' test for defining privacy interests under Article I, section 9").

Instead of starting with *Katz* and then modifying the federal test, we might want to begin our textual analysis by examining the plain, ordinary meaning of the word "search." *See Jones v. Hoss*, 132 Or 175, 178, 285 P 205 (1930) ("In construing a constitutional provision," "[w]ords which have no well-established technical or legal significance are to be given their plain, natural and ordinary meaning."). Applying that approach, we might first need to

decide whether "search" as used in Article I, section 9, had an established legal significance that could prevent us from giving that word its ordinary meaning. If not, we might start with a dictionary definition of the word. The dictionary defines "search" as: "to look into or over carefully or thoroughly in an effort to find something." *Webster's Third New Int'l Dictionary* 2048 (unabridged ed 2002). Under that definition, the police would conduct a "search" whenever they "look into or over" something to find evidence of a crime. That commonsense approach to what constitutes a "search" would dispense with any need to examine whether the police had invaded a constitutionally protected privacy interest in determining whether their actions constituted a "search."[6]

As applied to this case, I think that the police conducted a "search" within the meaning of Article I, section 9, when the police initially "looked over" the information that A&W had collected before contacting the police. That search likely intruded on defendant's right to be secure in his person, home, papers, and effects. But under the circumstances, I would conclude that that unwarranted search was not unreasonable—and thus, the evidence that A&W collected on its own before contacting the police could be used to obtain an appropriate search warrant to obtain additional evidence—because that evidence was initially gathered by A&W on its own initiative and voluntarily turned over to the police. *See State v. Sines*, 359 Or 41, 62, 379 P3d 502 (2016) (holding that a search and seizure conducted by private individuals without police authorization or involvement did not violate Article I, section 9).

I would also conclude that the police use of a "packet sniffer" tracking device to find defendant's home was a "search" but not an unreasonable one, because merely detecting a signal broadcast from defendant's computer to locate him without using that information to discover the internet sites that defendant had accessed or the information that he had downloaded did not invade a privacy interest that is protected by Article I, section 9. That is, tracking a signal that is emitted by defendant's computer to locate him—without

[6] The privacy inquiry seems more connected, at least textually, to determining whether a police "search" intrudes upon the right of the people "to be secure in their persons, houses, papers, and effects[.]" Or Const, Art I, § 9.

attempting to discover the substance of what defendant was accessing on his computer—did not invade defendant's right to be secure in his person, home, papers and effects.

I would reach the opposite conclusion with respect to the evidence that the police, working with A&W, obtained during the year-long surveillance of defendant's internet usage. Again, that would be a "search" under a commonsense understanding of the word, but it would be an unreasonable search, because a warrant was required for the police to engage in continued surveillance to discover the specific information that defendant had accessed via the internet. Such surveillance, in my view, infringed upon defendant's Article I, section 9, right to be "secure" in his person, home, papers, and effects, and it cannot be justified by any exception to the warrant requirement.

The affidavit that the state submitted in support of its request for a warrant describes both the information that A&W initially turned over to the police—which, in my view, the police permissibly received without a warrant—and the information that the police impermissibly obtained during the subsequent year-long warrantless surveillance of defendant's internet usage. Thus, I agree with the Court of Appeals that the trial court on remand must reconsider whether the evidence obtained from the warranted search of defendant's home and computer must be suppressed under the standards described in *State v. DeJong*, 368 Or 640, 497 P3d 710 (2021). *De Witt Simons*, 329 Or App at 514-25; *see also State v. Turay*, 371 Or 128, 167-69, 532 P3d 57 (2023) (remanding to trial court to apply *DeJong* in determining whether evidence collected during the execution of a warrant that, in part, failed to satisfy the "particularity" requirement of Article I, section 9, must be suppressed).

To the extent that the majority opinion's disposition of this case—a remand to the trial court for further consideration of defendant's combined motion to controvert and suppress—permits that inquiry, I concur in that disposition. But, for the reasons stated above, I respectfully dissent from the majority opinion's conclusion that defendant had a constitutionally protected privacy right to use A&W's Wi-Fi network.