IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON, Plaintiff-Respondent, Respondent on Review, v. CARYN ALINE NASCIMENTO, aka Caryn Aline Demars, Defendant-Appellant, Petitioner on Review.	Jefferson County Circuit Court No. 09FE0092 CA A147290 SC S063197

BRIEF ON THE MERITS OF RESPONDENT ON REVIEW, STATE OF OREGON

Review of the Decision of the Court of Appeals
on Appeal from a Judgment
of the Circuit Court for Jefferson County
Honorable GEORGE W. NEILSON, Judge

Opinion Filed: February 4, 2015
Affirmed/Valid
Before: Armstrong, Presiding Judge, and
Nakamoto, Judge, and Egan, Judge

Continued…

ERNEST LANNET #013248
Chief Defender
Office of Public Defense Services
DANIEL C. BENNETT #073304
Deputy Public Defender
1175 Court St. NE
Salem, Oregon 97301
Telephone: (503) 378-3349
Email: dan.bennett@opds.state.or.us

Attorneys for Petitioner on Review

J. ASHLEE ALBIES #051846
Creighton & Rose PC
815 SW 2nd Ave, Ste 500
Portland, OR 97204
Telephone: (503) 221-1792
Email: ashlee@civilrightspdx.com

Attorney for *Amicus Curiae*

JAMIE L. WILLIAMS, Esq.
CA Bar No. 250087
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Attorney for *Amicus Curiae*

ELLEN F. ROSENBLUM #753239
Attorney General
PAUL L. SMITH #001870
Deputy Solicitor General
PATRICK M. EBBETT #970513
Senior Assistant Attorney General
1162 Court St. NE
Salem, Oregon 97301-4096
Telephone: (503) 378-4402
Email:
patrick.m.ebbett@doj.state.or.us

Attorneys for Respondent on Review

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases Cited

Constitutional & Statutory Provisions

Other Authorities

BRIEF ON THE MERITS OF RESPONDENT ON REVIEW, STATE OF OREGON

INTRODUCTION

This case concerns the proper interpretation of ORS 164.377(4), Oregon's computer crime statute. That statute imposes criminal liability on a person who "knowingly and without authorization uses, accesses, or attempts to access," among other things, a computer or computer system. This case requires the court to decide whether the state's evidence entitled the jury to find that defendant used or accessed her employer's Oregon Lottery terminal "without authorization" under the computer crime statute. As explained below, the state's evidence permitted the jury to conclude that defendant accessed her employer's lottery terminal outside the narrow circumstances in which her employer allowed her to do so, and thus accessed the computer "without authorization" under ORS 164.377(4).

QUESTION PRESENTED AND PROPOSED RULE OF LAW

Question Presented

Under ORS 164.377(4), a person commits a computer crime when, "without authorization" she uses, accesses, or attempts to access a computer or computer system. Does an employee access a computer "without authorization" when she is permitted to physically access the computer in a

particular circumstance, but accesses the computer when that circumstance does not exist?

Proposed Rule of Law

Yes. When an employee accesses her employer's computer outside the circumstances in which she is permitted to, she accesses the computer "without authorization," and thereby violates ORS 166.377(4).

SUMMARY OF ARGUMENT

ORS 164.377(4) provides that "[a]ny person who knowingly and without authorization uses, accesses, or attempts to access any computer, computer system, [or] computer network, * * * commits computer crime." Defendant violated that statute when she knowingly accessed her employer's lottery terminal on an occasion when she did not have permission to access it.

As the plain meaning of "without authorization" reflects, ORS 164.337(4) prohibits a person from accessing a computer any time that she accesses it outside the circumstances in which she is permitted to do so. Defendant asks this court to construe the term "authorization" in an all-or-nothing fashion: if a person is authorized to access a computer under any circumstances, she necessarily has authority to access the computer under all circumstances, and any restrictions on that authorization are "manner-of-use" restrictions outside the scope of ORS 164.377(4)'s prohibition. But that interpretation is unsupported by both the plain text and the broader statutory

context in which the term appears—specifically, the criminal trespass statutes. Although the legislature's primary motive in enacting the computer crime statute was to criminalize unauthorized remote access of computers, it chose broader language that applies to a wider range of conduct. Given that language, this court should hold that the phrase "without authorization," as used in ORS 164.377(4), encompasses a person's access of a computer outside the circumstances in which she is permitted to do so.

Here, defendant's employer conditionally authorized her to access the lottery terminal only in particular, limited circumstances—circumstances that did not exist when she accessed the terminal. Because the evidence permitted a rational trier of fact to conclude that defendant accessed her employer's computer outside the narrow circumstances in which she was permitted to, this court should affirm the trial court's denial of defendant's motion for judgment of acquittal.

STATEMENT OF MATERIAL FACTS

Defendant worked as a clerk behind the deli counter at a convenience store. (Tr 75-76). The store had a lottery terminal that printed out lottery tickets through a connection to the Oregon Lottery network. (Tr 77-78). The vice-president of the company that owned the store testified that defendant did not have authority to print lottery tickets. (Tr 105-06). The store manager testified, however, that while lottery sales were not generally part of a deli

worker's job, she trained defendant how to use the terminal so that she could sell and validate tickets for customers when the cashiers were busy or taking a break. (Tr 188, 195). The prosecutor conceded in response to defendant's motion for judgment of acquittal that defendant had some authority to operate the terminal to sell tickets. (Tr 291).

About a year after defendant was hired, the store manager discovered large shortfalls in cash receipts for sales of lottery tickets. (Tr 93-99, 184). An investigation revealed that large shortfalls and high lottery wagers occurred only during defendant's shifts. (Tr 87, 93). The store's surveillance video showed that when no customers or other employees were present, defendant would leave her work station behind the deli counter, access the lottery machine, and print lottery tickets without paying for them. (Tr 90; Ex 7). Upon discovering defendant's actions, the vice-president confronted defendant and immediately fired her. (Tr 104). The vice-president contacted police, and the ensuing investigation revealed that the store had suffered approximately $10,000 in losses based on defendant's thefts. (Tr 103, 164-65).

A grand jury indicted defendant with aggravated first-degree theft and computer crime. At trial, defendant moved for a judgment of acquittal on the computer crime charge, arguing that the state introduced insufficient evidence that defendant committed computer crime because "we do know she had authority to access the machines." (Tr 291-92). The trial court denied the

motion. (Tr 292). The jury later found defendant guilty of both aggravated first-degree theft and computer crime. (Tr 349-50).

On appeal, defendant challenged the denial of her acquittal motion. Defendant reasoned that because her employer gave her authorization to access the lottery terminal, she could not be guilty of using or accessing the computer "without authorization." (App Br 12). The Court of Appeals affirmed. *State v. Nascimento*, 268 Or App 718, 722, 343 P3d 654, *rev allowed*, 357 Or 324 (2015). It concluded that the evidence showed that defendant did not have authorization to access the lottery terminal when she did. *Id.* In particular, the court determined that the evidence was sufficient to show that the store manager gave defendant limited authorization to physically access the terminal only when a customer wanted to buy or validate a ticket and the cashier was unavailable—and that, when she accessed the terminal outside that circumstance, she acted "without authorization." *Id.* at 72.

ARGUMENT

ORS 164.377(4) protects owners of computers, computer systems, and computer networks from the unauthorized access of their computers and information they contain. It provides:

> 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.

ORS 164.377(4).

Applying the standard principles of statutory construction, accessing a computer outside the limited circumstances in which a person is permitted to constitutes accessing the computer "without authorization," and violates ORS 163.377(4). Defendant's interpretation of those words—that they only prohibit use of a computer that is *always* off-limits to the defendant (Pet BOM 15)—is not consistent with the text, context, or legislative history of the computer crime statute. Here, viewed most favorably to the state, the evidence established that defendant had permission to access the lottery terminal only in a single circumstance: when (1) the cashier was busy or away and (2) a customer wanted to buy or validate a lottery ticket. Because defendant accessed the terminal when no customer needed to be served, she accessed the terminal "without authorization."

A. ORS 164.377(4) prohibits accessing a computer outside the scope of a person permission to access it.

When interpreting a statute, this court applies the methodology set forth in *State v. Gaines*, 346 Or 160, 206 P3d 1042 (2009). In so doing, this court looks first to the statute's text, context, and legislative history, and then, if necessary, resorts to general maxims of statutory construction. *Id.* at 172. The "paramount goal" of statutory interpretation is to determine the legislature's intent. *Id.* at 171. And "there is no more persuasive evidence of the intent of

the legislature than the words by which the legislature undertook to give expression to its wishes. * * * Only the text of the statute receives the consideration and approval of a majority of the members of the legislature, as required to have the effect of law." *Id.* As explained below, applying that methodology here reveals that ORS 164.377(4)'s prohibition on accessing a computer "without authorization" applies when an employee accesses an employer's computer outside the circumstances in which she is permitted to do so.

1. The plain meaning of "without authorization" includes accessing a computer outside the scope of a person's permission to do so.

The legislature did not define the term "without authorization." When a term is undefined, this court "ordinarily look[s] to the plain meaning of the statute's text." *State v. Dickerson*, 356 Or 822, 829, 345 P3d 447 (2015). The ordinary meaning of a statutory term can be determined by reference to its dictionary definition. *Jenkins v. Board of Parole*, 356 Or 186, 194, 335 P3d 828 (2014) ("Because the legislature has not expressly defined the words in the disputed phrase, dictionary definitions of the words * * * can be useful.").

Here, the ordinary meaning of ORS 164.477(4)'s key phrase—"without authorization"—is plain and unambiguous. When the 1985 legislature enacted ORS 164.377(4), the term "authorize" meant—as it does today—"to endorse, empower, justify, or permit by or as by some recognized or proper authority (as

custom, evidence, personal right, or regulating power)." *Webster's Third New Int'l Dictionary* 146 (unabridged ed 1981). To the extent "authorization" may be considered a legal term, legal dictionaries in existence at the time similarly defined "authorize" as "[t]o empower; to give a right or authority to act * * * [t]o permit a thing to be done in the future." *Black's Law Dictionary* 122 (5th ed 1979); *see Dickerson*, 356 Or at 829-30 (legal dictionaries in existence at the time of the statute's enactment are useful for determining the meaning of undefined legal terms).

In other words, "authorization" is permission. Nothing in the plain meaning of "authorization" implies that authorization is an all-or-nothing concept, or that a person who gives authorization cannot limit the authorization to particular circumstances. It follows, therefore, that when a computer owner permits a person to access a computer only under certain circumstances, the person does not have authorization for ORS 164.377(4)'s purposes to access it on other occasions.

2. Statutory context in trespass law reinforces the plain meaning of "without authorization."

This court has emphasized that the words of a statute must be read in "the context of the statutory provision at issue, which includes other provisions of the same statute and other related statutes." *PGE v. Bureau of Labor and Industries*, 317 Or 606, 611, 859 P2d 1143 (1993). Related provisions of

ORS chapter 164 support the conclusion that ORS 164.377(4)—in prohibiting use of a computer "without authorization"—prohibits any access to a computer outside the circumstances in which a person is permitted to access it.

ORS 164.377(4) does not exist in a vacuum. It appears in ORS chapter 164, which generally defines criminal "offenses against property," including criminal trespass and computer crime. ORS 164.015 *et seq*. The text of ORS 164.377(4) models criminal trespass law that existed prior to its enactment. The second-degree criminal trespass statute—enacted in 1971—prohibits entering unlawfully "upon premises." ORS 164.245; Or Laws 1971 ch 743, § 139.[1] Entering "unlawfully" means, among other things, entering premises when "at the time of such entry" the person "is not otherwise licensed or privileged to do so." ORS 164.205(3)(a). Similarly, ORS 164.377(4) prohibits accessing a computer "without authorization." Just as a person may not access property without permission, a person may not access a computer without permission. That resemblance is no coincidence. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 NYU L Rev 1596, 1617 (2003) ("the available evidence suggests that legislators mostly saw [unauthorized access computer crime

[1] ORS 164.245 provides that "[a] person commits the crime of criminal trespass in the second degree if the person enters or remains unlawfully in a motor vehicle or in or upon premises." ORS 164.245(1).

statutes] as doing for computers what trespass and burglary laws did for real property").

Under trespass law, a property owner can provide a limited "license"—or, put differently, limited "authorization"—to access premises. If a person who possesses a limited license enters the premises outside the parameters of that license, the person commits criminal trespass. That basic principle is illustrated in *State v. Evans*, 267 Or App 762, 341 P3d 833(2014). There, the defendant asked the victim if he could use her bathroom and the victim consented, but defendant also entered the victim's bedroom, where he stole her purse. 267 Or App at 763-64. The defendant was convicted of burglary which, like criminal trespass, includes the element of "enter[ing] or remain[ing] unlawfully" but also the additional element that the person does so "with intent to commit a crime therein." ORS 164.215. The conviction was proper because there was an "express limitation on the license or privilege afforded defendant," which he violated because he "had no license or privilege to wander elsewhere in the victim's home." *Evans*, 267 Or App at 766-67. *See also State v. Holte*, 170 Or App 377, 382, 12 P3d 553 (2000) (burglary defendant's right to be in victim's house was limited to exclude entry into victim's bedroom). In the same way, a computer owner can provide limited "authorization" to access a computer.

Simply put, in chapter 164 the legislature recognized that property owners may limit access to certain areas of property and may limit access to certain times. If, for example, a property owner offers a limited license for entry by posting a sign saying "premises open to the public between the hours of 8:00 a.m. and 5:00 p.m.," and a member of the public enters the property at 8:00 p.m., the person commits criminal trespass because "at the time of such entry" the person did not have a "license or privilege" to do so. Likewise, by analogy, a person commits computer crime when a computer owner permits the person to access the owner's computer only on certain occasions, if the person nonetheless accesses the computer on other occasions. Thus, the context of ORS 164.377(4) reflects that the legislature intended to criminalize any unauthorized access of a computer.

Defendant concedes that ORS 164.377(4) embodies criminal trespass principles. (Pet BOM 18-19). But she ignores the pertinent analogies between trespass law and ORS 164.377(4). Instead, defendant mistakenly compares her actions to those of a person who has permission to be in a building but does "something improper within." (Pet BOM 18). To apply the trespass analogy, at the time defendant accessed the terminal, she did not have permission to be in the "building," regardless of whether she "did something improper within." That is, defendant did not have permission to access the lottery terminal at all at the time she did "something improper."

That analogy also explains why *amicus* is wrong when it insists a person only accesses a computer "without authorization" when the person circumvents a "technological access barrier." (Amicus Br at 7). Nothing in the text of ORS 164.377(4) or the trespass law in which it is rooted suggests that a person must circumvent some sort of barrier, technological or otherwise, to trespass either on premises or a computer. Insisting that a person does not access a computer "without authorization" unless he or she breaches a technological access barrier is akin to arguing that the law of trespass protects only landowners who put fences around their property. That is not the law. If the legislature wished to limit the scope of the statute to those who defeat a technological access barrier, it could have said that. This court may not "insert what has been omitted" from ORS 164.377(4). *See* ORS 174.010 (so stating).

In a nutshell, read in the context of the other trespass provisions of chapter 164, the phrase "without authorization" in ORS 164.377(4) encompasses accessing a computer on an occasion when the person is not permitted to access it. Such an action is analogous to a criminal trespass—it is, in effect, a "computer trespass." Accordingly, the text of ORS 164.377(4), read in context, reflects the legislature's intent: a person violates ORS 164.377(4) when the person accesses a computer on an occasion when the person is not permitted to do so.

3. Nothing in the legislative history of ORS 164.377(4) requires a different conclusion.

The legislature chose a broad solution to a specific problem when it enacted ORS 164.377 in 1985. A key motivation behind ORS 164.377 was to criminalize unauthorized remote access to computers. *See, e.g.*, Tape 576 at 20, House Committee on Judiciary, Subcommittee 1, May 6, 1985 (witness describing bill as addressing "the problem of computer crime, or computer hackers if you will"). Nonetheless, the text that the 1985 legislature ultimately adopted is not so limited. It prohibits "access" that is "without authorization." Although the legislature could have adopted text that criminalized unauthorized *remote* access exclusively, it did not. The legislature's choice of words controls the statutory interpretation.

Generally, "[a] court shall give the weight to the legislative history that the court considers to be appropriate." ORS 174.020(3). But "legislative history cannot substitute for, or contradict the text of, [a] statute." *White v. Jubitz Corp*., 347 Or 212, 223, 219 P3d 566 (2009). In other words, "[w]hen the text of a statute is truly capable of having only one meaning, no weight can be given to legislative history that suggests—or even confirms—that legislators intended something different." *Gaines*, 346 Or at 173.

Here, the legislature's adoption of a broadly worded prohibition on any "access" that is "without authorization" is significant. *See, e.g.*, *Hamilton v.*

Paynter, 342 Or 48, 55, 149 P3d 131 (2006) ("[T]he statutory text shows that, even if the legislature had a particular problem in mind, it chose to use a broader solution[.]"); *South Beach Marina, Inc. v. Dept. of Rev.*, 301 Or 524, 531, 724 P2d 788 (1986) ("Statutes ordinarily are drafted in order to address some known or identifiable problem, but the chosen solution may not always be narrowly confined to the precise problem. The legislature may and often does choose broader language that applies to a wider range of circumstances than the precise problem that triggered legislative attention."). Although the legislature was motivated by a desire to criminalize unauthorized remote access to computers, it chose wording that criminalized a broader range of conduct.

Moreover, nothing in the legislative history contains any statements indicating that the legislature intended Oregon courts, in construing the text at issue, to apply something other than the ordinary meaning of "access" or "without authorization." *See State v. Walker*, 356 Or 4, 333 P3d 316 (2015) (although legislature was concerned primarily with large-scale organized crime when it enacted organized crime statute, language was broad enough to include small-scale organized criminal activity, including shoplifting).

In light of the legislature's ultimate choice of words, its identification of a particular problem—unauthorized remote access of computers—does not mean that the statute must be read to exclude its application in areas outside that concern. The statutory text controls, regardless of any statement made by an

individual at the time the legislature considered passage of the statute. Here, that text prohibits any access of a computer that is unauthorized.[2]

4. The constitutional avoidance canon does not aid defendant.

Defendant also relies on the canon of construction that statutes should be interpreted to avoid constitutional problems. But because the text and context are clear and unambiguous, this court need not resort to such a canon of construction. In any event, defendant's constitutional objection is unfounded.

---

[2] Defendant relies on a pair of Ninth Circuit cases in support of her argument, both of which interpret the federal Computer Fraud and Abuse Act (CFAA), *United States v. Nosal*, 676 F3d 854 (9th Cir 2012), and *LVRC Holdings v. Brekka*, 581 F3d 1127 (9th Cir 2009). But nothing in the legislative history of ORS 164.377(4) suggests that it was modeled on the CFAA. To the contrary, during hearings on the legislation, Representative Springer asked a witness whether any federal law addressed computer crime, and the witness responded, "To my knowledge there's been no federal statute passed." Tape 576 at 298, House Committee on Judiciary, Subcommittee 1, May 6, 1985.

In any event, those cases do not conflict with the state's interpretation of ORS 164.377(4). Those cases concerned whether employees violated the CFAA by misusing computerized data they were *authorized* to access on company computers. *Nosal*, 676 F3d at 856; *Brekka*, 580 F3d at 1130. Under those circumstances—which were unlike the facts here, where defendant was only permitted to access her employer's computer in a single limited circumstance—the Ninth Circuit held that violations of internal policies or duties of loyalty regarding the use of company data did not run afoul of the CFAA. *Nosal*, 676 F3d at 863; *Brekka*, 580 F3d at 1133-35. Here, as the Court of Appeals recognized, defendant's liability was based on her lack of authorization to access the terminal, not the manner in which she used it: "This is not a case where defendant had general authorization to be on a computer to carry out her duties, but then used the computer in a manner that violated company policy[.]" *Nascimento*, 268 Or App at 722.

Under the constitutional avoidance canon, "in choosing between alternative interpretations of an ambiguous statute, this court must choose the interpretation which will avoid any serious constitutional difficulty." *State v. Duggan*, 290 Or 369, 373, 624 P2d 572 (1981). Defendant contends that an interpretation of the statute that would encompass her conduct in this case would implicate constitutional vagueness concerns. (Pet BOM 30-34). For the reasons explained below, she is incorrect.

As defendant notes, under Article 1, sections 20 and 21 of the Oregon Constitution, "[a] criminal statute must be sufficiently explicit to inform those who are subject to it of what conduct on their part will render them liable to its penalties." *State v. Graves*, 299 Or 189, 195, 700 P2d 244 (1985). The federal Due Process Clause requires that a criminal statute be sufficiently clear to give "the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly." *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 US 489, 498, 102 S Ct 1186, 71 L Ed 2d 362 (1982). Here, the ordinary meaning of the phrase "without authorization uses, accesses, or attempts to access any computer" unambiguously encompasses accessing a computer on an occasion when a person does not have permission to access it.

Furthermore, a *mens rea* requirement in a criminal statute "may mitigate a law's vagueness, especially with respect to the adequacy of notice to the

complainant that his conduct is proscribed." *Village of Hoffman Estates*, 455 US at 499. ORS 164.377(4) contains a *mens rea* requirement: a person must "knowingly" violate a use or access restriction. *See* ORS 161.085(8) (a person acts "knowingly" when the person "acts with awareness that the conduct of the person is of a nature so described or that a circumstance so described exists").

Moreover, the computer crime statute is sufficiently definite. As discussed above, it in many ways mirrors the criminal trespass statute. "Unauthorized" access of a computer is no more indefinite than the prohibition on entering premises when "not otherwise licensed or privileged to do so." ORS 164.205(3)(a). Juries—and at the judgment of acquittal stage, judges—are regularly called upon to make such determinations.

Defendant does not confront those reasons for why the statute is not vague. Instead, defendant contends that employees who play solitaire, send emails to family, or otherwise violate their employers' computer use policies will be subject to prosecution. (Pet BOM 26-27, 31-32). Accordingly, she asserts that an interpretation contrary to her own "would make it a crime to take any action on a computer that has not been expressly authorized by the computer's owner." (Pet BOM 31). In defendant's view, that would render the statute insufficiently explicit to inform potential violators of what conduct would violate the statute, implicating "significant constitutional vagueness concerns." (Pet BOM 30-34).

But defendant's vagueness argument confuses the restriction on access in this case as a restriction on the manner in which she used the terminal after she accessed it. She argues that the statute "targets people who *do not have authority* to use a computer, but it does not regulate the manner in which such people may actually use the computer." (Pet BOM 15; emphasis in original). In defendant's view, because she "was authorized to use the lottery computer * * * and expected to do as part of her work duties," she did not violate the statute because it "does not speak to the *manner* of use." (Pet BOM 15; emphasis in original). Defendant is mistaken.

This is not a case in which defendant had unfettered access to the lottery terminal in the course of using it for her work duties, and also used it for other purposes in violation of company policy. Rather, her employer gave her *limited* authorization to access the terminal. This case therefore does not implicate defendant's concerns that ORS 164.377(4) could criminalize all manner of computer use policies.

In short, the text, context, and legislative history of ORS 164.377(4) together reflect that a person accesses a computer "without authorization" whenever the person accesses a computer outside the limited circumstances in which she is permitted to access it.

B. The state introduced sufficient evidence that defendant was not authorized to access the lottery terminal when she did.

In reviewing a trial court's denial of a motion for a judgment of acquittal, this court "considers whether any rational trier of fact, accepting reasonable inferences and making reasonable credibility choices, could have found the essential elements of the crime beyond a reasonable doubt." *State v. Lupoli*, 348 Or 346, 366, 234 P3d 117 (2010). In doing so, this court "reviews the facts in the light most favorable to the state and draws all reasonable inferences in the state's favor." *Id.*

To prove that defendant accessed a computer "without authorization," the state had to prove that defendant was not permitted to access the lottery terminal when she did so. Viewed most favorably to the state, the evidence entitled a rational trier of fact to conclude beyond a reasonable doubt that the stated proved all of the elements of a computer crime under ORS 164.377(4). *See State v. Cunningham*, 320 Or 47, 63, 880 P2d 431 (1994), *cert den*, 514 US 1005 (1995) (in reviewing denial of motion for judgment of acquittal, the evidence is viewed in the light most favorable to the state). The state presented evidence that defendant was permitted to access the terminal only to serve lottery customers when the cashier was busy or away. (Tr 91, 105-06, 188, 195). The state also introduced testimony and video evidence that defendant nonetheless accessed the terminal on occasions when there were no lottery

customers to serve. (Tr 90; Ex 7). The jury could therefore reasonably find that defendant was permitted to access the terminal only when the cashier was unavailable and a customer wanted to buy or validate a ticket, and further find that defendant violated that limitation.[3]

In arguing to the contrary, defendant essentially contends that because she was authorized to access the lottery terminal in certain limited circumstances, she also had authorization to access it whenever she pleased. That proposition ignores the plain meaning of "without authorization." When defendant accessed the terminal outside the single circumstance in which she was allowed to, she was no more entitled to access the terminal than an employee who was prohibited from accessing the terminal at all. By accessing the terminal when she did not have permission to—regardless of her particular manner of using the terminal after she accessed it—defendant violated ORS 164.377(4).

---

[3] Alternatively, viewing the evidence most favorably to the state, defendant was not authorized to access the lottery terminal at all. The vice-president of the company that owned the store testified that defendant did not have authority to print lottery tickets. (Tr 105-06). That testimony, viewed most favorably to the state, provides an independent basis to affirm the denial of defendant's motion for judgment of acquittal. To be sure, the prosecutor conceded in response to defendant's motion for judgment of acquittal that defendant had some authority to operate the terminal to sell tickets. (Tr 291). But that concession cannot dictate whether the evidence presented suffices—as a matter of law—to permit a jury to convict.

In sum, viewed most favorably the state, the evidence showed that defendant was only permitted to access the lottery terminal when a customer needed to buy or validate a ticket and a cashier was unavailable. The evidence also showed that defendant accessed the terminal outside that narrow circumstance. The trial court correctly denied defendant's motion for judgment of acquittal.

CONCLUSION

This court should affirm the decision of the Court of Appeals and the trial court's judgment of conviction.

Respectfully submitted,

ELLEN F. ROSENBLUM
Attorney General
PAUL L. SMITH
Deputy Solicitor General

/s/ Patrick M. Ebbett

PATRICK M. EBBETT #970513
Senior Assistant Attorney General
patrick.m.ebbett@doj.state.or.us

Attorneys for Plaintiff-Respondent
State of Oregon

PME:bmg/6839049

NOTICE OF FILING AND PROOF OF SERVICE

I certify that on October 8, 2015, I directed the original Brief on the Merits of Respondent on Review, State of Oregon to be electronically filed with the Appellate Court Administrator, Appellate Records Section, and electronically served upon Ernest Lannet and Daniel C. Bennett, attorneys for appellant, and J. Ashlee Albies, attorney for amicus curiae, by using the court's electronic filing system.

I further certify that on October 8, 2015, I directed the Brief on the Merits of Respondent on Review, State of Oregon to be served upon Jamie L. Williams, attorney for amicus curiae, by sending two copies, with postage prepaid, in an envelope addressed to:

Jamie L. Williams, Esq.
CA Bar No. 250087
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

/ / / / /

/ / / / /

/ / / / /

/ / / / /

/ / / / /

/ / / / /

/ / / / /

CERTIFICATE OF COMPLIANCE WITH ORAP 5.05(2)(d)

I certify that (1) this brief complies with the word-count limitation in ORAP 5.05(2)(b) and (2) the word-count of this brief (as described in ORAP 5.05(2)(a)) is 4,821 words. I further certify that the size of the type in this brief is not smaller than 14 point for both the text of the brief and footnotes as required by ORAP 5.05(2)(b).

/s/ Patrick M. Ebbett

PATRICK M. EBBETT #970513
Senior Assistant Attorney General
patrick.m.ebbett@doj.state.or.us

Attorney for Plaintiff-Respondent

PME:bmg/6839049