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 Case No. 09FE0092 CA A147290 S063197

BRIEF ON THE MERITS OF PETITIONER ON REVIEW

Review the decision of the Court of Appeals
on an appeal from a judgment of the Circuit Court
for Jefferson County
Honorable George W. Neilson, Judge

Opinion Filed: February 4, 2015
Author of Opinion: Armstrong, P.J.,
Before: Armstrong, Presiding Judge, and Nakamoto, Judge, and Egan, Judge

ERNEST G. LANNET #013248
Chief Defender
Criminal Appellate Section
DANIEL C. BENNETT #073304
Senior Deputy Public Defender
Office of Public Defense Services
1175 Court Street NE
Salem, OR 97301
Dan.Bennett@opds.state.or.us
Phone: (503) 378-3349
Attorneys for Petitioner on Review

ELLEN F. ROSENBLUM #753239
Attorney General
ANNA JOYCE #013112
Solicitor General
PATRICK M. EBBETT #970513
Assistant Attorney General
400 Justice Building
1162 Court Street NE
Salem, OR 97301
patrick.m.ebbett@doj.state.or.us
Phone: (503) 378-4402
Attorneys for Respondent on Review

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases Cited

Statutory Provisions

Others

PETITIONER'S BRIEF ON THE MERITS

INTRODUCTION

This case presents an issue of statutory interpretation. The question is whether ORS 164.377(4)[1] makes it a crime for person to use a computer in a manner for which she has not received specific permission.

QUESTION PRESENTED AND PROPOSED RULE OF LAW

Question Presented

When a person authorizes another to use a computer for a certain purpose, does the latter person commit computer crime, ORS 164.377(4), by using the computer for a different purpose?

Proposed Rule of Law

By making it a criminal offense to use a computer without authorization, the 1985 legislature intended ORS 164.377(4) to criminalize hacking into a computer which a person has no right to access. When a person has permission

[1] During the pendency of this appeal, the Oregon Legislature amended ORS 164.377 to include "theft of an intimate image" within subsection (2), as well as certain definitions relevant to that addition. Or Laws 2015, ch 350, § 1. That amendment is not at issue in this case. Unless specifically noted otherwise, defendant refers throughout this brief to the 2001 version of the statute, which was in effect at the time this case arose.

to use a computer system she is authorized to use that computer, even if she uses the computer for an impermissible purpose. ORS 164.377(4) addresses the right to use or access a computer, not the manner of use.

SUMMARY OF ARGUMENT

ORS 164.377(4) applies to computer hacking. It does not govern the manner in which a person uses a computer.

This case involves a question of statutory interpretation, requiring this court to determine when someone is a "person who knowingly and without authorization uses, accesses or attempts to access any computer." By its plain text, that statute targets a class of people, those who lack authorization to access or use computers. It does not concern itself with the *manner* in which a person uses a computer. If a person is authorized to use or access a computer he or she may do so. If that person takes some action on the computer against the wishes of its owner it is a private matter, not a crime.

The context of the statute supports defendant's interpretation. The legislature *did* choose to make crimes out of certain actions a person can take on a computer. If a person uses a computer to defraud or steal, or if a person damages, alters, or destroys another person's data without permission, he or she violates different provisions of ORS 164.377. Those are the provisions under which the legislature chose to regulate the *manner* of use of a computer. ORS

164.377 regulates *access* to a computer. Defendant had the right to access the computer here.

Were there any ambiguity in the statute, the legislative history would resolve it in defendant's favor. ORS 164.377 was enacted in 1985 at the request of executives of telecommunications companies who made clear what their concern was: the novel threat of hackers unlawfully gaining access to computer systems. The discussion of the bill is replete with stories of hackers "dialing in" to computers illicitly and stealing or tampering with information. Witnesses made clear that the purpose of the bill was not to target people who used computer systems to which they had access.

Were this court to hold that a person violates ORS 164.377 whenever she takes some action on a computer contrary to the wishes of its owner, the statute would be unconstitutionally vague. It is the province of the legislature to define criminal laws. It may not, and clearly did not intend to, give every private computer use or access policy the force of criminal law. Instead, it intended to make it a crime for a person to access, to hack into, or to "dial" up on to a computer system when the owner did not grant that person permission. Defendant had permission to use the computer in this case, so she did not use or access it "without authorization."

SUMMARY OF HISTORICAL AND PROCEDURAL FACTS

The Court of Appeals summarized the historical facts in its opinion. Defendant provides that summary below, as augmented by a few additional, pertinent facts:

> "In October 2007, defendant was hired to work at the deli counter in a convenience store[, Tiger Mart]. The store had a touch-screen lottery terminal that produced draw-game tickets and was connected by phone line to the Oregon Lottery network. From the terminal, a clerk could print out a ticket for a selected game, and also could print ticket-sales reports. The store manager[, Donnely,] trained defendant on the use of the lottery terminal and authorized defendant to sell lottery tickets to, and validate tickets for customers, because deli clerks would assist at the counter when the counter employee was busy or on break, even though it was not their job. The general manager testified, however, that operating the lottery terminal and cash register was not part of defendant's job description as a deli clerk and that defendant did not have authorization to use the terminal. Store policy prohibited employees from purchasing lottery tickets or validating their own lottery tickets while on duty.

State v. Nascimento, 268 Or App 718, 719, 343 P3d 654 (2015).

Ryell Masood, a vice president of the corporation that owns Tiger Mart, testified that defendant did not have authorization to use the lottery machine. Tr. 105-06. However, he also explained that he was not involved in the daily operation of the store. Tr. 76. He was also not aware that defendant had been trained to use the machine by Donnelly. Tr. 117. Donnelly, defendant's direct supervisor, explained that defendant was authorized to sell lottery tickets. Tr. 195. Donnelly believed that she had personally trained defendant on using the

lottery ticket machine. Tr. 195. She said that the "deli" employees usually assisted with selling lottery tickets or ringing up purchases on the cash register if the "counter" employee was busy. Tr. 188. She gave defendant explicit permission to use the lottery machine. Tr. 195. Thus, to the extent that Masood believed that defendant was not "authorized" to use the computer to sell lottery tickets, he was mistaken. The prosecutor acknowledged, in responding to defendant's motion for judgment of acquittal, that "she did have some apparent authority to operate the machine to sell tickets and to conduct business of Tiger Mart * * *." Tr. 291.

> "About a year after defendant was hired, the store manager fell a few months behind in reconciling daily lottery ticket sales with the store's cash receipts. In February 2009, she discovered shortfalls in cash receipts for lottery sales of Keno tickets between November 2008 and February 2009, which prompted the general manager to investigate his records and involve the police. The investigation uncovered that large shortfalls and high-dollar wagers on Keno occurred only during defendant's shifts. The store's surveillance video showed that, when no one was around, defendant would leave the deli counter and print out and pocket lottery tickets from the lottery terminal. One of the high-dollar winning tickets printed during defendant's shift was redeemed by her by mail, and others were redeemed by her at a local grocery store."

Nascimento, 268 Or App at 720.

The state charged defendant with one count of aggravated theft in the first degree and one count of computer crime under ORS 164.377(4), which 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."

Defendant moved for judgment of acquittal on the computer crime count, arguing that she "did not unlawfully and knowingly without authorization use and access a computer system operated by Tiger Mart store, that being the lottery machine" because she was authorized to use that machine. Tr. 281. The prosecutor argued that defendant's particular use of the machine was "unauthorized." Tr. 291.

The trial court denied defendant's motion, ruling, "I believe there's sufficient evidence in the record that a person can create a lot of different inferences and what you really are doing there is (indiscernible) of the evidence." Tr. 292.

In the Court of Appeals, defendant argued that she was authorized to use the lottery computer and was, therefore, not guilty of using or accessing a computer system "without authorization." App. Br. at 12. The Court of Appeals affirmed defendant's conviction. The court quoted the state's argument that "a jury could reasonably conclude that defendant's use of the lottery machine was 'without authorization' because 'she had no authorization to use the lottery computer to purchase a lottery ticket for herself during her work shift—much less to steal a lottery ticket by printing it and not paying for it.'" *Nascimento*,

268 Or App at 721. The court characterized defendant's framing of the issue as "whether ORS 164.377(4) encompasses conduct that (1) only involves a person accessing a device itself without authorization or (2) also encompasses using a device, which the person otherwise has authorization to physically access, in a manner contrary to company policy or against the employer's interests." *Id.* at 722. The court then declined to answer that question:

> "Under the circumstances of this case, however, we need not resolve that issue. There is evidence in the record that defendant's store manager gave defendant limited authorization to physically access the lottery terminal to only sell tickets to, and validate tickets for, paying customers and only when the counter employee was not available to do so. This is not the case that defendant tries to make it out to be. This is not a case where defendant had general authorization to be on a computer to carry out her duties, but then used that computer in a manner that violated company policy—such as, to use defendant's example, by playing solitaire during work hours. For defendant's duties, the lottery terminal had but one function: to sell and validate lottery tickets. There was evidence from which the jury could conclude that she was authorized to access the physical device itself—the lottery terminal—only to serve paying customers."

Id.

This court allowed review. 357 Or 324.

ARGUMENT

This question before this court here is whether ORS 164.377(4) is a computer trespass statute – one that governs who may use or access a computer – or whether it is a statute that targets the manner in which a person uses a

computer. If the statute is the latter, it criminalizes an almost limitless range of conduct. If it is the former, it is a more limited, if broad, protection against trespass onto a computer system. It would serve, in other words, to prevent "hacking" into computers without the permission of the owners or otherwise using a computer to which one has no right of access.

Defendant's proposed interpretation – that ORS 164.377(4) bars only computer trespass – is compelled by the text, context, and legislative history of that provision. Moreover, defendant's proposed interpretation would harmonize Oregon's computer crime statute with the Ninth Circuit's reasoned interpretation of the analogous federal Computer Fraud and Abuse Act, discussed below. Finally, defendant's proposed interpretation of ORS 164.377(4) prevents a problem that arises under the broader interpretation adopted by the trial court – if that section targets violations of computer-use policies, it allows private entities to enact criminal laws by writing them into computer-use or terms-of-use policies and is unconstitutionally vague.

I. Relevant Statutes

Defendant sets out the computer crime statute, ORS 164.377, in full at Appendix 1-3. The most pertinent portions of that statute provides:

> "(1) As used in this section:
>
> "(a) To 'access' means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network.

"(b) 'Computer' means, but is not limited to, an electronic, magnetic, optical electrochemical or other high-speed data processing device that performs logical, arithmetic or memory functions by the manipulations of electronic, magnetic or optical signals or impulses, and includes the components of a computer and all input, output, processing, storage, software or communication facilities that are connected or related to such a device in a system or network.

"* * * * *

"(f) 'Computer system' means, but is not limited to, a set of related, connected or unconnected, computer equipment, devices and software. 'Computer system' also includes any computer, device or software 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.

"* * * * *

"(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.

"(3) Any person who knowingly and without authorization alters, damages or destroys 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.

> "(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.
>
> "(5) * * *
>
> "(b) 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."

In her brief, defendant discusses the similar federal Computer Fraud and Abuse Act (CFAA), 18 USC § 1030.[2] Defendant sets out an extended excerpt of that statute at Appendix 4-6. The most pertinent portion of that statute provides that whoever:

> "(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
>
> "* * * * *
>
> "(C) information from any protected computer;
>
> "* * * * *
>
> "(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud

[2] The analogous provision to ORS 164.377(4), the provision under which defendant was convicted, is 18 USC §1030(2), while the prohibited uses provisions found in ORS 164.377(2) and (3) find their analogs in 18 USC §1030(4) and (5).

and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

"(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

"(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

"(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

"* * * * *

"shall be punished as provided in subsection (c) of this section.

"* * * * *

"(2) the term 'protected computer' means a computer--

"* * * * *

"(B) which is used in or affecting interstate or foreign commerce or communication * * *

"* * * * *

"(6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;"

II. The sole issue in this case is the interpretation of ORS 164.377(4).

As a preliminary matter, defendant notes that she was charged only under ORS 164.377(4), and no other subsection is at issue. Count 2 of the indictment, the computer crime allegation, reads, in full,

> "COUNT 2
>
> "The defendant, on or between November 11, 2008 to February 6, 2009, in Jefferson County, Oregon, did unlawfully, 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."

ER 1 (emphasis added).[3]

Additionally, there is no reasonable factual dispute as to whether defendant was, in fact, permitted to use the lottery computer in the course of her duties. Although, as defendant acknowledged in her opening brief and petition for review, the vice president of the corporation that owns the convenience store

[3]Although the caption of the indictment refers to ORS 164.377(2), the state did not include in the indictment any allegation that defendant used a computer, computer system, computer network for any of the purposes outlined in that subsection. That is, the state did not allege that defendant's use of the computer was for the purpose of devising or executing a scheme to defraud (subsection (2)(a)); obtaining money, property, or services under false pretenses (subsection (2)(b)); or by committing theft (subsection (2)(c)). The state is limited to proving a crime in the manner in which it is charged. *See State v. Schoen*, 348 Or 207, 213, 228 P3d 1207 (2010) (when a defendant is charged with criminal mischief in the third degree only under a theory that he "tampered" with property a reviewing court will not consider whether he "interfered" with property even though the statute covers that conduct).

that employed defendant testified that defendant's work duties did not include using the lottery terminal, uncontradicted testimony from defendant's immediate supervisor established that defendant was trained on and authorized to use the lottery terminal and did not describe any limitation on her right to physically access the machine.

III. The text, context, and legislative history of subsection (4) of Oregon's computer crime statute demonstrate that its purpose is to thwart computer trespass.

The question before this court is whom the legislature meant to target when it referred to "Any person who knowingly and without authorization uses, accesses or attempts to access any computer" in ORS 164.377(4). To answer that question this court must engage in statutory interpretation. The goal of statutory interpretation is to discern the legislature's intent. ORS 174.020; *PGE v. Bureau of Labor and Industries*, 317 Or 606, 610-12, 859 P2d 1143 (1993). To that end, this court analyzes the text in context and does not insert or omit words through its interpretation. ORS 174.010; *PGE*, 317 Or at 610-12. This court may consider legislative history when offered by a party, and the court gives such history the weight it deems appropriate. ORS 174.020(1)(b); *State v. Gaines*, 346 Or 160, 171-72, 206 P3d 1042 (2009).

A. The text and context of ORS 164.377(4) demonstrate that it was intended to bar computer hacking, not to control the manner in which a person uses a computer

Defendant was permitted to use the lottery computer in the course of her duties. Defendant does *not* contend that she was permitted to obtain lottery tickets for herself without paying for them. Thus, the question is whether defendant was a "person who knowingly and without authorization uses, accesses or attempts to access any computer," when she was authorized to use a particular computer but used the computer in an improper manner.

The starting point for statutory construction is the text of the statute, because it "is the best evidence of the legislature's intent." *PGE*, 317 Or at 610. Here, the legislature did not define the terms "authorization" or "without authorization" in the computer crime statute. When a term is not defined by statute, this court will assume that the legislature used the natural and ordinary meaning of the words in the statute, and will consult a dictionary to determine the meaning. *State v. Ausmus*, 336 Or 493, 504, 85 P3d 864 (2004).

"Authorization" is defined as "**1 :** the act of authorizing **:** the state of being authorized." *Webster's Third New Int'l Dictionary* 146 (unabridged ed 1993).

"Authorize" is defined as

> "**1 a :** to endorse, empower, justify, or permit as by some recognized or proper authority * * * : **2** *obs* **:** to vouch for **:** confirm the truth or reality of by alleging one's own or

> another's authority **3** *obs* **:** to give legality or effective force to (a power, instrument, order) **4 a :** to endow with authority or effective legal power, warrant, or right **:** appoint, empower, or warrant regularly, legally, or officially * * * ."

Id.

A reviewing court also considers the grammatical construction of a statute in construing its meaning. *See Martin v. City of Albany*, 320 Or 175, 181, 880 P2d 926, 930 (1994) (noting that court does "not lightly disregard the legislature's choice of verb tense, because we assume that the legislature's choice is purposeful"). Here, in ORS 164.377(4), the subject of the sentence is the "*person who* knowingly and without authorization uses, accesses or attempts to access any computer * * *." The statute targets a category of people: those who use, access, or attempt to access computers when lacking authorization. Someone who meets that description is the one who "commits computer crime." A person is either "authorized" to use or access a computer, or she is not. Nowhere does the statute speak of authority to take certain actions on a computer or use it in a certain manner. That is, 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. In other words, the statute does not provide that an authorized person may lose that authority by operation of law.

Here, defendant was a person who was authorized to use the lottery computer at the convenience store because she was given permission to do so by her direct supervisor, trained to do so by her supervisor, and expected to do so as a part of her work duties. That is, she was "permit[ed] by some recognized or proper authority * * *" to use the lottery computer.

Once authorized, defendant remained authorized to use the computer because her authorization was never withdrawn. To hold to the contrary, this court must hold that a person is only authorized to use a computer to do specifically those things allowed in a computer use-policy or via other explicit direction from the computer's owner. Or, in other words, that a person becomes "unauthorized" to use a computer, as a matter of law, by taking any unpermitted actions on the device. Under such an interpretation, if a houseguest asked a homeowner for permission to check his email on the home computer, but also checked a sports score on it, he would not be "authorized" to access the computer. There is no indication in the text of the computer crime statute that the legislature intended such a broad, sweeping effect. The legislature could have, for example, barred "using a computer in an unauthorized manner." It did not do so. ORS 164.377(4) distinguishes only between those who *are* and *are not* authorized to use or access a computer. It does not speak to the *manner* of use.

Additionally, the context of ORS 164.377 suggests that the legislature intended to bar computer trespass, not use violations, in subsection (4). ORS 164.377 contains three general ways in which a person may commit computer crime: ORS 164.377(2) targets using a computer[4] to which one has access to commit fraud or theft, including "theft of proprietary information or theft of an intimate image."[5] ORS 164.377(3) targets altering, damaging, or destroying a computer [6] without authorization. Finally, ORS 164.377(4) targets merely accessing, attempting to access, or using a computer[7] without authorization.

A violation of subsection (2) or (3) is a felony, whereas a violation of subsection (4) is generally a misdemeanor (unless, as here, the computer at issue is "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"). Thus, subsections (2) and (3) target specific misuses of a computer and are generally categorized as more serious offenses. By contrast, subsection (4) targets merely accessing, using, or

---

[4] Or "computer system, computer network or any part thereof."

[5] As defendant acknowledged in her opening brief, it is likely that a jury could have determined that her conduct violated ORS 164.377(2). The state did not charge her under that provision.

[6] Or "computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network."

[7] Or any of the other related items covered in subsection (3).

attempting to access a computer without authorization and is the least serious offense. The legislature has specifically delineated which *particular uses* of a computer fall under the ambit of the statute in subsections (2) and (3).

If ORS 164.377 targeted misuse of office buildings rather than computers, subsection (2) would apply to a person who ran a fraudulent scheme within or simply stole items from an office, subsection (3) would apply to a vandal who damaged the building without permission, and subsection (4) would apply to a trespasser. Defendant may have done something improper within, but she was allowed to be there.

A comparison of ORS 164.377(2) and (4) provides other contextual clues to support defendant's interpretation that subsection (4) is concerned with computer trespass. Subsection (2) applies whenever a person "accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof." Subsection (4), by contrast, applies when a person "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." Aside from subsection (2)'s requirement of additional malfeasance, two principal differences exist between these subsections. First, subsection (2) covers both attempted *use* and attempted *access*, whereas the "attempt" provision in subsection (4) covers only attempted *access*. That the legislature

used a term in "one section and not in another section of the same statute indicates a purposeful omission." *Jordan v. SAIF Corp.*, 343 Or 208, 217, 167 P3d 451, (2007) (quoting *PGE*, 317 Or at 611). Specifically, the omission of attempted use from subsection (4) indicates that the focus of that section was to prohibit *access* by certain parties, not to limit the manner of their use.

The second difference between the two provisions is the range of systems covered by subsection (4). Whereas subsection (2) covers any "computer, computer system, computer network or any part thereof," subsection (4) covers any "computer, computer system, computer network, *or any computer software, program, documentation or data contained in such computer*, computer system or computer network." (emphasis added). Again, the differences suggest that the latter subsection is intended to prevent unauthorized trespass – to enter computer systems or view other related materials without permission. The inclusion of data and documentation in the list of protected items denotes a focus on maintaining privacy and confidentiality, not misuse.

Most telling is the absence of any textual suggestion that the legislature intended to give privately-enacted computer-use policies the force of criminal law. When the legislature has made violation of a private party's directive a crime, it has done so explicitly. For example, a person commits criminal trespass in the second degree if he or she "enters or remains unlawfully in a motor vehicle or in or upon premises." ORS 164.245. He or she commits

criminal trespass in the first degree if he or she, *inter alia*, "[h]aving been denied future entry to a building pursuant to a merchants notice of trespass, reenters the building during hours when the building is open to the public with the intent to commit theft therein." ORS 164.255(1)(b). To enter or remain unlawfully includes, along with other conduct, "[t]o fail to leave premises that are open to the public after being lawfully directed to do so by the person in charge * * *[and t]o enter premises that are open to the public after being lawfully directed not to enter the premises." ORS 164.205(3). Thus, while a criminal trespass may be predicated on a person violating the private direction of a merchant or other person, the legislature made explicit that such culpability will attach. If the legislature had wished to criminalize the violation of a computer use policy, it could have done so explicitly.[8]

B. ORS 164.377 was enacted by the legislature to bar computer trespass. Its proponents did not contemplate it being used to penalize violation of a computer use policy.

If the text and context of ORS 164.377(4) left any doubt that its purpose was only to target computer hackers, the legislative history removes all doubt.

ORS 164.377 arose as an amendment to House Bill 2795 in 1985. The initial version of that bill dealt with a different then-cutting-edge issue: the theft of cable television services. *See* Bill File, HB 295, 1985. At the request of Dave

[8] As defendant discusses below, such a statute might be unconstitutional.

Overstreet of the General Telephone Company, the House Judiciary Committee adopted an amendment adding what is now ORS 164.377 to that bill. *Id.*

The House Judiciary Subcommittee 1 discussed Overstreet's amendment on May 6, 1985. By way of introduction, Overstreet described the purpose behind the amendment: "We are this evening proposing amendments to House Bill 2795 specifically to deal with the problem of computer crime, or computer hackers if you will." Tape 576 at 20, House Committee on Judiciary, Subcommittee 1, May 6, 1985.

Next, Sterling Gibson, of General Telephone's security department, described the problem as the industry saw it:

> "Most businesses are growing to the point where they all have, or if they don't have now they will soon have, a computer running the business to some degree. And what we're trying to get into the statute is a part of the law that will prevent people from *calling in to someone's computer*"

to manipulate the data and create havoc. *Id.* at 50.

Gibson made clear that the target of the bill was computer "hackers." He provided several examples of the sort of conduct about which he was concerned: "kids" who remotely accessed the computers of a Canadian business and inadvertently altered business documents, students who used their computers to automatically "scan" telephone exchanges for unsecured computer systems into which they could remotely dial, and "kids" who post long-distance

telephone "billing codes" on computer bulletin board systems,[9] referring to a recent incident in Seattle. *Id.* at 118-152.

Representative Kopetski expressed concern that the amendment, if enacted, would apply to a constituent of who was a computer hobbyist. Marion County District Attorney Dale Penn assured him that the law did not apply to people who are allowed to access computer systems,

> "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. at 340.

The Senate Judiciary Committee addressed HB 2795 on June 7, 1985. The audio recording of that hearing has been lost, but the printed minutes reveal that the bulk of the discussion related to the cable television components of the bill. However, Overstreet spoke in support of the computer crime provision. According to the minutes, "Sections 7 and 8 of the bill address computer hackers – persons who use computer to defraud. Computers can now be used to

---

[9] A computer bulletin board system, or "BBS," is an online message board to which one connected via a modem over a phone line, popular among computer enthusiasts before the advent of the web. Scott Gilbertson, *Feb. 16, 1978: Bulletin Board Goes Electronic*, Wired (February 16, 2010), available at http://www.wired.com/2010/02/0216cbbs-first-bbs-bulletin-board/ (accessed July 30, 2015).

talk to other computers." Tape 180 side A at 125, Senate Committee on Judiciary, June 7, 1985 (minutes at page 18).

Those hearings demonstrate that the bill was motivated to address concerns very different from those that animate this case – concerns about hacking into a computer which one was no right to access at all. To which one does not "know the codes." The image in the minds of the legislators was not of an employee misusing a work computer, it was of a computer hacker dialing in to remote computer systems and accessing them without consent of their owners.

As important as the affirmative references to computer "hackers" as the concern animating the bill is the complete omission of any suggestion that the legislature intended the bill to apply to people who have a right to access a computer. Indeed, the legislators seemed entirely focused on *remote* access, discussing hackers "calling" into computers. Nowhere did any party suggest that a person might be liable for misusing a computer which she has a legitimate way of accessing.

In construing the statute, this court should bear in mind the different time in which it was enacted. At the time of HB 2795's enactment, the computer landscape was dramatically different from today. That is made clear by Gibson's reference to "people that sell time-share." Tape 576 at 50, House Committee on Judiciary, Subcommittee 1, May 6, 1985. "Time sharing" was a

process by which various users could rent time on a mainframe computer before the personal computer was common and when computers were rare and expensive. *See*, *e.g.*, https://en.wikipedia.org/wiki/Time-sharing (accessed July 19, 2015). Companies formed to offer commercial time sharing for profit, with one source estimating that approximately 150 such companies were created in the latter half of the 1960s. *See* Computer History Museum: Timesharing as a Business, http://www.computerhistory.org/revolution/mainframe-computers/7/181 (accessed July 19, 2015). In 1984, one year before Gibson's testimony, only 8.2 percent of American homes contained personal computers. Thom File, *Computer and Internet Use in the United States*, U.S. Census Bureau, P20-569 (2013) (available at https://www.census.gov/prod/2013pubs/p20-569.pdf).

ORS 164.377 was enacted in a time when mere access to a computer was a rare and valuable commodity. The drafters were concerned about the financial loss a person could suffer either if someone damaged the contents of a computer or accessed it without authorization. There is no suggestion that the legislature intended to criminalize authorized users' violations of a use policy.

Nor were any subsequent amendments to the bill intended to target the manner in which a person uses a computer. In 1989, the legislature passed House Bill 2518 to expand and add several definitions and to specify that theft of "proprietary data" falls under subsection (2)(c) of the statute. Or Laws 1989,

ch 737, § 1. That bill was, again, targeted computer hackers. *See* Testimony, House Judiciary Committee, Crime Subcommittee, HB 2518, Feb 16, 1989, Exhibit G, "Testimony of Gary Willhelms, Director of Legislative Affairs, US West Communications" (noting that bill arose from desire to "strengthen the law by stiffening the penalties for computer hacking").[10]

IV. This court should consider the Ninth Circuit's interpretation of the analogous CFAA in *Nosal* and *Brekka*.

Although this court has not previously had the opportunity to consider Oregon's computer crime statute, it can take guidance from the Ninth Circuit's consideration of the federal CFAA, 18 USC § 1030, in *LVRC Holdings LLC v. Brekka*, 581 F3d 1127, 1132 (9th Cir 2009) and *United States v. Nosal*, 676 F3d 854, 856 (9th Cir 2012). In *Brekka*, a company sued a former employee, under provisions of the CFAA which require establishing that a person "intentionally accesses a computer without authorization or exceeds authorized access" and that a person "accesses a protected computer without authorization, or exceeds

[10] Additonally, in 1991 the Legislature passed House Bill 3151. That bill authorized the Oregon Lottery to offer video lottery games. *Wolf v. Oregon Lottery Comm'n*, 209 Or App 670, 679, 149 P3d 303 (2006), *rev'd*, 344 Or 345 (2008). There is no indication in the legislative history of that provision that the legislature intended to broaden computer crime. Rather, that amendment merely included lottery computers under the ambit of the statute. Or Laws 1991, ch 962, §17. Also, in 2001, the legislature expanded ORS 164.377(1)'s definition of "computer" as part of a broad bill addressing several topics. Or Laws 2001, ch 870, §18. There was no relevant discussion.

authorized access[.]" In construing the text of that statute, the Ninth Circuit held that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it. Because LVRC permitted Brekka to use the company computer, the 'ordinary, contemporary, common meaning' * * * of the statute suggests that Brekka did not act 'without authorization.'" *Brekka*, 581 F3d at 1133 (citation omitted).

U.S. v. Nosal involves the question of whether a person who uses a computer for a purpose not permitted by his employer in a use policy has violated the provisions of the CFAA that bar either unauthorized computer access or access that "exceeds" authorization. The majority in that *en banc* decision noted that the government agreed that accessing a computer "without authorization" under the CFAA referred only to "hacking" into a computer without any authorization to use it. 676 F3d at 858. The court went farther and also held that the phrase "exceeds authorized access" on a computer *also* only applies to "hacking" and *not* to violating employer use restrictions. *Id.* at 863. In reaching its conclusion, the majority emphasized some of the dangers of "basing criminal liability on violations of private computer use policies":

> "Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the New York Times to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give

> them more than enough time to hone their sudoku skills behind bars."

Id. at 860.

In Oregon, however, even employees who place phone calls to family members may violate ORS 164.377(4) if doing so is against a company policy. That is so because, under the broad definition of computer in ORS 164.377(1)(b), which includes "an electronic, magnetic, optical electrochemical or other high-speed data processing device that performs logical, arithmetic or memory functions by the manipulations of electronic, magnetic or optical signals or impulses," a modern telephone is almost certainly a "computer" and its unauthorized use would fall under the statute.

The Fourth Circuit endorsed the reasoning of *Nosal*, holding "that an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer. Thus, he accesses a computer 'without authorization' when he gains admission to a computer without approval." *WEC Carolina Energy Solutions LLC v. Miller*, 687 F3d 199, 204 (4th Cir 2012). Further, the person "'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access. *Notably, neither of these definitions extends to the improper use of information validly accessed.*" *Id.* (internal citation omitted, emphasis added).

It is worth reiterating that the CFAA is much broader in an important respect than ORS 164.377(4). Whereas the latter bars only unauthorized use, access, or attempted access, the CFAA also targets *exceeding authorized access*. Thus, to continue defendant's analogy of an office building the CFAA targets not only people who unlawfully walk in the front door, but also those with permission to enter the building but who then continue into private areas. Even under that broader statute defendant would not be culpable because she never entered a place she was not permitted to be.

Professor Orin Kerr proposes a framework for interpreting the CFAA based upon social norms of access. Orin. S. Kerr, *Norms Of Computer Trespass* (Colum. L. Rev. forthcoming 2016) (manuscript at 7, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2601707). He argues that traditional trespass laws safely can contain textual ambiguity because social norms provide the real meaning of nebulous phrases such "not licensed or privileged" to enter. *Id. See also Florida v. Jardines*, __ US __, 133 S Ct 1409, 1415, 185 L Ed 2d 495 (2013) (complying with implicit understanding of acceptable manner of approaching a person's home "does not require fine-grained legal knowledge; it is generally managed without incident by the Nation's Girl Scouts and trick-or-treaters."). Kerr explains that the same principles govern computer trespass, but notes that "the norms of computer usage will be less intuitive for some readers than for others." Kerr (manuscript

at 14). After discussing many hard cases that can arise when computer trespass laws are applied to violations of terms-of-use policies on the web, Kerr turns to the norms of account-based cases – that is, cases where someone uses an account to access a computer. *Id.* (manuscript at 30). He argues that "[c]reating [an] account represents a specific delegation of access rights * * *." *Id.* (manuscript at 31).

When an employee has valid access to a computer account he or she is not trespassing by using that account. As Kerr concludes,

> "When an employer grants an account to an employee, the employee is authorized to access the account for any reasons. * * * The employer can revoke the account or fire the employee, either of which will withdraw authorization to use any authentication credentials to access an account. * * * An employee who acts outside of the scope of agency might be guilty of some other civil or criminal wrong, such as theft of trade secrets or breach of contract. But the employee is not guilty of computer trespass absent some kind of adverse action by the employer."

Id. (manuscript at 37).

The Tiger Mart did not give employees individual accounts on the lottery computer. Instead, the first person to arrive in the morning would "sign on using a retailer I.D. and a pass code." Tr. 31-32. However, as discussed above, defendant was authorized and expected to use that computer account as part of her duties. A representative of the lottery agreed that, whoever was authorized by a retailer to use a lottery machine was permitted to do so. Tr. 34-35. Thus, defendant was authorized to access and use the computer.

V. A trespass-oriented interpretation of ORS 164.377(4) avoids sweeping a broad array of otherwise lawful conduct under the ambit of that statute and allowing private entities to criminalize lawful conduct.

Because the text and context of ORS 164.377(4) make clear that the legislature did not intend to criminalize violations of computer use-restrictions, this court need not consider maxims of statutory construction. If it nevertheless reaches that level of analysis, however, this court should interpret the statute in such a way as to avoid constitutional concerns. *State v. Kitzman*, 323 Or 589, 602, 920 P2d 134 (1996) ("when one plausible construction of a statute is constitutional and another plausible construction of a statute is unconstitutional, courts will assume that the legislature intended the constitutional meaning").

If ORS 164.377 criminalizes violation of a privately-enacted use policy, it presents significant constitutional vagueness concerns. Under Oregon law,

> "[t]he terms of 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. * * * A criminal statute need not define an offense with such precision that a person in every case can determine in advance that a specific conduct will be within the statute's reach. However, a reasonable degree of certainty is required by Article I, sections 20 and 21."

State v. Graves, 299 Or 189, 195, 700 P2d 244 (1985). To satisfy the requirements of federal due process, "a penal statute [must] define the criminal offense [1] with sufficient definiteness that ordinary people can understand what conduct is prohibited and [2] in a manner that does not encourage arbitrary and discriminatory enforcement." *Skilling v. United States*, 561 US 358, 402-

03, 130 S Ct 2896, 177 L Ed 2d 619 (2010) (quoting *Kolender v. Lawson*, 461 US 352, 357, 103 S Ct 1855, 75 L Ed 2d 903 (1983) (brackets in *Skilling*). It is incumbent on the legislature, in defining a crime, to state what is prohibited. It may not delegate to some future body the task of determining what is unlawful. *See State v. Hodges*, 254 Or 21, 28, 457 P2d 491 (1969) ("Such a statute not only creates a serious danger of inequality in the administration of the criminal law, but it runs squarely contrary to the purpose of Oregon Constitution, Art. I, s 21, which prohibits the delegation of legislative power.").

Under the trial court's interpretation of ORS 164.377(4), it is almost certainly unconstitutionally vague. That statute would make it a crime to take any action on a computer that has not been expressly authorized by the computer's owner. Such restrictions may be incorporated in a computer use policy, which can be altered without limit at any time, or they may be mere oral declarations. An employee may arrive at work Monday morning to find that not only is the use of streaming is now against the terms of his or her employment, but that it is also a Class A misdemeanor.

The state does not dispute that this is the import of its position. At oral argument in the Court of Appeals, the following exchange took place:

> "**Judge Armstrong**: Just to be clear, is the state's view that the list of consequences of the application of an understanding that the state advances here would in fact make a violation of this

> statute the use of a computer to play a game of solitaire if the owner of the computer, the otherwise source of that authority had said, 'You can use this at the office but you can't do these things with it.' That sub (4) would thereby criminalize the person at the officer who's playing solitaire? That that's the understanding that the state believes is correct?
>
> "**The State:** I believe that's what the statute says. Of course, one difference here is that it would criminalize it, but sub (4) is typically a misdemeanor. It only becomes a felony if it's an Oregon* * * Lottery Computer.
>
> "**Judge Armstrong:** Well that will be some comfort, that it's just a misdemeanor.
>
> "**Judge Wollheim:** Excuse me, am I understanding your answer to be, 'Yes, playing solitaire on your OJD computer when you've been told not to, would subject you to 164.377(4), but it would be a misdemeanor because you're not taking very much?
>
> "**The State:** Well, it would be a misdemeanor because it only provides for a misdemeanor.
>
> "**Judge Wollheim:** I just want to make sure I understood.
>
> "**The State:** But, realistically, I think – I've never heard of anybody getting prosecuted * * * for the solitaire thing."

While a prosecution for playing solitaire is an amusing example, and while defendant agrees that such a prosecution would be unlikely, the problem of allowing the privatization of the creation of criminal law is a real one. A reasonable prosecutor may never bring charges against a person for illicitly whiling away time at work on a card came, federal prosecutors have charged a woman with violating the CFAA for creating a fake Myspace profile in contravention of that site's terms of service. *See United States v. Drew*, 259

FRD 449, 452 (CD Cal 2009). No limiting principle so far identified in this case would prevent liability under ORS 164.377(4) if a person, for example, accessed a web page while violating an aspect of its voluminous (and often unread)[11] terms of service.[12]

One commenter framed the constitutional problem presented by the state's interpretation of ORS 164.377(4) as a violation of the private nondelegation doctrine. Arguing that the CFAA, if interpreted to criminalize violations of use policies, constitutes a private delegation of lawmaking, the author writes,

> "Congress has passed no law, and no agency of the federal government is empowered to issue rules, regarding what types of use restrictions qualify as governing authorization and thus fall under the CFAA's domain. And no review, approval, or collaborative lawmaking process restricts criminal application of the CFAA to only fair or even rational use restrictions."

---

[11] One study estimated that the average American internet would need to spend 201 hours per year to read every privacy policy her or she encountered. Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 565 (2009). The failure to do so is probably a good thing, as this would result in $781 billion in lost time annually. *Id.*

[12] And defendant's proposed interpretation is not a panacea. For example, a modern smartphone is almost certainly a "computer." If a person picks up a friend's iPhone without permission and unlocks it to check the time, he or she is likely using and accessing that computer without authorization, even under defendant's proposed trespass-based interpretation. Although this statute is a rough fit for the modern world of computers, defendant does not ask that this court rewrite it. *See State v. Guzek*, 322 Or 245, 264, 906 P2d 272 (1995) (court not authorized to rewrite a statute or ignore its plain meaning).

Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv L Rev 751, 769 (2013).

CONCLUSION

Enacted a generation ago, Oregon's computer crime statute was not intended to transform computer-use policies into private criminal statutes. Such a broad interpretation is not consistent with the text, context, or legislative history of that statute. Nor is it necessary. ORS 164.377(2) criminalizes the use of computer for various improper purposes. Indeed, defendant's conduct in this case likely would have fallen under that provision had the grand jury alleged it. To broaden the reach ORS 164.377(4) to cover defendant's conduct, this court would have to sweep an almost unlimited number of people under its reach. As Professor Kerr writes,

> "The checking of personal e-mail, viewing a weather report, or loading up a news site is the modern equivalent of getting up to stretch, or to talk briefly with a coworker. It is downtime, time spent recharging mental batteries. And yet because it uses a computer, it is also technically 'accessing' a protected computer. Each visit, each checking, and each viewing involves entering a command into a computer network and retrieving information from a server. Assuming that using a computer to retrieve information 'accesses' that computer, the interpretation that courts give to lack of authorization ends up determining whether these keystrokes amount to federal crimes."

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1585-86 (2010) (footnotes omitted). This is no less true

under Oregon's computer crime scheme, and making these acts into crimes is not what the Oregon Legislature intended. This court should reverse the decision of the Court of Appeals.

Respectfully submitted,

ERNEST G. LANNET
CHIEF DEFENDER
CRIMINAL APPELLATE SECTION
OFFICE OF PUBLIC DEFENSE SERVICES

ESigned

_____

DANIEL C. BENNETT OSB #073304
SENIOR DEPUTY PUBLIC DEFENDER
Dan.Bennett@opds.state.or.us

Attorneys for Defendant-Appellant
Caryn Aline Nascimento

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

Petition length

I certify that (1) this petition complies with the word-count limitation in ORAP 9.05(3)(a) and (2) the word-count of this petition (as described in ORAP 5.05(2)(a)) is 8,562 words.

Type size

I certify that the size of the type in this petition is not smaller than 14 point for both the text of the petition and footnotes as required by ORAP 5.05(4)(f).

NOTICE OF FILING AND PROOF OF SERVICE

I certify that I directed the original Brief on the Merits of Petitioner on Review to be filed with the Appellate Court Administrator, Appellate Courts Records Section, 1163 State Street, Salem, Oregon 97301, on August 4, 2015.

I further certify that I directed the Brief on the Merits of Petitioner on Review to be served upon Anna Joyce attorney for Respondent on Review, on August 4, 2015, by having the document personally delivered to:

Anna Joyce #013112
Solicitor General
400 Justice Building
1162 Court Street NE
Salem, OR 97301
Phone: (503) 378-4402
Attorney for Respondent on Review

Respectfully submitted,

ERNEST G. LANNET
CHIEF DEFENDER
CRIMINAL APPELLATE SECTION
OFFICE OF PUBLIC DEFENSE SERVICES

ESigned

_____

DANIEL C. BENNETT OSB #073304
SENIOR DEPUTY PUBLIC DEFENDER
Dan.Bennett@opds.state.or.us
Attorneys for Petitioner on Review
Caryn Aline Nascimento