
IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON,
Plaintiff-Appellee,

v.

CARYN ALINE NASCIMENTO,
aka CARYN ALINE DEMARS,
Defendant-Appellant.

Jefferson County Circuit Court
Case No. 09FE0092

Appellate Court No. A147290

S063197

**BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF PETITION FOR REVIEW OF DEFENDANT-
APPELLANT**

Petition for Review of Decision of the Court of Appeals
On appeal from the Judgment of the Circuit Court
For Jefferson County for the State of Oregon
Honorable GEORGE W. NEILSON, Judge

Opinion Filed: February 4, 2015

Author of Opinion: Armstrong, Presiding Judge

Before: Armstrong, Presiding Judge; Nakamoto, Judge; and Egan, Judge

ELECTRONIC FRONTIER
FOUNDATION
Jamie L. Williams, Esq.
(CA State Bar. No. 250087)
(*pro hac vice* pending)
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993

CREIGHTON & ROSE, PC
J. Ashlee Albies, Esq.
(OR State Bar No. 05184)
815 SW Second Ave., Suite 500
Portland, OR 97204
Tel: (503) 221-1792
Fax: (503) 223-1516

Counsel for *Amicus Curiae*
ELECTRONIC FRONTIER FOUNDATION

TABLE OF CONTENTS

SUMMARY OF ARGUMENT	1
ARGUMENT	2
I. THE COURT SHOULD GRANT REVIEW BECAUSE THIS CASE PRESENTS A SIGNIFICANT ISSUE OF LAW THAT IS A MATTER OF FIRST IMPRESSION FOR THIS COURT.	2
A. The Court of Appeals’ Incorrectly Found That Its Decision Did Not Involve Construction of ORS 164.377(4).....	3
B. The Restriction Here Is a <i>De Facto</i> Use Restriction, and the Distinction Drawn by the Court of Appeals Does Not Hold Up to Scrutiny.	5
II. THE COURT SHOULD GRANT REVIEW BECAUSE THE COURT OF APPEALS’ HOLDING AFFECTS A VAST NUMBER OF INDIVIDUALS.....	10
A. The Court of Appeals’ Decision Turns a Vast Number of Ordinary Individuals Into Criminals.....	10
B. The Court of Appeals’ Decision Renders ORS 164.377 Unconstitutionally Vague.	16
CONCLUSION.....	20

TABLE OF AUTHORITIES

STATE CASES

<i>Badger v. Paulson Inv. Co.</i> , 311 Or. 14, 803 P.2d 1178 (1991).....	13
<i>Computer Concepts, Inc. v. Brandt</i> , 310 Or. 706, 801 P.2d 800 (1990).....	13
<i>Karsun v. Kelley</i> , 258 Or. 155, 482 P.2d 533 (1971).....	13
<i>State v. Nascimento</i> , 268 Or. App. 718, 343 P.3d 654 (2015).....	<i>passim</i>

FEDERAL CASES

<i>Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.</i> , 690 F. Supp. 2d 1267 (M.D. Ala. 2010).....	12
<i>Black & Decker, Inc. v. Smith</i> , 568 F. Supp. 2d 929 (W.D. Tenn. 2008).....	12
<i>Brett Senior & Assocs., P.C. v. Fitzgerald</i> , No. 06-cv-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007).....	12
<i>Clarity Servs., Inc. v. Barney</i> , 698 F. Supp. 2d 1309 (M.D. Fla. 2010).....	12
<i>Connally v. Gen. Const. Co.</i> , 269 U.S. 385 (1926).....	16
<i>Craigslist Inc. v. 3Taps Inc.</i> , 942 F. Supp. 2d 962 (N.D. Cal. 2013).....	8
<i>Diamond Power Int'l, Inc. v. Davidson</i> , 540 F. Supp. 2d 1322 (N.D. Ga. 2007).....	12

<i>Dresser-Rand Co. v. Jones</i> , 957 F. Supp. 2d 610 (E.D. Pa. 2013).....	12
<i>Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Masuda</i> , 390 F. Supp. 2d 479 (D. Md. 2005).....	12
<i>Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc.</i> , No. 08-cv-3980-JS-ETB, 2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009)....	12
<i>Koch Industries, Inc. v. Does</i> , No. 2:10-cv-1275-DAK, 2011 WL 1775765 (D. Utah May 9, 2011).....	12
<i>Kolender v. Lawson</i> , 461 U.S. 352 (1983)	16
<i>LewisBurke Associates, LLC v. Widder</i> , 725 F. Supp. 2d 187 (D.D.C. 2010).....	12
<i>Lockheed Martin Corp. v. Speed</i> , No. 6:05-cv-1580-ORL, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006).....	12
<i>LVRC Holdings LLC v. Brekka</i> , 581 F.3d 1127 (9th Cir. 2009)	5, 11
<i>Nat’l City Bank, N.A. v. Republic Mortgage Home Loans, LLC</i> , No. 09-cv-1550-RSL, 2010 WL 959925 (W.D. Wash. Mar. 12, 2010).....	12
<i>Orbit One Commc’ns, Inc. v. Numerex Corp.</i> , 692 F. Supp. 2d 373 (S.D.N.Y. 2010)	12
<i>ReMedPar, Inc. v. AllParts Med., LLC</i> , 683 F. Supp. 2d 605 (M.D. Tenn. 2010)	12
<i>Scottrade, Inc. v. BroCo Investments, Inc.</i> , 774 F. Supp. 2d 573 (S.D.N.Y. 2011)	12
<i>Shamrock Foods Co. v. Gast</i> , 535 F. Supp. 2d 962 (D. Ariz. 2008).....	12

<i>Skilling v. United States</i> , 561 U.S. 358 (2010)	16
<i>United States v. Kozminski</i> , 487 U.S. 931 (1988)	18, 19
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012) (en banc)	<i>passim</i>
<i>WEC Carolina Energy Solutions LLC v. Miller</i> , 687 F.3d 199 (4th Cir. 2012)	6, 11

STATE STATUTES

Oregon Revised Statute 164.057	14
Oregon Revised Statute 164.377(4)	<i>passim</i>

FEDERAL STATUTES

18 U.S.C. § 1030	<i>passim</i>
------------------------	---------------

STATE RULES

Oreagaon Rules of Appellate Procedure, Rule 9.07	2, 10, 15, 20
--	---------------

OTHER AUTHORITIES

Dartmouth College, Employment Policies and Procedures Manual	18
Employee Handbook, Policies and Procedures	18
Robin K. Kutz, <i>Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act</i> , 27 Wm. & Mary L. Rev. 783 (1986)	13
Orin S. Kerr, <i>Vagueness Challenges to the Computer Fraud and Abuse Act</i> , 94 Minn. L. Rev. 1561 (2010)	16
Susan M. Heathfield, <i>Internet and Email Policy</i>	17

The American Heritage Dictionary (5th ed. 2014)..... 5

Virginia Dep't of Human Resource Management, *Use of the Internet and
Electronic Communications Systems*..... 18

SUMMARY OF ARGUMENT

The Court of Appeals upheld Defendant Caryn Nascimento’s computer crime conviction based on her act of accessing a lottery terminal—a computer that she was authorized to access for work-related purposes—for an improper and non-work related purpose. In so doing, the court implicitly interpreted the phrase “without authorization” of Oregon’s computer crime statute, ORS 164.377(4), to include instances where an employee with authorization to access a computer uses that access in violation of an employer’s computer use policy. Although the Court of Appeals purported to avoid construing the phrase “without authorization” in the statute, construing the phrase is exactly what the lower court did. *See State v. Nascimento*, 268 Or. App. 718, 722, 343 P.3d 654, 656 (2015).

The Court of Appeals’ implicit interpretation of the phrase “without authorization” extends ORS 164.377(4) to make criminals out of millions of unsuspecting Oregonians on the basis of innocuous and routine behavior. The Ninth Circuit, *en banc*, has explicitly rejected such a broad interpretation of parallel language in the federal computer crime statute, the Computer Fraud and Abuse Act (“CFAA”), for precisely this reason. *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (*en banc*) (“Were we to adopt the government’s proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct.”).

The Court of Appeals' decision is thus of far greater import than it would like to believe. This case not only presents a matter of first impression for this Court—the interpretation of ORS 164.377(4)—but it will also affect millions of individuals within the state of Oregon who will find themselves within the reach of the statute as a result of the Court of Appeals' expansive interpretation. Review is therefore necessary under ORAP 9.07 to ensure that Oregon's computer crime statute does not inadvertently transform vast numbers of ordinary individuals into criminals for innocuous, everyday behavior. This Court should therefore grant Ms. Nascimento's petition for review.

ARGUMENT

I. THE COURT SHOULD GRANT REVIEW BECAUSE THIS CASE PRESENTS A SIGNIFICANT ISSUE OF LAW THAT IS A MATTER OF FIRST IMPRESSION FOR THIS COURT.

Pursuant to ORAP 9.07, two of the listed criteria relevant to the decision whether to grant discretionary review are (i) whether the case presents a significant issue of law, such as the interpretation of a statute, and (ii) whether the issue is one of first impression for the Court. *See* ORAP 9.07(1)(b), (5). Both of these criteria are presented here. Namely, this case implicates the proper interpretation of the phrase “without authorization” for purposes of ORS 164.377(4)—a question that has not yet been addressed by this Court and which has significant implications on the statute's scope.

A. The Court of Appeals’ Incorrectly Found That Its Decision Did Not Involve Construction of ORS 164.377(4).

ORS 164.377(4) provides that “[a]ny 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) (emphasis added). The Court of Appeals upheld Ms. Nascimento’s computer crime conviction based on her act of accessing a lottery terminal—a computer that she was authorized to access for purposes of selling and validating lottery tickets for paying customers—for an improper and non-work related purpose, *i.e.*, printing lottery tickets for herself without paying for them. *Nascimento*, 268 Or. App. at 722. The Court of Appeals incorrectly found that its decision to affirm Ms. Nascimento’s conviction did not involve construction of ORS 164.377(4), stating that it need not resolve the issue of whether the statute “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 interest.” *Nascimento*, 268 Or. App. at 722. Although the court did not explicitly answer this question, its decision implicitly did by concluding that the actions of Ms. Nascimento—*i.e.*, an employee

with authorization to access a computer who used that access in violation of an employer-imposed computer use restriction—fell within the purview of the statute.

In declaring that it was not resolving the issue of whether ORS 164.377(4) encompasses the use of a device that a person has authorization to physically access in a manner contrary to company policy, the Court of Appeals drew a distinction between the restriction imposed on Ms. Nascimento and other forms of employee computer use restrictions, such as a restriction against playing solitaire on a work computer. *Id.* According to the Court of Appeals, Ms. Nascimento had “limited authorization to *physically access* the lottery terminal” to either sell or validate lottery tickets for paying customers, rather than “general authorization to be on a computer to carry out her duties[.]” *Id.* (emphasis in original). The court reasoned that having such “limited authorization” is different than having “general authorization” but being subject to limits imposed via corporate computer use restrictions, such as a restriction against “playing solitaire during work hours.” *Id.*

The court, however, failed to outline the nature of the difference between these two purported forms of authorization. And indeed, upon closer scrutiny, it is clear that there is no true distinction. Both the limitation imposed on Ms. Nascimento by her employer (the prohibition against using the lottery computer for anything but selling or validating lottery tickets for paying customers) and limitations on computer use imposed by written corporate policies

(prohibitions against using a work computer for non-work-related purposes) are *de facto* computer use restrictions. The Court of Appeals simply found two different ways to describe the very same thing.

B. The Restriction Here Is a *De Facto* Use Restriction, and the Distinction Drawn by the Court of Appeals Does Not Hold Up to Scrutiny.

An employer gives an employee “authorization” to access a company computer when the employer gives her permission to use it. *See The American Heritage Dictionary* (5th ed. 2014), available at <https://www.ahdictionary.com> (last visited May 6, 2015) (defining “authorize” as “[t]o grant authority or power to;” and “[t]o give permission for (something); sanction[.]”); *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (defining “authorization” for purposes of the CFAA to mean granting an employee permission to use a computer). As such, an employee accesses a computer “without authorization” when she accesses data or information she does not have permission to access. In the context of the CFAA—the federal computer crime statute, which has language similar to that of ORS 164.377¹—federal courts

¹ Both the CFAA and ORS 164.377(4) include the phrase “without authorization.” The CFAA prohibits “intentionally access[ing] a computer *without authorization* or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer[.]” *See* 18 U.S.C. § 1030(a)(2)(C) (emphasis added). Similarly, ORS 164.377(4) provides that “[a]ny 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

distinguish between access restrictions and use restrictions in determining whether an employee has accessed a computer without authorization or in excess of their authorization. *See, e.g., Nosal*, 676 F.3d at 863–64. Use restrictions refer to restrictions governing how a person can use their access to a computer, or information stored thereon, while access restrictions are technological restrictions on what data they can actually access. And according to both the Ninth and Fourth Circuit Courts of Appeal, the two most recent federal circuit courts to address the issue, when an employee who is authorized (*i.e.*, who has permission) to access a computer uses that access in violation of a computer use restriction, her access is not rendered unauthorized. *See id.* at 863–64 (“[W]e hold that ‘exceeds authorized access’ in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.”) (emphasis in original); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 205 (4th Cir. 2012) (noting that where “an employee uses his own username and password to access

data contained in such computer, computer system or computer network, commits computer crime.” ORS 164.377(4) (emphasis added). The fact that the CFAA encompasses individuals who act both without authorization and in excess of authorization shows they are clearly two distinct concepts. Notably, unlike the CFAA, ORS 164.377 does not include the phrase “exceed[ing] authorized access.” Thus, the Court of Appeals in essence rewrote the statute to add that concept to ORS 164.377 to find that Ms. Nascimento, who it was undisputed had access to the lottery computer for limited purposes, violated the computer crime statute. And as explained below, even if ORS 164.377 encompasses individuals who exceed their access, she did not exceed that access (or act without authorization) by using her access for an improper purpose.

the information and then puts it to an impermissible use his ‘manner’ of access remains valid”).

In other words, violating a computer use restriction does not change the fact that the employee is authorized to access the computer. In order to access the computer “without authorization,” or in excess of authorization, the employee must have circumvented a “technological access barrier”—a security measure built into the technology designed to control who has the ability to access certain kinds of data—via “hacking” or some form of manipulation of the computer’s security and thereby obtained information that she would not otherwise have been able to obtain. *See Nosal*, 676 F.3d at 858 (“If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not ‘entitled *so* to obtain.’”) (emphasis in original).

The Court of Appeals failed to engage in an analysis of whether the restriction at issue in this case—the prohibition against using the lottery computer for anything other than selling or validating lottery tickets for paying customers—was a use restriction or an access restriction. Instead, through characterizing Ms. Nascimento’s access as “limited” as opposed to “general,” the court incorrectly assumed that the restriction was one on access, rather than on *use*. *See Nascimento*, 268 Or. App. at 721–22. But this attempt to distinguish the restriction

imposed on Ms. Nascimento from other forms of computer use restrictions misconstrues the nature of the restriction at issue—which governed Ms. Nascimento’s use of the lottery computer, not whether she could access it at all. Indeed, the only restriction on Ms. Nascimento’s ability to use the lottery computer was the purpose for which she was accessing it. *See id.* at 722 (“[t]he state does not deny that defendant had limited, implicit authorization from the store manager to access the lottery terminal to sell tickets to paying customers.”). Since the restriction at issue here depends entirely on the purpose underlying her *use* of the computer, it is a *de facto* use restriction. *See Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 969–70 (N.D. Cal. 2013) (finding that a website’s terms of use—which provided rules about how site visitors could use data and prohibited the use of data in ways that violated the site’s terms of use—provided “use” restrictions regardless of the fact that they were “framed in terms of ‘access’”). And unlike a true access restriction, Ms. Nascimento *did* have unlimited access to the lottery computer for purposes of selling or validating lottery tickets, and did not have to “hack” or otherwise circumvent any technological access barrier to access the computer on the instances underlying this case. *See Nosal*, 676 F.3d at 858, 863–64. The restriction at issue here is thus a clear use restriction, not an access restriction.

As such, the only basis for concluding that Ms. Nascimento had “limited authorization” is the fact that she was subject to an employer-imposed computer use restriction delineating how she could use the lottery computer. *See Nascimento*, 268 Or. App. at 722. Indeed, employees subject to restrictions against using work computers to play computer games or check personal email could equally be said to have “limited authorization” to use the computers for work-related purposes. The fact that the use restriction imposed on Ms. Nascimento was more restrictive than many other forms of computer use restrictions does not change the fact that it is a restriction on use, not access. As both the limitation imposed on Ms. Nascimento by her employer and limitations on computer use imposed by written corporate policies are *de facto* use restrictions, the purported distinction drawn by the Court of Appeals does not hold up to scrutiny.

Through upholding Ms. Nascimento’s conviction based on her act of accessing the lottery computer in violation of her employer-imposed computer use restriction, the court affirmatively answered the very question it purported not to answer—*i.e.*, whether ORS 164.377(4) “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 interest.” *See Nascimento*, 268 Or. App. at 722. This question is not only one of statutory interpretation (and thus a significant issue of law), but also an issue of first impression for this Court. As

such, review of the Court of Appeals' decision is warranted and appropriate under ORAP 9.07(1)(b) and (5).

II. THE COURT SHOULD GRANT REVIEW BECAUSE THE COURT OF APPEALS' HOLDING AFFECTS A VAST NUMBER OF INDIVIDUALS.

Not only does this case present a significant issue of law that is a matter of first impression for this Court, but the Court of Appeals' decision, if allowed to stand, will affect millions of individuals within the state of Oregon—another criterion relevant to the decision whether to grant discretionary review. *See* ORAP 9.07(3) (listing as one criterion “whether many people are affected by the decision in the case”). Namely, through broadly construing the phrase “without authorization” to include violations of employer-imposed computer use restrictions, the decision turns a vast number of ordinary individuals into criminals for everyday, innocuous behavior and renders the statute unconstitutionally vague.

A. The Court of Appeals' Decision Turns a Vast Number of Ordinary Individuals Into Criminals.

Although employees are seldom disciplined for the occasional use of work computers for personal purposes, such activities are routinely prohibited by corporate computer use policies. The Court of Appeals' decision transforms such minor dalliances into crimes. In this way, the court turns ORS 164.377(4) on its head by allowing employers—rather than the legislature—to unilaterally decide

what behavior is “authorized” and what behavior constitutes criminal activity. The decision thereby opens millions of individual employees to criminal liability.

The concern over transforming millions of ordinary individuals into criminals based on innocuous, everyday behavior has led numerous federal courts interpreting the similarly worded CFAA—including the Ninth and Fourth Circuit Courts of Appeals, the two most recent federal circuit courts to address the issue—to narrowly interpret the phrases “without authorization” and “exceeds authorized access” for purposes of the CFAA.² *See Nosal*, 676 F.3d at 856, 859–63; *WEC Carolina*, 687 F.3d at 206. Both the Ninth and Fourth Circuit have interpreted the phrase “without authorization” to refer to situations where a person “has no rights, limited or otherwise, to access the computer in question”—*i.e.*, when she “accesses a computer *without any permission at all.*” *Brekka*, 581 F.3d at 1133; *see also WEC Carolina*, 687 F.3d at 206 (finding “without authorization” applies “only when an individual accesses a computer without permission). Both circuits interpret the phrase “exceeds authorized access” to refer to situations where a person “has permission to access the computer, but accesses information on the computer that the person is not entitled to access.” *See Brekka*, 581 F.3d at 1133; *see also WEC Carolina*, 687 F.3d at 206 (narrowly interpreting the phrase

² For the text of section 1030(a)(2)(C) of the CFAA, *see supra* note 1.

“exceeds authorized access” to apply “only when an individual . . . alters information on a computer beyond that which he is authorized to access”).

The narrow interpretation adopted by both the Ninth and Fourth Circuits, and the majority of other federal courts to address the issue,³ thereby criminalizes only the actions of those who access information on a computer that they are not entitled to obtain at all, not the actions of those who have authority to access information on a computer but who do so in violation of an employer-imposed computer use restriction. Such a narrow interpretation ensures that what was meant to be a computer crime statute is not transformed into a massive

³ For other federal court decisions narrowly interpreting the CFAA to not include situations involving the misuse of data a person is otherwise entitled to obtain, see *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013); *Scottrade, Inc. v. BroCo Investments, Inc.*, 774 F. Supp. 2d 573, 584 (S.D.N.Y. 2011); *Orbit One Commc’ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385–86 (S.D.N.Y. 2010); *LewisBurke Associates, LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010); *Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272–73 (M.D. Ala. 2010); *Clarity Servs., Inc. v. Barney*, 698 F. Supp. 2d 1309, 1315–16 (M.D. Fla. 2010); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 613 (M.D. Tenn. 2010); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929, 934–36 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 966–967 (D. Ariz. 2008); *Diamond Power Int’l., Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); *Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005); see also *Koch Industries, Inc. v. Does*, No. 2:10-cv-1275-DAK, 2011 WL 1775765, at *8 (D. Utah May 9, 2011); *Nat’l City Bank, N.A. v. Republic Mortgage Home Loans, LLC*, No. C09-1550RSL, 2010 WL 959925, at *3 (W.D. Wash. Mar. 12, 2010); *Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc.*, No. 08-cv-3980-JS-ETB, 2009 WL 2524864, at *5–6 (E.D.N.Y. Aug. 14, 2009); *Brett Senior & Assocs., P.C. v. Fitzgerald*, No. 06-cv-1412, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007); *Lockheed Martin Corp. v. Speed*, No. 6:05-cv-1580-ORL, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006).

misappropriation statute. As noted above, both the CFAA and ORS 164.377(4) employ similar “without authorization” language, and the two computer crime statutes should therefore be interpreted similarly.⁴ See *Badger v. Paulson Inv. Co.*, 311 Or. 14, 21, 803 P.2d 1178, 1182 (1991) (“In situations involving Oregon laws in large measure drawn from a federal counterpart, it is appropriate to look for guidance to federal court decisions interpreting similar federal laws, even though those decisions do not bind us.”); Robin K. Kutz, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 Wm. & Mary L. Rev. 783, 789 & n.31 (1986) (noting that Oregon’s computer crime law was one of various state computer crime laws originally modeled on the 1977 or 1979 version of the proposed Federal Computer Systems Protection Act); see also *Computer Concepts, Inc. v. Brandt*, 310 Or. 706, 714 n.7, 801 P.2d 800, 805 n. 7 (1990) (looking to federal cases “for guidance in interpreting the meaning of ‘investment contract’”); *Karsun v. Kelley*, 258 Or. 155, 161, 482 P.2d 533, 536 (1971) (because ORS 59.115(1)(b) (1967) adopted “substantially the same terms” as 15 U.S.C. § 771(2) (1933), “the legislative history of that act, as well as decisions construing its provisions, are of significant

⁴ See *supra* Note 1.

interest”). And indeed, the public policy implications of broadly interpreting the phrase are the same for both statutes.⁵

The Court of Appeals’ sweeping interpretation of ORS 164.377 creates the potential for draconian results not only in the context of employees who momentarily stray from their work duties, but also in the context of Internet users who unknowingly violate a website’s terms of use. The court’s holding that a person acts “without authorization” if she violates a policy regarding the use of a computer that she is otherwise authorized to access could be extended to an Internet user who accesses a website in violation of a written terms of service. For example, Facebook’s terms of use provide that “[y]ou will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.”⁶ But as the Ninth Circuit noted *en banc*, “[I]ying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight.” *Nosal*, 676 F.3d at 862. Under the Court of Appeals’ expansive reading of ORS 164.377, if a user shaves a few

⁵ Adopting the Ninth and Fourth Circuits’ narrow interpretation of “without authorization” does not mean the state has no way to prosecute Ms. Nascimento for printing out lottery tickets for herself without paying for them. Statutes criminalizing theft are sufficient to cover such behavior. Indeed, here, Ms. Nascimento was also separately charged and convicted of one count of aggravated first-degree theft (a Class B felony), a result *Amicus* does not challenge. See *Nascimento*, 268 Or. App. at 719; ORS 164.057.

⁶ Facebook, Statement of Rights and Responsibilities § 4, <http://www.facebook.com/terms.php> (last visited May 7, 2015).

years off her age in her profile information, asserts that she is single when she is in fact married, or seeks to obfuscate her current physical location, hometown or educational history for any number of legitimate reasons, she violates the computer crime law. *See id.* The court’s decision thus opens the door to turning millions of individual Internet users—not just millions of individual employees—into criminals for typical and routine Internet activity.

The Court of Appeals’ decision will thus affect a vast number of people, and review is appropriate and warranted under ORAP 9.07(3) on this basis alone—*i.e.*, to ensure that the interpretation of the statute does not inadvertently transform a vast numbers of ordinary individuals into criminals for innocuous, everyday behavior. *See* ORAP 9.07(3). In addition, through bringing more individuals within the reach of the statute, the issue presented in this case will also inevitably arise more often. Namely, if the Court of Appeals’ decision is upheld, ORS 164.377 will become an overbroad criminal misappropriation statute, and more individuals will be prosecuted under the statute for violations of computer use restrictions. Review is thus also appropriate and warranted under ORAP 9.07(2). *See* ORAP 9.07(2) (listing “[w]hether the issue or a similar issue arises often” as another criterion relevant to the decision whether to grant discretionary review).

B. The Court of Appeals' Decision Renders ORS 164.377 Unconstitutionally Vague.

The Court of Appeals' decision affects millions of individuals within the state of Oregon not only through turning them into criminals on the basis of innocuous, everyday behavior, but also through rendering ORS 164.377(4) unconstitutionally vague. The U.S. Supreme Court notes a criminal statute can violate due process and be void for vagueness if it either fails to provide fair notice as to what is criminal or has the potential to lead to arbitrary and discriminatory prosecutions. *See Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). Here, the Court of Appeals' reading of the statute fails both of these due process requirements.

In regard to notice, it is axiomatic that due process requires criminal statutes to provide ample notice of what conduct is prohibited. *See Connally v. Gen. Const. Co.*, 269 U.S. 385, 391 (1926). But the Court of Appeals' decision makes the essential meaning of ORS 164.377(4) dependent on employer-imposed policies and restrictions. Basing criminal liability on employer-imposed computer use restrictions—which are frequently unread, generally lengthy, and largely privately created, and which can be altered without notice—fail to put individuals on adequate notice of what conduct is criminally prohibited. *See Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1586 (2010) (making criminal liability dependent on an employer's

computer use restrictions “gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited”). Furthermore, making criminal liability dependent on an employer’s computer use restrictions confers on employers the power to outlaw any conduct they wish without the sufficient clarity and specificity required of criminal law. And because employers, like website owners, retain the right to modify their corporate policies or terms of use at any time without notice, “behavior that wasn’t criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.” *Nosal*, 676 F.3d at 862. As such, the Ninth Circuit has held that “[s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read.” *Id.* at 860.

Widely available sample Internet use policies further demonstrate the notice problems inherent in premising criminal liability on corporate use policies. One sample Internet and email usage policy, for example, warns that “Internet use, on Company time, is authorized to conduct Company business only,” and “[o]nly people appropriately authorized, for Company purposes, may use the Internet[.]”⁷ Another sample policy vaguely states that computer use restrictions include, “but

⁷ Susan M. Heathfield, *Internet and Email Policy*, http://humanresources.about.com/od/policiesandsamples1/a/email_policy.htm (last visited May 07, 2015).

are not limited to” seven specific prohibitions, as well as “any other activities designated as prohibited by the agency.”⁸ As indicated above, a policy’s lack of specificity is often made worse by the fact that employers may reserve the right to change policies at any time, and not necessarily with advance notice.⁹ Attaching criminal punishment to breaches of these vague, boilerplate policies makes it impossible for employees to know what conduct is criminally punishable at any given time.

In regard to arbitrary and discriminatory prosecution, through interpreting ORS 164.377 to “criminalize a broad range of day-to-day activit[ies]” the Court of Appeals subjects employees and Internet users alike to prosecution at the whim of prosecutors, who can then pick and choose which violations they wish to penalize. *See United States v. Kozminski*, 487 U.S. 931, 949 (1988) (rejecting interpretation of statute because it would “criminalize a broad range of day-to-day activity” and “subject individuals to the risk of arbitrary or discriminatory prosecution and

⁸ Virginia Dep’t of Human Resource Management, *Use of the Internet and Electronic Communications Systems*, <http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol1175useofinternet.pdf?sfvrsn=2> (last visited May 07, 2015).

⁹ *See, e.g.*, Employee Handbook, Policies and Procedures, <http://www.hrvillage.com/PandP/all.htm> (last visited May 7, 2015) (“The policies stated in this handbook are subject to change at any time at the sole discretion of the Company. From time to time, you may receive updated information regarding any changes in policy.”); Dartmouth College, Employment Policies and Procedures Manual, <http://www.dartmouth.edu/~hrs/policy> (last visited May 07, 2015) (“The policies are intended as guidelines only, and they may be modified, supplemented, or revoked at any time at the College’s discretion.”).

conviction”). As indicated above, many social media websites prohibit lying about or otherwise misrepresenting personal information. But under the Court of Appeals’ holding, “[t]he difference between puffery and prosecution may depend on whether you happen to be someone [a prosecutor] has reason to go after.” *See Nosal*, 676 F.3d at 862. It is this potential for abuse that has led most federal courts, as explained earlier, to reject a broad interpretation of phrases “without authorization” and “exceeds authorization” for the purposes of the CFAA. As the Ninth Circuit noted in the context of the CFAA, a broad statutory interpretation would ““delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes’ and would ‘subject individuals to the risk of arbitrary or discriminatory prosecution and conviction.’” *Nosal*, 676 F.3d at 862 (citing *Kozminski*, 487 U.S. at 949). Here, by giving that much power to prosecutors, the Court of Appeals has “invit[ed] discriminatory and arbitrary enforcement.” *Nosal*, 676 F.3d at 862.

The decision in this case will thus effect millions of ordinary individuals in the state of Oregon, not only by turning them into criminals on the basis of innocuous, everyday behavior, but also by ensuring that they are not on notice of what constitutes criminal activity under ORS 164.377 and leaving them open to

arbitrary and discriminatory prosecution. As such, review of the Court of Appeals' decision is warranted and appropriate under ORAP 9.07(3).

CONCLUSION

For the foregoing reasons, review is warranted and appropriate under ORAP 9.07, and necessary to ensure that Oregon's computer crime statute does not inadvertently transform vast numbers of ordinary individuals into criminals for innocuous, everyday behavior. This Court should grant Ms. Nascimento's petition for review.

Dated: May 12, 2015

Respectfully submitted,

/s/ J. Ashlee Albies

J. Ashlee Albies
OR Bar No. 05184
CREIGHTON & ROSE, PC
815 SW Second Ave, Suite 500
Portland, OR 97204
Tel: (503) 221-1792
Fax: (503) 223-1516

Jamie L. Williams
(*pro hac vice* pending)
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993

Counsel for *Amicus Curiae*
ELECTRONIC FRONTIER
FOUNDATION

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of ORAP 9.05(3)(a) because this brief contains 4,813 words, excluding the parts of the brief exempted by ORAP 5.05(2)(a).

2. This brief complies with the typeface and type style requirements of ORAP 5.05(4)(f) because this brief has been prepared in a proportionally spaced Times New Roman typeface, 14-point font.

Dated: May 12, 2015

/s/ J. Ashlee Albies
J. Ashlee Albies

**CERTIFICATE OF SERVICE
NOTICE OF FILING AND PROOF OF SERVICE**

I certify that I directed the original *amicus curiae* brief to be filed with the Appellate Court Administrator, Appellate Courts Records Section, 1163 State Street, Salem, Oregon, 97301, on May 12, 2015, by electronic filing.

I further certify that a copy of the *amicus curiae* brief was e-served pursuant to ORAP 16.45 on DANIEL C. BENNETT (#073304), attorney for the Petitioner on Review, on May 12, 2015.

I further certify that a copy of the *amicus curiae* brief was e-served pursuant to ORAP 16.45 on ELLEN F. ROSENBLUM (#753239), ANNA JOYCE (#013112), and JENNIFER S. LLOYD (#943724), attorneys for the Respondent on Review, on May 12, 2015.

Dated: May 12, 2015

/s/ J. Ashlee Albies
J. Ashlee Albies