# IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON, Respondent on Review,

v

RAJI AFIFE AZAR, Petitioner on Review.

(CC 18CR28295) (CA A170612) (SC S069578)

On review from the Court of Appeals.\*

Argued and submitted March 3, 2023.

Zachary Lovett Mazer, Deputy Public Defender, Office of Public Defense Services, Salem, argued the cause and filed the briefs for petitioner on review. Also on the briefs was Ernest G. Lannet, Chief Defender, Criminal Appellate Section.

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

Before Flynn, Chief Justice, and Duncan, Garrett, DeHoog, Bushong and Masih, Justices, and Balmer, Senior Judge, Justice pro tempore.\*\*\*

DeHOOG, J.

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

Bushong, J., dissented and filed an opinion, in which Garrett, J., and Balmer, S.J., joined.

 $<sup>^{\</sup>ast}$  Appeal from Multnomah County Circuit Court, Kenneth R. Walker, Judge. 318 Or App 724, 509 P3d 668 (2022).

<sup>\*\*</sup> James, J., did not participate in the consideration or decision of this case. Baldwin, Senior Judge, Justice pro tempore, participated in oral argument, but did not participate in the consideration or decision of this case.

### DeHOOG, J.

Under the Oregon Criminal Code, a person commits the offense of "computer crime" if, in relevant part, the person accesses or uses (or attempts to access or use) a computer, computer system, or computer network for the purpose of committing theft. ORS 164.377(2)(c).¹ At issue in this case is whether defendant's conduct fell within the scope of that provision. That is, does knowingly selling stolen property using the online auction site eBay—conduct that defendant does not dispute would constitute theft by receiving under ORS 164.095²—constitute computer crime?

The Court of Appeals, in a divided opinion, concluded that such conduct constitutes computer crime, and it upheld the trial court's denial of defendant's motion for judgment of acquittal as to the relevant charges against him. State v. Azar, 318 Or App 724, 738, 509 P3d 668 (2022). As we explain below, we conclude that the legislature did not intend for the computer crime statute to reach conduct such as defendant's, which may constitute "theft" within the meaning of the Criminal Code but neither interferes with another's protected interests in—or electronically located on—a computer, computer system, or computer network

<sup>&</sup>lt;sup>1</sup> ORS 164.377(2) provides, in part:

<sup>&</sup>quot;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:

**<sup>&</sup>quot;\*\*\***\*\*

<sup>&</sup>quot;(c) Committing theft, including, but not limited to, theft of proprietary information or theft of an intimate image."

<sup>&</sup>lt;sup>2</sup> Under ORS 164.095(1),

<sup>&</sup>quot;[a] person commits theft by receiving if the person receives, retains, conceals or disposes of property of another knowing or having good reason to know that the property was the subject of theft."

Although "disposes" is not defined by statute, defendant does not dispute that selling property that a person knows or should know is stolen constitutes theft by receiving. See State v. Farmer, 44 Or App 157, 160, 605 P2d 716 (1980) (reaching that conclusion based upon ORS 164.055(1)(c), which provides that theft by receiving constitutes theft in the first degree when "committed by buying, selling, borrowing or lending on the security of the property"). We assume for purposes of the present discussion that selling stolen property with the requisite mental state constitutes theft by receiving, but we express no opinion on when in the course of a transaction an online sale qualifies as "dispos[ing]," whether at the time of the sale, at the time the property is physically transferred, or at some other time.

(computer),<sup>3</sup> nor depends on computer technology as the means of gaining access to the thing that the person seeks to unlawfully obtain. Here, the conduct with which the state charged defendant involved the theft of merchandise that bore no relationship to eBay's or anyone else's protected interests in computers, their contents, or rights held in digital form, and defendant was not dependent on computer technology to gain access to something he sought to steal. Thus, we conclude that the trial court erred in denying defendant's motion for judgment of acquittal and, accordingly, reverse, in part, the decision of the Court of Appeals.<sup>4</sup>

#### I. BACKGROUND

#### A. Facts

When reviewing the denial of a motion for judgment of acquittal, "we view the evidence in the light most favorable to the state to determine whether any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *State v. Hubbell*, 371 Or 340, 343, 537 P3d 503 (2023). The Court of Appeals opinion sets forth the relevant facts—which are undisputed—in some detail. *Azar*, 318 Or App at 727-28. In brief, eBay is an internet site on which individuals can post items for sale either through an online auction or at fixed, "buy-it-now" prices. The eBay website processes purchasers' payments using—among other services—PayPal, an online payment platform. Sellers can then transfer funds received via PayPal into their own bank accounts.

<sup>&</sup>lt;sup>3</sup> The parties do not distinguish whether, for purposes of the computer crime statute, using eBay's online sales platform should be considered using (or accessing) a "computer," a "computer system," a "computer network," or some combination of all three, nor do they suggest that any such distinction might bear on our assessment of the arguments or our interpretation of ORS 164.377(2)(c). Thus, we use those terms largely interchangeably and use the term "computer" to collectively reference all three terms.

<sup>&</sup>lt;sup>4</sup> At trial, the jury convicted defendant of three counts of computer crime and other offenses. Four of those convictions were nonunanimous. On appeal, the Court of Appeals reversed and remanded defendant's four nonunanimous convictions—including the three counts of computer crime at issue here—under *Ramos v. Louisiana*, 590 US \_\_\_\_, 140 S Ct 1390, 206 L Ed 2d 583 (2020). *Azar*, 318 Or App at 726. Our decision regarding defendant's three computer crime convictions does not affect the Court of Appeals' ruling as to the remaining nonunanimous conviction.

As part of an investigation into a series of thefts from several retail stores, undercover investigators sold defendant various items of merchandise, falsely telling him that the items had been stolen. Law enforcement officers were then able to track the "stolen" merchandise by purchasing items from an eBay account associated with defendant and confirming that those items were the ones that they had sold to defendant. Police later arrested defendant, who admitted that he had used his sister's eBay account to sell stolen property. Defendant further admitted that he had obtained the sales proceeds by transferring the funds from his sister's PayPal account into his own PayPal account, and from there into his bank account.

## B. Procedural History

As a result of that conduct, the state charged defendant with, in relevant part, three counts of "computer crime," ORS 164.377(2)(c). The state's theory, as set out in the indictment, was that, by selling merchandise on eBay that he believed to be stolen, defendant had "access[ed] and use[d] a computer, computer system, and computer network for the purpose of committing theft of property" by receiving. At trial, defendant moved for judgment of acquittal as to those counts, arguing that the state had not proved that he had engaged in "computer hacking," which, he asserted, was required to establish computer crime. Defendant further argued that, if the computer crime statute could be applied broadly enough to encompass his conduct, then it would be unconstitutionally vague. The trial court denied defendant's

<sup>&</sup>lt;sup>5</sup> Defendant also was charged with and ultimately convicted of multiple counts of attempted first-degree theft (ORS 161.405 and ORS 164.055), laundering a monetary instrument (ORS 164.170), and conspiracy (ORS 161.450). Those other convictions are not at issue on review.

<sup>&</sup>lt;sup>6</sup> In *State v. Nascimento*, 360 Or 28, 42, 379 P3d 484 (2016), this court addressed a different subsection of the computer crime statute, ORS 164.377(4), which prohibits, in part, the *unauthorized* use or accessing of computers, computer systems, computer networks, or the data they contain. We observed that such intrusion or unauthorized access by third parties was commonly referred to as "hacking." *Nascimento*, 360 Or at 42 (observing more generally that, as introduced, the bill that later encompassed "computer crime" was initially concerned with the theft of cable television services). We understand defendant to use the term "hacking" in the same way. *See Webster's Third New Int'l Dictionary* 1018 (unabridged ed 2002) (defining "hacking," as relevant here, to mean "the gaining of unauthorized access to data in a system or computer").

motion, and a nonunanimous jury convicted defendant of those counts.

Defendant appealed, reprising his arguments from the trial court. The Court of Appeals reversed and remanded defendant's nonunanimous convictions for a new trial, but it otherwise affirmed. Azar, 318 Or App at 726. In a split decision, the majority held that "a person violates [ORS 164.377(2)] when the person's use or access of a computer is the direct, necessary means by which the person accomplishes one of the prohibited purposes in ORS 164.377(2)(a) through (c)." Id. at 737. The court rejected defendant's argument that computer crime is limited to computer hacking, as well as his contextual argument that "theft" under ORS 164.377(2)(c) is limited to taking something from a computer and does not encompass all conduct that might satisfy one of the various statutory definitions of "theft." In concluding otherwise, the court reasoned that, because "theft" has an "established legal meaning" in the Criminal Code, "theft" as used in ORS 164.377(2)(c) encompasses each of the forms of theft described in ORS 164.015, including theft by receiving, see ORS 164.015(5) (incorporating ORS 164.095 (defining that offense)). Id. at 733-34. As to defendant's vagueness challenge, the court explained that, because it construed the computer crime statute to require that a defendant's "use or access[ing]" of a computer be "more than incidental" and "the direct, necessary means" by which the defendant "accomplishes one of the prohibited purposes" identified in ORS 164.377(2)—including "[clommitting theft"—the statute "would allow a person of ordinary intelligence to understand the scope of what is prohibited \*\*\*." Id. at 737-38. That, the majority opinion concluded, resolved any constitutional concerns. Id.

Judge Pagán disagreed. He reasoned that the legislative history of ORS 164.377 indicated that the statute "was intended to address the type of criminal activity we most associate with hacking or other nefarious access to networks or computers, not simply the use of electronics to commit crimes." *Id.* at 743 (Pagán, J., concurring in part and dissenting in part). Based in part on subsequent amendments to ORS 164.377(2)(c), Judge Pagán viewed the computer

crime statute as somewhat "analogous to burglary—that is, accessing a place a person is not allowed to be with the intention of committing a crime *in that place*." *Id.* at 740 (emphasis in original). Judge Pagán further reasoned that, due to the ubiquitous nature of computer technology in modern society, the majority's understanding of the statute would encompass far more conduct than the legislature could have anticipated and would elevate any number of minor offenses to Class C felonies, which could not, in his view, have been what the legislature intended. *Id.* at 743.

Defendant sought review in this court, which we allowed.

#### II. DISCUSSION

Defendant argues on review that, as relevant here, computer crime under ORS 164.377(2)(c) is limited to "accessing or using another person's computer, computer system, or computer network to commit an unauthorized taking of information or data from that computer, computer system, or computer network \*\*\*." It follows, defendant reasons, that his conduct in utilizing eBay for the purpose of selling merchandise that he believed to be stolen—conduct that defendant appears to accept would be theft by receiving under ORS 164.095 if successfully carried out—does not constitute computer crime. More specifically, because "theft" as that term is used in ORS 164.377(2)(c) does not, in his view, encompass theft by receiving, his conduct of using or accessing eBay online to commit that offense is not "us[ing]" or "access[ing]" a computer "for the purpose of \*\*\* [c]ommitting theft" within the meaning of that paragraph. Defendant thus concludes that the trial court erred when it denied his motion for judgment of acquittal.

## A. The Text and Context of ORS 164,377(2)(c)

"When, as here, a trial court denies a defendant's motion for judgment of acquittal based on an interpretation of a statute, we review the denial for errors of law." *State v. Haley*, 371 Or 108, 112, 531 P3d 142 (2023). The specific statutory question in defendant's case is whether ORS 164.377(2)(c) encompasses his undisputed conduct of selling purportedly stolen merchandise on eBay. We resolve

that question under the framework set out in *State v. Gaines*, 346 Or 160, 206 P3d 1042 (2009). Our goal is to determine the intent of the legislature that enacted that provision. *Id.* at 171. In making that determination, we consider the disputed statutory text in context, together with any available legislative history that we find helpful. *Id.* at 172. If a statute's intended meaning remains unclear to us following our examination of its text, context, and legislative history, we may turn to general maxims of statutory interpretation for additional guidance. *See, e.g., Chaimov v. Dept. of Admin. Services*, 370 Or 382, 398 n 7, 520 P3d 406 (2022) (noting limited circumstances in which it may be appropriate for courts to consider general maxims of statutory interpretation).

In this case, the state charged defendant with computer crime based on his alleged violation of ORS 164.377 (2)(c), which provides:

"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:

**"**\*\*\*\*

"(c) Committing theft, including, but not limited to, theft of proprietary information or theft of an intimate image."

The disputed text here is "accesses \*\*\* or uses \*\*\* any computer \*\*\* for the purpose of \*\*\* [c]ommitting theft." On its face, that language is quite broad and can plausibly be understood to capture utilizing eBay to facilitate theft as defined by Oregon law, including theft by receiving under ORS 164.095, the specific form of "theft" underlying defendant's charges. But, as we will explain, an examination of the text and context of ORS 164.377(2)(c) leaves open the question whether the legislature intended to capture conduct such as defendant's—specifically, the lawful use of another's computer system in the course of committing theft—when it prohibited using or accessing computers "for the purpose" of committing theft. That is, when—if ever—might using or

 $<sup>^{7}</sup>$  As originally enacted, the conduct addressed under ORS 164.377(2)(c) was limited to "[c]ommitting theft." Or Laws 1985, ch 537, § 8 (enacting House Bill (HB) 2795 (1985)).

accessing a computer in the course of committing a theft not constitute use or access for the purpose of committing theft? As noted, the Court of Appeals effectively concluded that a person lacks that purpose when their use or accessing of a computer is merely "incidental," and not the "direct, necessary means" of committing the theft. See Azar, 318 Or App at 737. As the following indicates, our ultimate conclusion in this case aligns with the implicit reasoning of the Court of Appeals—as well as that of the dissenting opinion in this court—which we understand to be that, despite the facially broad language of ORS 164.377(2)(c), the legislature did not intend that provision to apply as expansively as its plain terms could possibly reach. However, despite our agreement on that point, we ultimately disagree as to what limitation applies.

We turn to the relevant terms. Some of those terms are defined within the computer crime statute itself. Those include "access," which 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." ORS 164.377(1)(a). At a minimum, conducting sales transactions through eBay necessarily entails "communicat[ing]" with "a computer, computer system or computer network," and defendant does not contend that he did not "access" eBay when he used that platform to market items that he believed to be stolen. Similarly, although "uses" is not statutorily defined, that term too is quite broad and, in isolation, would seem to capture availing oneself of an online service, such as eBay. The various meanings of "use" include "to carry out a purpose or action by means of: make instrumental to an end or process: apply to advantage: turn to account: UTILIZE." Webster's Third New Int'l Dictionary 2524 (unabridged ed 2002); see also PGE v. Bureau of Labor and Industries, 317 Or 606, 611, 859 P2d 1143 (1993) (explaining that "words of common usage typically should be given their plain, natural, and ordinary meaning"). Thus, the term "uses," like the term "access," might be understood to apply to defendant's alleged conduct: One who employs eBay to conduct online sales "uses," for at least that purpose, eBay and, by extension, the computer, computer system, or computer network on which eBay operates.

And, if all that ORS 164.377(2)(c) required were that a person use or access a computer for any purpose bearing some nonincidental connection to an act of theft, then our inquiry would likely be complete. However, even an initial examination of the statutory context suggests certain parameters around those otherwise broad terms. "A statute's context includes, among other things, its immediate context—the phrase or sentence in which the term appears and its broader context, which includes other statutes on the same subject." Shepard Investment Group LLC v. Ormandy, 371 Or 285, 290, 533 P3d 774 (2023). As noted above, the various meanings of "use" include "to carry out a purpose or action by means of," Webster's at 2524, and ORS 164.377(2)(c) expressly states which "purpose" brings the "use" of a computer within the statute's coverage: "the purpose of \*\*\* [c]ommitting theft \*\*\*." Moreover, given the legislature's chosen phrasing—"uses \*\*\* for the purpose of," rather than, for example, "uses in the course of"—the legislature may have sought to limit the application of ORS 164.377(2)(c) to uses that in fact "carry out" that purpose, and not any use that in some way facilitates "theft." Under that reading, defendant's conduct would constitute computer crime only if the act itself of using eBay constituted a theft within the meaning of ORS 164.377(2)(c).

That qualifying language in ORS 164.377(2)(c)—"for the purpose \*\*\* of "[c]ommitting theft"—does not independently shed much light on the intended scope of the statute. The word "purpose" commonly means "something that one sets before [themselves] as an object to be attained: an end or aim to be kept in view in any plan, measure, exertion, or operation: DESIGN." Webster's at 1847. So, for defendant's conduct of using or accessing the eBay platform to constitute computer crime in this case, he must at least have had a certain objective in mind, specifically, "[c]ommitting theft." But, as noted above, the word "use" itself appears to imply purpose-driven conduct, and the fact that the state must prove a specific purpose does not provide any further indication whether having

<sup>&</sup>lt;sup>8</sup> As noted, the plain meanings of "use" include "to carry out a purpose," *Webster's* at 2524, and, in turn, "carry out" conveys the idea of bringing something to its conclusion, *see id.* at 344 (meanings of "carry out" include "to bring to a successful issue" and "to continue to an end or stopping point").

that objective is sufficient to render a "use" of a computer "computer crime" or, if not, what else the state must prove to establish a violation of ORS 164.377(2)(c).

"Committing," in turn, means, as pertinent here, to engage in specific conduct that the law makes punishable as a crime. See Black's Law Dictionary 248, 334 (5th ed 1979) (defining "commit" as "[t]o perpetrate \*\*\* a crime" and "crime" as a "positive or negative act in violation of penal law"); see also DCBS v. Muliro, 359 Or 736, 746, 380 P3d 736 (2016) ("When a term is a legal one, we look to its established legal meaning as revealed by, for starters at least, legal dictionaries." (Internal quotation marks omitted.)) And as ORS 164.377(2)(c) expressly provides, the relevant crime for purposes of our analysis is "theft." Again, however, nothing in the word "[c]ommitting" or its immediate context tells us whether ORS 164.377(2)(c) contemplates anything more than facilitating a theft by using or accessing a computer, whether it be the extraction of something from that computer (as defendant argues), the successful completion of some form of theft—even if, as here, the theft involves property wholly external to any computer—or the realization of some other theft-related goal.

That brings us, finally, to the term "theft," which raises one of the parties' central disputes in this case: whether "theft," as used in ORS 164.377(2)(c), is intended to encompass the various meanings of theft found in other parts of the Criminal Code (as the state contends), or, instead, "theft" has a narrower meaning when it comes to computer crime, one that (as defendant argues) limits ORS 164.377(2)(c) in a way that excludes theft by receiving, the form of theft prosecuted in this case. For the reasons that follow, we conclude that, under ORS 164.377(2)(c), "theft" has the same meaning as it does elsewhere in the property crimes chapter of the Criminal Code. As we also explain, however, that conclusion does not resolve the ultimate question raised by defendant's appeal, namely, whether that provision reaches his specific conduct in this case.

We begin by observing, as defendant emphasizes, that ORS 164.377 does not define "theft," despite defining many of the other terms that the statute uses. See, e.g., ORS

164.377(1)(a) (defining "access"); ORS 164.377(1)(b) (defining "computer"); ORS 164.377(1)(j) (defining "property"). Nor does it expressly incorporate the meaning of that term from the theft section of the property crimes chapter, including the offenses identified in ORS 164.015 (stating that one "commits theft" by, among other things, "commit[ting] theft by receiving as provided by ORS 164.095"). Defendant relies on those contextual clues as evidence that the legislature intended for "theft" in ORS 164.377(2)(c) to have its plain and ordinary meaning, which he argues is "an unauthorized taking." See Webster's at 2369 (defining "theft" as "the act of stealing; \*\*\* the felonious taking and removing of personal property with intent to deprive the rightful owner of it" or "the taking of property unlawfully (as by robbery, embezzlement, fraud)"); see also The American Heritage Dictionary of the English Language 1334 (1st ed 1969) (defining "theft" as "the act or an instance of stealing; larceny"). Under that reading, "theft" would seem not to include theft by receiving—at least as alleged here—because that crime does not appear to require a "taking." See ORS 164.095 ("A person commits theft by receiving if the person receives, retains, conceals or disposes of property \*\*\*.").

The state responds that the legislature had no need to define "theft" for purposes of the computer crime statute, because that term already had a well-defined legal meaning in Oregon when it enacted that law: the meaning found in ORS 164.015, which is not limited to theft by taking. And because the two statutes appear in the same chapter of the Criminal Code, the state would rely on this court's "general assumption" that "the legislature intended the same word to have the same meaning throughout related statutes unless something in the text or context of the statute suggest a contrary intention." Village at Main Street, Phase II v. Dept. of Rev., 356 Or 164, 175, 339 P3d 428 (2014); see also State v. Cloutier, 351 Or 68, 99, 261 P3d 1234 (2011) (so stating). The state also compares the computer crime statute to ORS 164.235, which narrows the scope of "theft" to "theft by a physical taking" in prohibiting possession of burglar's tools. It argues that, because the legislature did not similarly narrow the scope of "theft" in the computer crime statute, we should not narrow it ourselves as a matter of statutory construction. because that would violate our duty under ORS 174.010 to avoid "insert[ing] what has been omitted" by the legislature.

We conclude that "theft" as used in ORS 164.377(2)(c) encompasses, as a general matter, those offenses identified as theft in ORS 164.015, including theft by receiving. The legislature enacted ORS 164.377 in 1985, Or Laws 1985, ch 537, § 8. over a decade after it "eliminate[d] the traditionally distinct crimes of larceny, larceny by trick, embezzlement, obtaining property by false pretenses, receiving stolen property and extortion and \*\*\* consolidate[d] them into one crime called 'theft.'" Commentary to Criminal Law Revision Commission Proposed Oregon Code, Final Draft and Report § 123, 132 (July 1970); see also Or Laws 1971, ch 743, § 123 (providing five circumstances in which a person commits "theft"). Thus, as the state notes and the Court of Appeals reasoned, "theft" had a well-established legal meaning when the legislature enacted the computer crime statute, a meaning not limited to theft by taking. Moreover, House Bill (HB) 2795 (1985), which included the computer crime provisions now compiled at ORS 164.377, also contained provisions amending the theft provisions of ORS chapter 164. Accordingly, we can safely assume that the legislature was aware of the meaning of "theft" in ORS 164.015 when it enacted ORS 164.677(2)(c). See Jack L. Landau, Oregon Statutory Construction, 97 Or L Rev 583, 638 (2019) (noting that "'context' for a statute is essentially anything of which the legislature could have been aware at the time of a given enactment"). Additionally, ORS 164.015 and ORS 164.377 are closely related, in that they both address the wrongful interference with property rights of others and appear in the same chapter of the Criminal Code. As a result, unless something else about the text or context of either statute suggests a contrary intention, we assume that the legislature intended "theft" to have the same meaning in both. See State v. Colgrove, 370 Or 474, 483, 521 P3d 456 (2022) (stating that principle).

<sup>&</sup>lt;sup>9</sup> We need not determine whether "theft" as used in ORS 164.377(2)(c) also encompasses forms of theft defined by other statutes, including ORS 164.125 (theft of services) and ORS 164.162 (mail theft). Further, although we conclude that, in theory, ORS 164.377(2)(c) encompasses theft by receiving, ORS 164.095, which is a form of theft identified in ORS 164.015, we discuss below whether, as a practical matter, it was intended to capture conduct of the sort admitted by defendant.

In our view, nothing suggests a contrary intention. Defendant contends otherwise. He offers various contextual clues that he asserts support the view that "theft" in ORS 164.377(2)(c) has a meaning independent of its statutory definitions, one limited to the unauthorized taking of property from a computer. Among other things, defendant argues that, because ORS 164.377(2)(a) and (2)(b) criminalize conduct analogous to theft by deception, it would be illogical for ORS 164.377(2)(c) to criminalize that same conduct, which would result if we accepted the state's meaning of "theft."

We are not persuaded. It is true that, in addition to prohibiting using or accessing a computer for purposes of committing theft, ORS 164.377(2) also proscribes two other "theft-like" forms of conduct:

"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; [or]
- "(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises[.]"

And, as defendant points out, both ORS 164.377(2)(a) and (2)(b) proscribe conduct analogous to theft by deception, which is both separately defined in ORS 164.085<sup>10</sup> and one of the forms of theft listed in ORS 164.015. Defendant reasons that, if the legislature had intended for ORS 164.377(2)(c) to capture those other forms of theft, it would have had no

<sup>&</sup>lt;sup>10</sup> ORS 164.085(1) provides, in part:

<sup>&</sup>quot;A person, who obtains property of another thereby, commits theft by deception when, with intent to defraud, the person:

<sup>&</sup>quot;(a) Creates or confirms another's false impression of law, value, intention, or other state of mind that the actor does not believe to be true:

<sup>&</sup>quot;(b) Fails to correct a false impression that the person previously created or confirmed; [or]

**<sup>&</sup>quot;\*\*\***\*\*

<sup>&</sup>quot;(e) Promises performance that the person does not intend to perform or knows will not be performed."

reason to separately define computer crime to include the conduct proscribed by ORS 164.377(2)(a) and (b).

We acknowledge that, as defendant observes, there would appear to be considerable overlap between the conduct that paragraphs (2)(a) and (b) proscribe and the conduct that paragraph (2)(c) encompasses if, as the state argues, "theft" in paragraph (2)(c) wholly incorporates ORS 164.015. Notably, however, paragraphs (2)(a) and (b) are not entirely coextensive with any form of theft listed in ORS 164.015. Among other differences, paragraph (2)(a) prohibits simply devising a fraudulent scheme—whereas theft by deception requires actually obtaining property—and paragraph (2)(b) applies to fraudulently obtaining services, not just property, and therefore is broader than theft by deception and any other form of theft defined in ORS 164.015.11 Moreover, as we have recognized, "the fact that a proposed interpretation of a statute creates some measure of redundancy is not, by itself, necessarily fatal. Redundancy in communication is a fact of life and of law." Cloutier, 351 Or at 97; see also State v. Fonte, 363 Or 327, 343, 422 P3d 202 (2018) (noting that "it may be possible for the same person to commit acts that constitute more than one type of theft under ORS 164.015"). And here, given the broad scope of the computer crime statute, we find it likely that any perceived redundancy is the product of the legislature's effort to enact a comprehensive statute, and not evidence that the legislature intended for ORS 164.377 including its reference to "theft"—to be wholly self-contained.

In sum, the text and context of ORS 164.377(2)(c) do not support defendant's narrow construction, one that would limit the scope of that provision to using or accessing a computer for the purpose of taking something from that or another computer. However, that conclusion does not answer the question at the core of this case: When does using or accessing a computer in the course of committing theft amount to using or accessing the computer "for the purpose of \*\*\* [c]ommitting theft"? Is it whenever the use or access facilitates a theft? Is it when, as the Court of Appeals

<sup>&</sup>lt;sup>11</sup> A separate theft statute, ORS 164.125 (theft of services), *does* cover obtaining services by deception, but the state has not argued that theft of services is another form of theft covered by ORS 164.377(2)(c), nor has that statute been offered as additional context for the computer crime statute.

concluded, "the person's use or access[ing] of a computer is the direct, necessary means by which the person accomplishes" a theft? See Azar, 318 Or App at 737. Or did the legislature intend some different scope when it enacted the computer crime statute? Because our assessment of the text and context of ORS 164.377(2)(c) leaves open the question whether that provision encompass defendant's conduct, any legislative history that sheds light on that question could inform our final conclusion regarding the intended scope of the statute. Thus, we now turn our attention to whether anything in the legislative history of ORS 164.377 is helpful in that regard.

### B. The Legislative History of ORS 164.377

This court recognized in *Nascimento*, 360 Or at 42, that the legislature's primary concern in adopting the computer crime provisions of HB 2795 was computer "hacking" the unauthorized use or accessing of computers or the data they contained. Defendant relies on that point to support his argument that we should narrowly construe what it means to "use" or "access" a computer system for purposes of committing theft. Although the state agrees that the primary concern of the legislature that established the offense of computer crime was hacking, it attaches less significance to that point than defendant. The state contends that the 1985 legislative history pertinent to that conduct focused on what later became ORS 164.377(4) (prohibiting unauthorized use or accessing of computers and their contents) and ORS 164.377(3) (prohibiting unauthorized alteration, damage, or destruction of same), and not ORS 164.377(2), the provision at issue in this case. The state further argues that, despite having the principal goal of addressing computer hacking, the legislature may well have had other objectives in mind

whether, by requiring that the use of a computer be the "direct, necessary means" of accomplishing a theft (and not merely "incidental"), that court intended to require more than a causal relationship between the use and the result, and, if so, what degree of necessity would suffice. We note that, although defendant's use of eBay may well have enhanced his ability to market the spoils of his crimes—as well as to avoid apprehension—it is less than obvious how eBay was "necessary," at least if, by "necessary," the Court of Appeals meant that defendant could not have committed theft by receiving without his reliance on eBay, or on any computer technology for that matter.

when it passed HB 2795. See Nascimento, 360 Or at 44 (noting that the "legislature may and often does choose broader language that applies to a wider range of circumstances than the precise problem that triggered legislative attention" (Internal quotation marks omitted.)).

Having reviewed the legislative history of the computer crime statute, we conclude that it does not support as expansive an application of ORS 164.377(2)(c) as the Court of Appeals' opinion would allow. When it was first introduced in the legislature, HB 2795 was directed at the theft of television cable services and included text amending the existing theft of services statute, ORS 164.125. Tape Recording, House Committee on Judiciary, Subcommittee 1, Apr 11, 1985, Tape 425 (statement of Rep Randy Miller); see also Or Laws 1985, ch 537, §§ 1-7. The "computer crime" text came later at the request of the American Electronics Association and was introduced as an amendment to HB 2795 by representatives of General Telephone Company of the Northwest (General Telephone). Tape Recording, House Committee on Judiciary, Subcommittee 1, May 6, 1985, Tape 576 (statement of Chair Richard Springer).

Sterling Gibson, a security officer for General Telephone, testified that the purpose of the amendment was to "prevent people from calling into someone's computer" and manipulating a business's data. *Id.* When Chairperson Springer asked whether the existing theft of services statute already criminalized the conduct described in the amendment, Gibson responded that "a lot of times it may not be theft[.]" Id. He continued that, even though "it may be construed as theft, \*\*\* the actual act was the manipulation, or changing of documents" that are "vital" to an organization's survival. Id. He further explained that that conduct "isn't theft, that's manipulation" and later reiterated that "we're not necessarily dealing with the theft of something, [we're dealing with] manipulation." Id. Gibson said that, in his experience, when law enforcement sought to prosecute acts of computer hacking, they had found the theft of services statutes "too broad" and "not useable." Id.

Echoing Gibson's testimony, Legislative Counsel Leslie Hammond later explained to the full House Committee

on Judiciary that HB 2795 was intended to address "the idea of people who use their computers or instruments to get access to computer systems or networks and then gain by using the information or program that belongs to someone else." Tape Recording, House Committee on Judiciary, HB 2795, May 13, 1985, Tape 613, Side A; see also id. (explaining that the bill makes "it a crime for people to access a computer system to which they don't belong or to destroy or damage the property"). Hammond also prepared a staff summary for the committee explaining that the bill was intended to address the problem of people "using computers to break into computer systems to steal information or programming." Staff Measure Summary, House Committee on Judiciary, HB 2795 (1985). The bill passed the committee without further discussion. Tape Recording, House Committee on Judiciary, HB 2795, May 13, 1985, Tape 613, Side A.

That legislative history readily supports what is undisputed here: HB 2795's proponents were most concerned with the sort of conduct criminalized by subsections (3) and (4) of ORS 164.377, which explicitly address the protection of computers and their contents from intrusion. Admittedly less clear is what conduct the legislature was targeting when it chose to also criminalize using or accessing computers for the purposes of "[c]ommitting theft," ORS 164.377(2)(c). But what evidence there is in the legislative history indicates to us that, like subsections (3) and (4), ORS 164.377(2)(c) was enacted to protect computers and their contents; it was not enacted to provide broad protection from computers and their potential value as instruments of crime, whether or not a person's crime bore any relationship to the computer used or the contents accessed. In other words, the evidence suggests a more limited understanding of ORS 164.377(2)(c), one that, like computer hacking, was focused on computers, their contents, and the access that computer technology could give would-be thieves to electronically stored or managed data and services. That evidence includes (1) the measure summary's identified concern that individuals were stealing "information or programming" from computers, Staff Measure Summary, House Committee on Judiciary, HB 2795 (1985); (2) legislative counsel's explanation that the underlying concern was "people who use their computers or

instruments to get access to computer systems or networks" and "using the information or program that belongs to someone else," Tape Recording, House Committee on Judiciary, HB 2795, May 13, 1985, Tape 613, Side A; (3) proponents' accounts of electronically stored business data being manipulated or altered; and (4) the fact that HB 2795's original objective was to address those who were surreptitiously acquiring cable television services—an electronically distributed commodity—for free. We turn next to what that limitation is; that is, what qualifies as "use" or "access"?

# C. What qualifies as "use" or "access" under ORS 164.377 (2)(c)?

As we have just discussed, the legislative history suggests that the legislature that enacted ORS 164.377(2)(c) never intended that provision to reach every act of theft that somehow involved using or otherwise accessing a computer. Rather, the legislature's overriding goal was to stop people from getting into computer systems for nefarious purposes, as Judge Pagán observed. That understanding suggests the need for some limiting principle as to what constitutes use or access for purposes of theft under the statute. We are cognizant that our understanding of the legislative history can only inform our construction of the legislatively enacted text; it cannot justify the adoption of limitations that the text of ORS 164.377(2)(c) cannot support. See ORS 174.010 (in construing statutes, courts may not insert what the legislature has omitted). For that reason, we have already rejected defendant's argument that "theft" as used in ORS 164.377(2)(c) is limited to taking things from a computer the only permissible limitation on what constitutes a qualifying theft is that the person must have "use[d]" or "access[ed]" a computer "for the purpose of" committing it. 13 And, based on our review of the text and context of ORS 164.377(2)(c), we have also concluded that a qualifying theft may take any one of the various forms of theft listed under ORS 164.015, including, at least arguably, theft by receiving. However, our review of the legislative history persuades us—as the

<sup>&</sup>lt;sup>13</sup> Indeed, nothing in the statute even limits its scope to crimes completed entirely within the confines of a computer system. We address the implications of that fact below.

Court of Appeals seems to have been persuaded by other considerations—that not every act of using or accessing a computer in the course of engaging in theft qualifies as use or access "for the purpose of \*\*\* [c]ommitting theft."

Before determining which acts do qualify, we first note that we disagree with the Court of Appeals' test, which we understand to be that the person's use or accessing of a computer must be the "direct, necessary means" by which the person committed a theft and that the use or access must be more than "incidental." Azar, 318 Or App at 738. For one thing, that test does not adequately reflect the purpose for which the legislature enacted the computer crime statute, as reflected in its legislative history. And for another, the Court of Appeals' test is, in our view, unworkable. That is, "direct [and] necessary" is susceptible to myriad meanings, and nothing in the Court of Appeals' decision explains which meaning applies.<sup>14</sup> Notably, although defendant in this case chose to employ computer technology in the course of his criminal conduct, it is far from apparent that he could not have committed the underlying offense without using eBav. as the crime of "fencing" stolen property was committed far before the advent of the internet or of electronics of any sort. Thus, at least to the panel majority in the Court of Appeals, "necessary" must mean something less than truly "necessary," but what may qualify is far from clear. See Webster's at 1511 (including, among other definitions of "necessary," the ideas of being absolutely required, essential, or indispensable).

Relatedly, the Court of Appeals' requirement that a person's use or access of a computer be more than

<sup>14</sup> The word "direct" is relatively clear and, when used in the term "direct means," appears to mean "leading by the \*\*\* shortest way to a point or end" and suggests immediacy between the use or accessing and its objective. See Webster's at 640 (defining the adjectival form of "direct"). But when such use or accessing might be "necessary" is far less clear. It may require a merely practical necessity, such that it suffices if the person's decision to use a computer bears a "but for" relationship with a prohibited outcome—e.g., "if he had not used a computer, he would not have committed a theft"—or, instead, it may require that computer technology play an essential or indispensable role in the commission of the person's crime, such that the person could not have committed the charged offense had they not had been able to use or access a computer. See id. at 1511 (defining "necessary" to include "that cannot be done without: that must be done or had: absolutely required: ESSENTIAL, INDISPENSIBLE").

"incidental" does not improve matters. There is no way to anticipate when a particular prosecutor, jury, or court will view one or another use of computer technology as merely "incidental." We therefore do not share the Court of Appeals' optimism that its test is sufficient to "allow a person of ordinary intelligence to understand the scope of what is prohibited" so as to alleviate defendant's vagueness concerns. <sup>15</sup> See Azar, 318 Or App at 738. Thus, although we agree with the Court of Appeals that it is appropriate to articulate the intended scope of ORS 164.377(2)(c), we disagree with its ultimate determination as to what that scope is.

We, therefore, describe the scope of ORS 164.377(2)(c) differently, in a way that is both workable—that is, understandable and predictable—and true to the legislature's principal goal in enacting the computer crime statute, specifically, to deter the targeting of computers and the data they contain. In so doing, however, we find it significant that the legislature also had in mind those who were using technology as a means of surreptitiously gaining access to services they could not otherwise access—specifically, free cable television services. Thus, in determining the scope of ORS 164.377(2)(c), we allow for the possibility that the legislature intended for "computer crime" to capture at least some conduct that reaches beyond the strict confines of any computer, computer system, or computer network. Synthesizing those principles, we conclude that, for a person's use or accessing of a computer to be "for the purpose of \*\*\* [c]ommitting theft" under ORS 164.377(2)(c), the theft at issue must either interfere with another's property rights in—or electronically located on—a computer, computer system, or computer network, or depend on such computer technology as the means

<sup>&</sup>lt;sup>15</sup> Like the Court of Appeals majority, the dissent in this court appears to recognize that, without some limiting principle, ORS 164.377(2)(c) has the potential to capture significantly more conduct than the legislature intended. 372 Or at 189-90 (Bushong, J., dissenting) (recognizing that some computer uses would likely be too "incidental" to be what legislature intended to reach; observing that the Court of Appeals described defendant's computer use as the "principal mechanism" of fencing operation). But neither the Court of Appeals majority nor the dissent here suggests that, under ORS 164.377(2)(c), a person's computer use must be the "principal" means by which they accomplish their theft. Thus, like the Court of Appeals, the dissenting opinion in this court offers only the unworkable standard of computer use that is not "incidental."

of accessing the thing that the person seeks to unlawfully obtain.

## D. ORS 164.377(2)(c) does not apply to defendant's conduct.

Turning to the application of that standard to this case, we emphasize that, despite the limits that our construction may impose on the computer crime statute, ORS 164.377 (2)(c) remains broadly applicable. In addition to protecting a broad range of property interests existing—physically or in electronic form—on computers, computer systems, or computer networks, we have also construed that provision to capture forms of theft that rely on the special access to protected interests that computer technology might allow. Thus, although we need not for purposes of this case delineate the full range of conduct that ORS 164.377(2)(c) might reach, we observe, for example, that it would necessarily capture such conduct as manipulating computerized bank records or other conduct that takes place via a computer but that affects interests existing outside the digital realm. That being said, even with that rather broad understanding of what it means to access or use a computer for purposes of theft, it does not encompass defendant's conduct here.

In this case, defendant does not dispute that his conduct in selling purportedly stolen property on eBay constituted theft by receiving. That conduct, however, did not interfere with any interest that eBay or anyone else had in a computer, computer system, or computer network, or in any electronic contents thereof. Nor did defendant use eBay or any other computer technology to gain access to property that he sought to unlawfully obtain—to the extent that anyone actually accessed the purportedly stolen merchandise at issue in this case, it is apparent that they did so by physically entering the retail locations where such items were sold. Under those circumstances, defendant's conduct cannot have constituted computer crime.<sup>16</sup>

<sup>&</sup>lt;sup>16</sup> The dissent suggests that there is an incongruity between suggesting that it might well be computer crime for a person to obtain the fruits of theft through eBay, but not to dispose of them through the same platform. 372 Or at 190-91 (Bushong, J., dissenting). Even assuming that the dissent's premise is correct, we disagree that our construction leads to incongruous results. Much like the crime of burglary focuses on the entry or remaining upon premises to commit a crime, not on the departure from premises with the fruits of that crime, the legislature's

#### III. CONCLUSION

We conclude that a person does not violate ORS 164.377(2)(c) merely by permissibly using an online platform such as eBay in the course of committing a theft, whether theft by receiving or some other form of theft. Although ORS 164.377.(2)(c) broadly prohibits using or accessing a computer to commit theft, the theft at issue must either (1) interfere with another's protected interests in either the computer or its contents, or (2) depend on computer technology to gain access to whatever it is that the person seeks to unlawfully obtain. As alleged in this case, defendant's conduct of theft by receiving, while conducted on a computer, did not relate to anything about the computer he used or its contents, and defendant did not depend on a computer to gain access to the purportedly stolen property. The trial court therefore erred in denying defendant's motion for judgment of acquittal as to the allegations of computer crime. We reverse the trial court's denial of defendant's motion for judgment of acquittal, reverse, in part, the decision of the Court of Appeals, and remand for further proceedings.

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

## BUSHONG, J., dissenting.

Defendant used a computer to sell stolen merchandise on eBay, obtaining money from those sales through PayPal accounts that he accessed using a computer. The majority opinion concludes that defendant's use of a computer to commit those crimes does not constitute "computer crime" in violation of ORS 164.377 because the legislative

focus in enacting the computer crime statute was on the use of computers as means of—and protecting computers against—intrusion. 372 Or at 180-81 (discussing that focus).

¹ eBay is an internet platform that allows "private sellers to list goods they wish to sell, either through an auction or at a fixed price." eBay Inc. v. MercExchange, LLC, 547 US 388, 390, 126 S Ct 1837, 164 L Ed 2d 641 (2006). The eBay website processes purchasers' payments using PayPal, which is an internet service that allows "business[es] or private individual[s] to send and receive payments" online. Comb v. PayPal Inc., 218 F Supp 2d 1165, 1166 (ND CA 2002). Sellers can transfer funds processed through PayPal into their own bank accounts. Id.

history suggests "a more limited understanding" of what conduct the legislature intended to prohibit when it adopted the computer crime statute in 1985. I disagree with that conclusion. In my view, the majority opinion misreads the legislative history to reach a result that is contrary to the text of the statute. Accordingly, I respectfully dissent.

As the majority opinion points out, a person commits computer crime in violation of ORS 164.377(2)(c) if the person knowingly "accesses" or "uses" a computer, computer system, or computer network, for the purpose of "committing theft."2 The majority opinion explains that "theft" had a well-established meaning when the computer crime statute was enacted and that theft by receiving as defined in ORS 164.015 was included in the conduct covered by the statute. I agree with that reading of the statute's text. But the majority opinion goes astray when it interprets "access" or "use" narrowly to cover only conduct that "either interfere[s] with another's rights in—or electronically located on—a computer, computer system, or computer network, or depend[s] on such computer technology as a means of accessing the thing that the person seeks unlawfully to obtain." 372 Or at 183-84.

That interpretation finds no support in the text or context of the statute, and the majority opinion does not suggest that it does. Instead, the majority opinion relies on the legislative history to support its narrow interpretation of the statutory text. But that interpretation conflicts with the plain meaning of the text, and we have long recognized that "there is no more persuasive evidence of the intent of the legislature than the words by which the legislature undertook to give expression to its wishes." *State v. Gaines*, 346 Or 160, 171, 206 P3d 1042 (2009) (internal quotations marks omitted).

The words used here—to "access" and "use"—a computer to commit theft are not limited by any words suggesting that the "rights" a person may have obtained or

<sup>&</sup>lt;sup>2</sup> The computer crime statute defines "computer," "computer system," and "computer network." *See* ORS 164.377(1)(b) - (d). Defendant does not dispute that, by engaging eBay and PayPal online, he accessed a computer, a computer system, or a computer network.

interfered with when the person used or accessed a computer must be "in or located on" a computer to constitute computer crime. Nor are there any words limiting the reach of the statute to using computer technology "as a means of accessing the thing that the person seeks unlawfully to obtain." Instead, paragraph (1)(a) of the computer crime statute broadly defines "access" to mean "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." ORS 164.377(1)(a) (emphasis added). The majority opinion interprets that definition to include a limitation that the legislature omitted, contrary to accepted rules of statutory interpretation. See ORS 174.010 (in interpreting statutes, courts may not "insert what has been omitted").

The majority opinion's interpretation also overlooks the fact that subsection (2) of the computer crime statute expressly states what *the purpose* of using or accessing a computer must be for the conduct to be considered computer crime. That provision states that a person commits computer crime when the person knowingly uses or accesses a computer "for the purpose of" (among other things) "[c] ommitting theft." ORS 164.377(2)(c). The statute does not say that, to constitute computer crime, a person must use or access a computer for "the purpose of" obtaining or interfering with rights "in or located on" a computer, nor does it say that the thief's purpose must be to "access the thing that the person seeks unlawfully to obtain." But that is the effect of the majority opinion's interpretation.

Moreover, although the legislative discussions leading to the enactment of the statute focused primarily on the problem of "computer hacking," as the majority opinion points out, the legislature ultimately adopted a statute that broadly covers conduct beyond "hacking." That commonly occurs during the legislative process. See, e.g., State v. Nascimento, 360 Or 28, 44, 379 P3d 484 (2016) (recognizing that the legislature "'may and often does choose broader language that applies to a wider range of circumstances than the precise problem that triggered legislative attention" (quoting South Beach Marina, Inc. v. Dept. of Rev., 301 Or 524, 531, 724 P2d 788 (1986))); Hamilton v. Paynter, 342 Or

48, 55, 149 P3d 131 (2006) ("[T]he statutory text shows that, even if the legislature had a particular problem in mind, it chose to use a broader solution."). That does not mean that we must interpret the statute "in the broadest sense that the text might permit." *Nascimento*, 360 Or at 44. Rather, "'legislative history would be a basis on which we appropriately may construe the text more narrowly'" if that history "reveals that the legislature had a narrower understanding of the term in mind, and if that narrower meaning is consistent with the text, even if not compelled by it[.]'" *Id*. (quoting *State v. Walker*, 356 Or 4, 17, 333 P3d 316 (2014)).

Here, the words used in the computer crime statute—"access" and "use"—broadly apply to a wider range of circumstances than the hacking problem that triggered the legislative enactment in 1985. As explained above, the "narrower meaning" adopted by the majority opinion is inconsistent with the text enacted by the legislature, and as explained below, there is no evidence in the legislative history that the legislature had a narrower understanding of those terms in mind when it included that text in the computer crime statute. In fact, if the legislature were to reconsider the computer crime statute in 2024 and wanted to be certain that the statute covered this type of conduct—using a computer to access eBay to sell stolen goods for payments processed through PayPal—it would not need to amend the statute at all. The words in the existing statute—"using" or "accessing" a computer, computer system, or computer network to commit theft (including theft by receiving)—work just fine to encompass that conduct.

The legislative history confirms that the legislature did not have a narrower meaning in mind when it defined computer crime to include any use or access of a computer to commit theft. The widespread use of computer technology was in its early stages when the bill that became ORS 164.377 was enacted in 1985. When the need for a computer crime bill was initially discussed during a 1981 hearing of the Senate Committee on Justice, Senator Kulongoski asked whether it would be "a fair statement to say that the purpose of the bill is not so much necessarily [the] problems [of] today, as problems that could arise as we move into

an age where we utilize computers more and more[.]" Tape Recording, Senate Committee on Justice, SB 439, Mar 25, 1981, Tape 83, Side B (statement of Sen Ted Kulongoski). Two years later, one witness told the Senate Committee on Judiciary that they were "living during a period of history which has seen an incredible explosion of technological advances," and that "[e]very indicator predicts the 1980s to be a decade of overwhelming technological change, probably exceeding in impact all the years preceding them. In all likelihood, in the next very few years 'a computer in every home' will become a reality." Testimony, Senate Committee on Judiciary, SB 149, Feb 23, 1983, Ex A (statement of Terry Hippenhammer). That witness further explained that colleges and universities across the country were considering requiring all students to own a microcomputer and he broadly described the "potential abuse" that could occur. Id. Another witness described computer crime as "the crime of the future that is rapidly becoming the crime of the present." Testimony, Senate Committee on Judiciary, SB 149, Feb 23, 1983, Ex B (statement of Jim Mattis).

Thus, by the time the computer crime legislation passed in 1985, the legislature was aware that its understanding of how computers could be "used" or "accessed" to commit crimes was limited and that the technology was changing rapidly. Instead of enacting a law that narrowly addressed "hacking" and related problems that were brought to the legislature's attention at the time, the legislature chose to broadly define "computer crime" to include "using" or "accessing" a computer for the purpose of committing theft, regardless of how the computer was used to commit the theft, the nature of the information or property rights obtained or affected by a wrongdoer's use or access of a computer, or the wrongdoer's ability to "otherwise access" the property without using a computer.

That broad wording does not mean that the legislature necessarily intended "computer crime" to include using a computer *in any way* to facilitate the commission of a crime. Some uses are so incidental—sending an email to confirm the time and place of a meeting before committing a theft or using the internet to locate a store to shoplift, for

example—that it is unlikely that the legislature would have considered them to rise to the level of "computer crime." But where a defendant's use of a computer is integral to the operation of a criminal enterprise—the Court of Appeals described defendant's use of a computer in this case as "the principal mechanism for his extensive fencing operation," *State v. Azar*, 318 Or App 724, 738, 508 P3d 668 (2022)—I would conclude that the conduct is covered by the computer crime statute.<sup>3</sup>

That conclusion is consistent with a common-sense understanding of what it means to "access" or "use" a computer for the purpose of committing a crime. The defendant in this case built a criminal enterprise centered on using a computer to access eBay and PayPal to facilitate his illegal fencing operation. The eBay website allowed defendant to market stolen goods to millions of internet users, something he could not have done without the website and a computer to access it. The PayPal platform allowed defendant to receive payments for those stolen goods without risk, something he could not have done without that internet platform.<sup>4</sup> And given the scope of defendant's fencing operation, using eBay and PayPal instead of selling stolen goods in person may have reduced the risk of attracting the attention of neighbors and law enforcement.

Under the majority opinion's test, using a computer "as a means of accessing the thing that the person seeks unlawfully to obtain" would be a computer crime covered by the statute. 372 Or at 183-84. Thus, under that test, using a computer to *obtain* stolen goods as part of an illegal fencing operation would be a computer crime but using a computer to *sell* stolen goods as part of the same criminal enterprise

<sup>&</sup>lt;sup>3</sup> The majority opinion and this dissenting opinion attempt to discern how the legislature intended a statute enacted in 1985 would apply to present day circumstances. Given the evolution of our understanding of how computers can be used to commit crimes, further legislation to clarify what was intended to be a "computer crime" could remove any uncertainty in this area.

<sup>&</sup>lt;sup>4</sup> Without PayPal or a similar internet payment platform, defendant would have to receive payment via the mail—which by its nature involves some risk of loss—or in person. A person receiving payment for stolen goods in those ways runs the risk that a check may bounce, that counterfeit currency may be given, or that the buyer might choose to rob the seller instead of paying for the stolen goods.

would not be a computer crime. The majority opinion cites no evidence in the statutory text, context, or legislative history for such a distinction, nor does it offer any good reason why the legislature would intend to criminalize as computer crime using a computer to obtain stolen goods but not to sell them.

Defendant's use of a computer to conduct an illegal fencing operation—which is theft by receiving under Oregon law—falls squarely within the conduct that is prohibited by the computer crime statute. The majority opinion's contrary conclusion based on its narrow interpretation of the statute is, in my view, wrong. Accordingly, I respectfully dissent.

Garrett, J., and Balmer, S.J., join in this dissenting opinion.