IN THE SUPREME COURT OF THE
STATE OF OREGON

STATE OF OREGON,
Respondent on Review,
v.
CARYN ALINE NASCIMENTO,
Petitioner on Review.
(CC 09FE0092, CA A147290, SC S063197)

On review from the Court of Appeals.*

Argued and submitted November 12, 2015.

Daniel C. Bennett, Deputy Public Defender, Salem, argued the cause and submitted the brief for the petitioner. With him on the brief was Ernest G. Lannet, Chief Defender, Office of Public Defense Services.

Patrick M. Ebbett, Assistant Attorney General, Salem, argued the cause and filed the brief for the respondent. With him on the brief was Ellen F. Rosenblum, Attorney General, and Anna Joyce, Solicitor General.

J. Ashlee Albies, Creighton & Rose PC, Portland, filed the brief for *amicus curiae* Electronic Frontier Foundation. With her on the brief was Jamie L. Williams, Electronic Frontier Foundation, San Francisco, California.

Before Balmer, C. J., and Kistler, Walters, Landau, Baldwin, Brewer, JJ.**

BALMER, C. J.

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

---

* Appeal from Jefferson County Circuit Court, George W. Neilson, Judge. 268 Or App 718, 343 P3d 654 (2015).

** Linder, J., retired December 31, 2015, and did not participate in the decision. Nakamoto, J., did not participate in the consideration or decision of this case.

BALMER, C. J.

The narrow but potentially far-reaching issue in this case is the scope of ORS 164.377(4), which makes it a crime to use, access, or attempt to access a computer or computer network "without authorization." The state argues that, although defendant's employer authorized her to use the computer terminal at issue here, defendant did so for a purpose not permitted by her employer and thus was guilty of computer crime. Defendant contends that, because her access to and use of the computer terminal was authorized by her employer, she cannot be guilty of violating ORS 164.377(4), even if she used the computer for an impermissible purpose. She concedes, however, that her use may have violated her employer's policies or other provisions of ORS 164.377. For the reasons explained below, we agree that defendant's conduct did not violate subsection (4) of the statute, and, accordingly, that the trial court erred in denying her motion for judgment of acquittal. We therefore reverse defendant's computer crime conviction.

Defendant was convicted of theft and computer crime for using a computer terminal at work, which was linked to the Oregon State Lottery, to print and steal lottery tickets. She appealed the conviction for computer crime, arguing that the trial court erred in denying her motion for judgment of acquittal on that count because, she argued, she was "authorized" to use the computer terminal and therefore had not violated ORS 164.377(4).[1] In reviewing the denial of a motion for judgment of acquittal, we describe the facts and all reasonable inferences that may be drawn from those facts in the light most favorable to the state. *State v. Walker*, 356 Or 4, 6, 333 P3d 316 (2014).

Defendant was employed as a deli clerk at Tiger Mart, a convenience store in Madras, beginning in 2007. In February 2009, Masood, the vice-president of the store's parent company, investigated issues relating to the sale of lottery tickets at the Tiger Mart. He found that, between November 2008 and February 2009, there were unexplained

[1] Defendant did not challenge the theft conviction on appeal.

cash shortages well beyond the amount expected in the operation of such a store, sometimes exceeding $1,000 a day. He soon determined that the store also showed a surprisingly large number of sales of Keno lottery tickets, including sales of an unusual number of high-priced tickets. The total shortages between November 2008 and February 2009 exceeded $16,000. After examining cash register receipts and lottery reports, he concluded that the shortages related to the sale of Keno tickets and that they occurred on days when defendant was working. Masood also reviewed video recordings and observed occasions when defendant would move from the deli area to the cash register area and print out and pocket Keno tickets from the lottery terminal. Masood suspected that defendant was printing and taking—but not paying for—those Keno tickets. Although Masood did not work in the store himself and did not train defendant, he testified at one point that defendant was not authorized to use the lottery terminal to dispense Keno tickets, and at another point, in response to a question about whether defendant was supposed to be operating the lottery terminal, stated "Not as far as I know." He further indicated that, to the best of his knowledge, defendant had not been trained to operate the lottery terminal that dispensed Keno tickets.

Donelly, the manager of the Tiger Mart and defendant's direct supervisor, testified that she had trained defendant and other deli employees to use the cash register and the lottery terminal, and that they routinely were required to use them when other employees were busy or taking breaks. She testified that she had authorized defendant to use the lottery terminal and the cash register. She indicated that that practice had been in place before the current owners took over the convenience store and that she did not recall there being any policy prohibiting deli clerks from operating the cash register or the lottery terminal. Another deli employee confirmed Donelly's testimony about deli workers' regular use of the cash register and lottery terminal. Both Masood and Donelly, as well as the other employee, testified that the store had a policy that employees were not to purchase or redeem lottery tickets on their own behalf while on duty.

The state presented evidence about the lottery terminal itself and how defendant was trained to use it. The lottery terminal is a touchscreen machine that is networked to the Oregon State Lottery. The terminal has only three functions: It can print lottery tickets, it can scan lottery tickets to validate whether they are winning tickets, and it can produce reports. It is not networked with the store's cash register. A manager needed to sign in once a day to activate the terminal, but the terminal did not otherwise require any sort of password to operate. Tiger Mart employees received training that, when they sold lottery tickets, they were to collect payment from customers and put the payment in the cash register before using the touchscreen on the lottery terminal to dispense the ticket or tickets.

The state also presented video evidence that, when no one else was around, defendant used the lottery terminal at the Tiger Mart to print Keno tickets, which she then pocketed. There also was evidence that defendant failed to pay for those Keno tickets. Other evidence showed that defendant had redeemed at least one winning ticket through the mail and had redeemed other tickets at a local store. Further evidence was presented correlating some of those tickets to video evidence of defendant using the lottery terminal at the Tiger Mart. Thus, evidence supported the state's theory that defendant used the lottery terminal to print lottery tickets that she took without paying for and that she later redeemed those tickets.

Defendant was charged with one count of aggravated first-degree theft, as well as computer crime. The computer crime statute, ORS 164.377, provides, in part:

> "(2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:
>
> "(a) Devising or executing any scheme or artifice to defraud;
>
> "(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or

> "(c) Committing theft, including, but not limited to, theft of proprietary information or theft of an intimate image.
>
> "* * * * *
>
> "(4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime."

It is of particular significance in this case how the computer crime count was charged. The caption of the indictment cited ORS 164.377(2), but the body of the indictment charged conduct that instead tracked ORS 164.377(4), including the "without authorization" wording that does not appear in subsection (2):

> "The defendant, on or between November 11, 2008 and February 6, 2009, in Jefferson County, Oregon, did knowingly and *without authorization use and access a computer system* operated by Tiger Mart Convenience Store, an entity, under contract to and at the direction of the Oregon State Lottery Commission; contrary to statute and against the peace and dignity of the State of Oregon."

(Emphasis added.)

After the state's evidence was presented, defendant moved for a judgment of acquittal, arguing that the state had not presented sufficient evidence to create a jury question as to whether defendant used the lottery terminal "without authorization," noting the evidence that deli clerks were, in fact, authorized to use the lottery terminal. The prosecutor did not dispute that point, but argued instead that

> "the access alone is not what makes this criminal. It's that the access is for the purpose of under three different categories, devising or executing a scheme or artifice to defraud obtaining money, property, or services through fraudulent pretenses or committing theft—
>
> "* * * * *

> "That's under—from the statute itself, ORS 164.377, and under *State v. Schwartz*, 173 Or App 301 [21 P3d 1128 (2001) (discussing subsections (2) and (3) of the statute)].
>
> "*****
>
> "So therefore, Your Honor, the fact that she did have some apparent authority to operate the machine to sell tickets and to conduct business of Tiger Mart [does not affect] the fact that she then also used the terminal to print out tickets for which she did not pay. That is the unauthorized—the knowing unauthorized use of the terminal. Such that she committed theft while she was doing that and therefore the State has met its elements on that crime."

The trial court denied defendant's motion for judgment of acquittal without explanation. In her closing argument, the prosecutor described the case as involving "a simple issue of did someone steal lottery tickets from the Tiger Mart—Tiger Mart here in town and the Oregon State Lottery." When discussing the computer crime count, the prosecutor stated:

> "[Defendant] went onto the computer, the computer was part of the Oregon State Lottery System, she printed out those tickets, and she did so with the purpose of stealing those tickets. So the theft of the tickets counts as the purpose that is that she is authorized [*sic*], that she was accessing a computer. We're not talking about the time when she was acting as an employee and actually selling tickets to customers who were paying for them. That's not the kind of behavior we're talking about. We're talking about her printing those tickets out for herself so that she could [indiscernible]."

In instructing the jury on computer crime, the trial court followed the wording in the indictment. That is, it instructed that the jury needed to find that defendant used or accessed a computer "without authorization."

As noted, the jury found defendant guilty of computer crime, as well as aggravated first-degree theft, and defendant appealed the computer crime conviction, arguing that the trial court erred in denying her motion for judgment of acquittal. In particular, she argued that ORS 164.377*(4)*

does not criminalize theft by means of a computer—rather, subsection (2) of the statute criminalizes that conduct. Defendant contended that subsection (4) relates only to using or accessing a computer without authorization, and the evidence in this case, while it could have supported a conviction under subsection (2), did not support a conviction under subsection (4). The Court of Appeals rejected that argument, concluding that "[t]here was evidence from which the jury could conclude that [defendant] was authorized to access the physical device itself—the lottery terminal—only to serve paying customers." *Nascimento*, 268 Or App at 722. It therefore concluded that the record was sufficient for the jury to have found that defendant used the computer "without authorization." *Id.*

In this court, defendant maintains that she did not use the lottery terminal "without authorization." She again acknowledges that the evidence could have been sufficient to establish a violation of subsection (2) of ORS 164.377—which prohibits, among other things, using or accessing a computer for the purpose of "obtaining money * * * by means of false or fraudulent pretenses" and "committing theft"—but reiterates that she was not charged under that subsection. *See, e.g.*, *State v. Briggen*, 112 Or 681, 683, 231 P 125 (1924) (court looks to the body of the indictment, not the caption, to determine what crime is charged). Defendant does not dispute that there was evidence that she accessed the lottery terminal to print tickets without having received payment—or having made payment herself—for the tickets. However, she argues that that act does not constitute accessing or using a computer "without authorization." Defendant also suggests that the Court of Appeals' interpretation of subsection (4) is so broad as to raise constitutional vagueness concerns.

The state makes two arguments in response. First, it asserts that defendant used the lottery terminal for a purpose not permitted by her employer. Specifically, the state introduced evidence that Tiger Mart's policy was that deli clerks like defendant were authorized to use the terminal only when a customer wanted to buy or validate a ticket and the cashier was unavailable, and that defendant's use of the terminal to print tickets for herself therefore was "without

authorization," as that term is used in ORS 164.377(4). The state contends that the statute is not unconstitutionally vague because it unambiguously prohibits a person from doing anything with a computer without permission. Second, apparently as an alternative basis for affirmance, the state argues that, even under defendant's definition of "authorization" as related to physical access or use of the computer, rather than access or use only in compliance with an employer's policies, evidence in the record supported the guilty verdict. Specifically, the state points to Masood's testimony that defendant was not authorized to use the terminal at all. As noted, at trial the prosecutor conceded, for purposes of defendant's motion for judgment of acquittal, that defendant did have authorization from her supervisor to use the lottery terminal. The state, however, now asserts that it may disavow that concession and argues that, although Masood's testimony on authorization was contradicted by all of the other evidence on that point, it nonetheless was sufficient to defeat defendant's motion. *See generally* *Outdoor Media Dimensions Inc. v. State of Oregon*, 331 Or 634, 659-60, 20 P3d 180 (2001) (reviewing court has discretion to affirm ruling of lower court on an alternative basis if facts support alternative basis, alternative view of evidence is consistent with trial court's ruling, and record would not have developed in materially different way had prevailing party raised alternative basis below).

We first address—and reject—the state's proffered alternative basis for affirmance. As the narrative above demonstrates, the prosecutor apparently was confused about how the computer crime offense had been charged in the indictment. That is, her argument in opposition to defendant's motion for judgment of acquittal focused on whether the state had provided adequate evidence to satisfy the requirements of ORS 164.377(2)(a), (b), or (c), rather than ORS 164.377(4). To the extent that the prosecutor addressed the concept of "authorization," she agreed that defendant had been given "authority [to] operate the machine to sell tickets and conduct the business of Tiger Mart," but argued that what made defendant's use of the lottery terminal "unauthorized" was that she used the lottery terminal for the purpose of *committing theft*, a use that is

expressly prohibited by ORS 164.377(2)(c). In making those arguments, the prosecutor conceded that defendant was, in fact, authorized by her supervisor as part of her employment to use the lottery terminal to print lottery tickets.

We agree with the state's general proposition that, at least in the abstract, a prosecutor in that circumstance *could* have argued that Masood's equivocal evidence about whether or not defendant was authorized to use the lottery terminal at all was sufficient to defeat a motion for judgment of acquittal on that point, given that the court was required to view all of the evidence in the light most favorable to the state, and not to weigh the evidence. But the prosecutor did not make that argument, and in fact conceded the point.[2] As noted, one of the criteria for our discretionary review of alternative bases for affirmance is whether, had an argument been made in the trial court, the record could have developed in a materially different way. *Outdoor Media*, 331 Or at 659-60. In this case, we have no doubt that, had the prosecutor made the argument that the state now makes, the record might well have developed differently.

The evidence on which the state now relies for affirmance on that ground was equivocal and weak, at best. Had the state relied on it in opposition to a motion for judgment of acquittal rather than disavowing it as the basis for its legal argument, defendant easily could have countered that evidence in her own case-in-chief, as there appears to have been no shortage of witnesses who would have confirmed that defendant was, in fact, trained by her supervisor to use the lottery terminal to print lottery tickets and was expected to do so as part of her job. *See, e.g.,* *State v. Dickerson*, 356 Or 822, 826-27, 345 P3d 477 (2015) (rejecting state's alternative basis for affirmance of denial of motion for judgment of acquittal on different factual theory than pursued by state

[2] We do not fault the prosecutor for failing to pursue that theory of the case. As noted, Masood's own testimony indicated that he did not have personal knowledge of whether defendant was authorized to use the lottery terminal, and the state presented extensive evidence that defendant had, in fact, been authorized by her supervisor to use the lottery terminal and had been trained to do so. Thus, while that theory of the case might have been viable as a technical matter, as a practical matter it is not surprising that the prosecutor would not ultimately want to rely on it in trying to secure a conviction.

at trial, in part because record might have developed differently had state raised theory below). As we observed in *State v. Burgess*, 352 Or 499, 504, 287 P3d 1093 (2012), based on the circumstances of that case, "it would be fundamentally unfair to defendant to sustain defendant's conviction on a separate factual and legal theory that has been proffered by the state for the first time on appeal." That is even more so in a circumstance such as this, where the state conceded in the trial court the factual and legal theory that it advances for the first time on appeal.

We thus return to the issue that was litigated in the lower courts: Whether defendant's use of the lottery terminal to print Keno tickets for herself—tickets that she did not pay for—constituted "computer crime" under ORS 164.377(4), because she printed those tickets "without authorization." Our goal is to determine the intent of the legislature in enacting that statutory provision, which we do by examining the text, context, and legislative history of the statute. *State v. Gaines*, 346 Or 160, 171, 206 P3d 1042 (2009). We again set out subsection (4):

> "Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime."[3]

Although ORS 164.377(1) provides definitions of numerous terms used in the computer crime statute, it does not define "authorization" or "without authorization." It does define "computer" and "computer system," and the latter term specifically includes lottery terminals. ORS 164.377(1)(b), (f). Subsection (1) also defines the verb "access," as "to instruct, communicate with, store data in, retrieve data from or otherwise make use of any

---

[3] A violation of ORS 164.377(4) generally is a misdemeanor. In this case, it was treated as a class C felony, because ORS 164.377(5)(b) provides:

> "Any violation of this section relating to a computer, computer network, computer program, computer software, computer system or data owned or operated by the Oregon State Lottery or rented, owned or operated by another person or entity under contract to or at the direction of the Oregon State Lottery Commission shall be a Class C felony."

resource on a computer, computer system or printer." ORS 164.377(1)(a). It is undisputed that, when defendant used the lottery terminal to dispense Keno tickets, she "used" and "accessed" a "computer system," as those terms are used in ORS 164.377.

As to the meaning of "without authorization," the state proposes an extremely broad definition, arguing that any time a person uses or accesses a computer for a purpose not permitted by the computer's owner, the person does so "without authorization" and commits computer crime. For that reason, the state contends, even though defendant was authorized to physically use the terminal to print Keno tickets, because she violated her employer's policy by using it to print Keno tickets for her own use (and also by not paying for them), her use was "without authorization," in violation of ORS 164.377(4). In short, the state's argument is that an employee's otherwise authorized use of an employer's computer is "without authorization"—and therefore a computer crime under ORS 164.377(4)—whenever the employee's access or use violates the employer's personnel or computer use policies.

Defendant, on the other hand, notes that the 1985 Legislative Assembly that enacted subsection (4) was concerned with remote "hacking" of computers by persons with no right to access those computers. Defendant suggests that the statute therefore was not meant to reach conduct such as hers, which she characterizes as "authorized use for an impermissible purpose." Rather, she argues, when a person is permitted to use an employer's computer system, and when the person uses the computer as permitted—here, to print lottery tickets—the person's use is "authorized," even if the use is for an impermissible purpose. She asserts that ORS 164.377(4) addresses authorization to use or access a computer, not the particular purpose for or circumstances of that use.

Amicus curiae Electronic Frontier Foundation contends that the Court of Appeals and the state's reading of the statute—which arguably criminalizes any computer use in violation of an employer's personnel or computer use policies—is unworkably broad because it gives private

entities the power to decide what conduct in the workplace is criminal and what is not. *Amicus* argues that "without authorization" should be construed narrowly, as federal courts have construed somewhat similar provisions in the Computer Fraud and Abuse Act, 18 USC § 1030, as accessing a computer by circumventing security measures, rather than simply violating an employer's use restriction policies.

As noted, the parties agree that defendant "accessed" and "used" a "computer network." The question is whether she did so "without authorization." The meanings of "authorization" and "authorize" are not obscure. "Authorization" is simply "the state of being authorized." *Webster's Third New Int'l Dictionary* 146 (unabridged ed 2002). "Authorize," in turn, means "to endorse, empower, justify, or permit by or as if by some recognized or proper authority." *Id.* We agree with defendant that her employer "empowered" and "permitted" her to use the lottery terminal. The actual use that she made of the lottery terminal—to print lottery tickets—was a use "authorized" by her employer.

The state does not disagree that defendant was authorized to use the lottery terminal to print lottery tickets, but contends that her use of the terminal became "unauthorized" when she used it to print tickets for herself without paying for them. That use was "unauthorized" within the meaning of ORS 164.377(4), the state contends, because it was for a purpose that was prohibited by her employer's policies. For her part, defendant concedes that she may have violated her employer's computer use or personnel policies by printing lottery tickets for herself and failing to pay for them. She also concedes that she may have violated provisions of the computer crime statute other than ORS 164.377(4), in addition to the theft statute under which she also was convicted. However, she maintains that ORS 164.377(4) does not criminalize her conduct here. She points out that she was trained and authorized to use the computer to print lottery tickets and, moreover, that she did not bypass any security measures or access any protected data. For those reasons, she asserts, her use of the computer to print lottery tickets was authorized, and it did not become "unauthorized," even though her purpose in printing tickets for her own use (and

not paying for them) violated her employer's personnel or computer use policies.

It is difficult to square the state's position with the text of ORS 164.377(4). The text establishes a binary division between those who are "authorized" to access or use a computer and those who are not. The text does not distinguish between use that is authorized for certain purposes (such as those permitted by employer policies) and use that otherwise would be authorized but that is inconsistent with those policies. Indeed, subsection (4) of the statute does not focus on the purpose or manner of use at all, but only on whether the access or use is "authorized."

As noted, "access" is defined in the computer crime statute as "retriev[ing] data" or "mak[ing] use of any resource on a computer." ORS 164.377(1)(a). If a person is "empowered" or "permitted"—the dictionary synonyms of "authorized"—by the appropriate authority to "retrieve data" or "make use" of the computer, then that use is "authorized." Applying those words in their ordinary senses, it is a stretch to suggest that an employee who uses her work computer to send a private email during the work day—or check Facebook or buy a movie ticket—contrary to her employer's policy against personal use, has "accessed" or "used" the computer "without authorization," although she may have violated her employer's policy. Nothing in the text of the statute suggests that the legislature intended such a result. As defendant argues, the state's interpretation would criminalize not only "unauthorized" use of a computer, but also "authorized use for an impermissible purpose." Such an interpretation would require adding words to the text of the statute that the legislature did not use. *See* ORS 174.010 (court may not add words to statute).

Viewed in that light, the text supports defendant's assertion that her use of the lottery terminal to print Keno tickets—as she was trained and permitted by her employer to do—was "authorized" use. The fact that she printed the tickets for her own use and did not pay for them may have violated company policies and other parts of the computer crime statute (in addition to the theft statute), but her use was not "without authorization" as that term is used in ORS

164.377(4).[4] That conclusion is supported by the evidence that, once a store manager had signed into the terminal and activated it at the beginning of the work day, employees such as defendant could use the terminal to print Keno tickets without additional authentication or permission. When defendant physically accessed and used the terminal to print Keno tickets, that access and use was authorized by her employer. Moreover, there was, for example, no evidence that defendant circumvented any computer security measures, misused another employee's password, or accessed any protected data. The sole basis for the state's claim that defendant's printing of Keno tickets was "unauthorized" was the employer's policy that employees were not supposed to print tickets for their own use and were supposed to obtain payment for tickets before printing them.

The legislative history of ORS 167.377(4) supports defendant's argument that the statute was intended to criminalize access or use of a computer by someone who had no authority to do so, the kind of intrusion or access to a computer by unauthorized third parties commonly referred to as "hacking." HB 2795, as introduced during the 1985 legislative session, was concerned with the theft of cable television services. *See* Bill File, HB 2795 (1985). Representatives of General Telephone Company urged the adoption of an amendment to that bill that would deal with a related problem, "computer crime, or computer hackers if you will." Tape Recording, House Judiciary Committee, Subcommittee 1, May 6, 1985, Tape 576 (testimony of Dave Overstreet, General Telephone Company). The head of General Telephone's security department noted that many businesses now used computers, stating that, "what we're trying to get into the statute is a part of the law that will prevent people from calling into someone's computer." *Id.*

[4] We do not rely on federal court interpretations of the Computer Fraud and Abuse Act, 18 USC § 1030, because the text of the federal and state statutes have some differences and because ORS 164.377 was passed a decade before the federal law. However, we note that the federal courts have interpreted that statute, which prohibits computer access "without authorization"—and also, arguably broader than the Oregon statute, use that "exceeds authorized access"—*not* to prohibit use that is otherwise authorized but that violates employer use restrictions. *See, e.g.*, *United States v. Nosal*, 676 F3d 854 (9th Cir 2012) (en banc) (so holding).

He gave, as examples, people who had obtained access to business computers that lacked security systems and had altered business documents, as well as individuals who had made their way remotely into telephone company computers and obtained and then publicly posted confidential telephone billing codes. *Id.*

In response to a legislator's concern that the amendment might restrict computer hobbyists who used telephone modems to connect with other computers, Marion County District Attorney Dale Penn emphasized that the law would apply to only third parties who had no authority to access the remote computer:

> "There we get into the definition of 'access.' I think *** if you call up to a computer system and you're not authorized you're probably not even going to be able to get the menu up. If you're calling to a bulletin board you're going to see the menu. And that's not what we're addressing here. *We're addressing a computer system in which you're not authorized to dial.* You won't know the codes."

Id. (Emphasis added.) Testimony before the Senate Judiciary Committee was to the same effect. General Telephone's representative, Overstreet, again testified in support of the computer crime provisions, which he described as addressing "computer hackers—persons who use computers to defraud." Tape Recording, Senate Judiciary Committee, June 7, 1985, Tape 180, Side A; Minutes, Senate Judiciary Committee, HB 2795, June 7, 1985, 18.

The legislative history thus shows that the computer crime provisions were intended to address the unauthorized access of a computer by "hackers" or by others who had no authority whatsoever to use the computer—who, in the context of the technology of the time, were "not authorized to dial." There is no indication at all that the bill would reach the conduct of a person, such as defendant here, who was authorized by a computer owner to use the computer, but did so in violation of the owner's policy or for a purpose not permitted by the owner.

The state acknowledges that legislative history and the concerns that animated the legislature's enactment of ORS 164.377. It argues, however, that the text that the

legislature adopted "is not so limited," and that it prohibits *all* "access" that is "without authorization." As both parties recognize, "[t]he legislature may and often does choose broader language that applies to a wider range of circumstances than the precise problem that triggered legislative attention." *South Beach Marina, Inc. v. Dept. of Rev.*, 301 Or 524, 531, 724 P2d 788 (1986). But that important teaching does not mean that we necessarily interpret statutes in the broadest possible sense that the text might permit. Indeed, as we recently noted in *Walker*, 356 Or at 17, "[i]f, in fact, the legislative history reveals that the legislature had a narrower understanding of the term in mind, and if that narrower meaning is consistent with the text, even if not compelled by it, the legislative history would be a basis on which we appropriately may construe the text more narrowly."

Here, the legislative history supports defendant's view that the legislature intended ORS 164.377(4) to prohibit computer access or use by a person who accessed or used a computer without permission or authorization from the owner. Nothing in the legislative history suggests that the statute was intended to reach a person who was trained and authorized to use a particular computer, but did so for an unpermitted purpose. As discussed above, the text and context of the statute provide a sufficient basis for deciding this case: ORS 164.377(4) does not distinguish between a person's "authorization" to access or use a computer for some purposes and not for others; the access or use is authorized, or it is not. The legislative history simply reinforces that interpretation.

In summary, we conclude that the phrase "without authorization" applies to the "use" or "access" of the computer. A person's "authorization" to access or use a computer may be restricted by a password or other authentication or security procedures—but defendant's employer here did not so restrict her use. Nor was defendant's use of the computer—to print lottery tickets—inconsistent with the scope of her authorized use. We disagree with the state's position that an employee's authorized use of an employer's computer becomes "without authorization" for purposes of ORS 164.377(4) simply because the employee used the computer for a purpose not permitted by the employer's personnel or

computer use policies.[5] Such impermissible use, of course, may lead to personnel actions or other private discipline or to possible proceedings under other statutes, but it does not violate ORS 164.377(4).

Applying that interpretation of ORS 164.377(4) to the facts here, we conclude that no reasonable juror could find that defendant accessed or used the lottery terminal "without authorization" when she printed Keno tickets for herself without paying for them. She was authorized to use the computer to print Keno tickets, and the fact that her conduct violated her employer's policy did not make her computer use "unauthorized." The trial court erred in denying defendant's motion for judgment of acquittal on the computer crime count.

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

---

[5] In interpreting the term "authorization" for purposes of this case, we do not mean to suggest that an employer or other computer owner may not devise means to restrict the scope of access that it authorizes for particular users. This case involves a computer terminal that printed Keno tickets and an employee who was trained and permitted to use the computer to perform that function. As discussed above, after a store manager "signed in" to the computer at the beginning of the day, trained employees, including defendant, were authorized to use the computer to print Keno tickets without further authentication, password use, or other identity verification. 360 Or at 32. A different analysis of "authorization" would be called for if an employer, through use of security codes, password-protected data, or encryption, blocks an employee from access to certain computer functions or data. In a similar vein, Orin Kerr suggests that the policy issues involving "unauthorized" use should be resolved by using authentication requirements—as many websites and computer networks already do—and considering access to be "unauthorized" when "a user bypasses an authentication requirement, either by using stolen credentials or bypassing security flaws to circumvent authentication." Orin Kerr, *Norms of Computer Trespass*, 116 Columbia L Rev 1143, 1171 (2016).