IN THE SUPREME COURT OF THE
STATE OF OREGON

STATE OF OREGON,
Respondent on Review,
v.
CATRICE PITTMAN,
Petitioner on Review.
(CC 16CN03799) (CA A162950) (SC S067312)

En Banc

On review from the Court of Appeals.*

Argued and submitted September 15, 2020.

Ernest G. Lannet, Chief Defender, Office of Public Defense Services, Salem, argued the cause and filed the briefs for petitioner on review. Also on the briefs was Sarah Laidlaw, Deputy Defender.

Jonathan N. Schildt, 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.

Kendra M. Matthews, Boise Matthews Ewing LLP, Portland, filed the brief for *amici curiae* ACLU of Oregon, American Civil Liberties Union, and Electronic Frontier Foundation. Also on the brief was Kelly Simon, ACLU Foundation of Oregon.

Franz H. Bruggemeier, Portland, filed the brief for *amici curiae* Oregon Justice Resource Center and Laurent Sacharoff.

WALTERS, C. J.

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

---

* On appeal from Marion County Circuit Court, Tracy A. Prall, Judge. 300 Or App 147, 452 P3d 1011 (2019).

WALTERS, C.J.

In connection with a criminal prosecution for delivery of methamphetamine, the trial court ordered defendant to unlock a passcode-protected cell phone that had been found in her purse. Defendant resisted, contending that the order required that she perform an act that would provide incriminating, testimonial evidence, violating her right against self-incrimination under Article I, section 12, of the Oregon Constitution and the Fifth Amendment to the United States Constitution. The trial court concluded that the order was lawful and held defendant in contempt. The Court of Appeals affirmed the contempt judgment. *State v. Pittman*, 300 Or App 147, 164, 452 P3d 1011 (2019). Although we agree with the state that there are circumstances in which such an order would not violate Article I, section 12, the record in this case does not include a factual finding by the trial court that would allow us to conclude that those circumstances are present here. Accordingly, we reverse.

I. BACKGROUND

Early one morning, defendant crashed her vehicle into a tree, injuring herself and the passengers in the car. Defendant and the passengers were transported to the hospital where staff provided defendant with trauma care and removed her clothing. While doing so, hospital staff discovered that defendant possessed a large amount of cash, a clear plastic baggie containing white powder, and a pipe, and they turned those items over to police officers. The officers believed (and later confirmed) that the white substance was methamphetamine. The officers also discovered that, inside the baggie containing methamphetamine, there were multiple smaller clear plastic baggies. The officers believed that the baggies were of the type commonly used to sell smaller amounts of drugs and that defendant was selling or distributing drugs. At the hospital, Officer Brian Frazzini attempted to take defendant's statement, and he observed that she appeared to be under the influence of a stimulant. Based on the totality of that evidence, the state eventually charged defendant with crimes, including delivery of methamphetamine, and booked her into jail.

While at the hospital, Officer Frazzini also made another observation that led to the seizure of the phone that is the focus of this case: He observed a "white smart phone style cell phone" in defendant's purse. The police obtained a warrant to seize and search the phone. After seizing the phone, they realized that it was passcode-protected and that they could not unlock it. Supported by Frazzini's affidavit reporting what he had observed at the hospital, Officer Garon Boyce applied for a second search warrant and requested that the court "compel" defendant to provide the "numeric PIN numbers, alphanumeric passwords, patterns codes or other coded information to unlock the phone." The court granted the second search warrant, and another officer, Officer Angus Emmons, met with defendant at the jail. He provided defendant with a copy of the warrant and asked her to unlock the phone. Defendant did not comply.

The state then filed a motion to compel defendant to unlock the phone. In its motion, the state acknowledged that, by unlocking the phone, defendant would "inferentially" communicate that she had control over, or access to, the phone, but "given that the defendant's phone was located in her purse, the defendant's words will not be an admission that the phone was in her control since the state has already established that fact." Accordingly, the state argued, compelling defendant to unlock the phone would not violate defendant's right against self-incrimination.

Defendant opposed the motion. She contended, among other things,[1] that compelling her to provide the passcode to the phone would violate her rights against self-incrimination under Article I, section 12, of the Oregon Constitution and the Fifth Amendment to the United States Constitution. She asserted that the acts of providing the passcode and unlocking the phone were each testimonial and could incriminate defendant because they would indicate that the phone belonged to her or that she had access to the contents of the phone.

At a hearing, Officer Emmons testified. He explained that his role at the Salem Police Department was to conduct

[1] Defendant also argued that the search warrant itself was overbroad and lacked particularity. That issue is not before our court.

technological investigations, and that the phone at issue was an iPhone, which is produced by Apple. Emmons explained that,

> "With Apple specifically, and other phones sometimes, the phone is encrypted by default, which means that all the data on the phone, any potential evidence on the phone, is encrypted to the point where we can't access it unless it's unlocked with either a user code or that biometric data that's sometimes available to unlock the phone."

He also testified that there was practically no way to break the encryption on the phone or to manually remove the memory chip from the phone—even if the chip were removed, the data on the chip would still be encrypted, and to use a computer to decrypt the data, a passcode would still be necessary.

The trial court granted the state's motion to compel. In a letter opinion, the trial court rejected defendant's argument that the state had failed to establish that she knew the passcode or contents of the phone. The trial court explained that, "[b]ased on defendant's possession of the iPhone, Officer Boyce's training and experience, and Officer Emmons' testimony," there was "probable cause to believe that defendant has knowledge of the passcode and contents of the iPhone." Therefore, the trial court ordered defendant to unlock the phone.

After issuance of its letter opinion, the court held a hearing.[2] The court did not instruct defendant to reveal the passcode to the phone; the court instructed her to unlock it. When defendant was handed the phone to enter the passcode, a detective observed that she entered, "123456." The phone did not unlock. The court again instructed defendant that she was under court order to unlock the phone and warned her that she would be held in contempt if she did not comply. Defendant again entered "123456," and the phone did not unlock. The court found defendant in contempt and sentenced her to 30 days in jail.

---

[2] Defendant had filed a motion to stay the proceeding at which defendant would be required to unlock the phone so that defendant could pursue mandamus relief. At the hearing, the court denied defendant's motion and required defendant to unlock the cell phone.

Defendant appealed the contempt judgment, raising, among other things,[3] a challenge to the constitutionality of the trial court's underlying order requiring her to unlock the phone.[4] She argued that the order compelling her to enter the passcode violated her rights under Article I, section 12, and the Fifth Amendment because the act of entering the passcode would be testimonial and incriminating: The act would have communicated that defendant owned or had access to the phone and its contents. Defendant also argued that the doctrine on which the trial court had relied—the so-called "foregone conclusion doctrine"—was inapplicable. Defendant argued that, to prevail under that doctrine, the state was required to establish that it could prove the facts that her act could reveal, *i.e.*, that she owned the phone and knew its passcode. Defendant asserted that the state had not met that burden. Defendant acknowledged that, because the police had found the phone in her purse, the state had evidence that permitted an inference that defendant owned the phone. Defendant argued, however, that she had not admitted owning the phone and that "the act of typing a correct passcode into the phone would be new and stronger evidence that defendant owned the phone and was connected to any inculpatory evidence discovered in the phone." Moreover, defendant asserted, because of the vast amount of private information maintained on cell phones, the state should be required to show that it already knew the incriminating information that the phone contained. According to defendant, because the state had to prove the facts that the act of unlocking the phone would provide and had not done so, the trial court's order was not lawful, and

[3] Defendant also argued that the trial court plainly erred in holding her in contempt because there was insufficient evidence showing that she willfully violated the trial court's order. The Court of Appeals rejected that argument without discussion. *Pittman*, 300 Or App at 152. Defendant does not ask this court to address that issue.

[4] In a contempt case, "a challenge to the merits of the underling order may be made in any appeal from an order of contempt where, for constitutional, statutory or practical reasons, no other remedy, either by appeal or mandamus, was available." *State v. Crenshaw*, 307 Or 160, 168, 764 P2d 1372 (1988). The parties agree that, here, no other remedy was available: Defendant requested a stay of the order compelling her to unlock the phone so that she could pursue mandamus, but that request was denied. The trial court's order required immediate compliance, and appeal from the judgment of contempt is the only practical remedy available to defendant.

the court had erred in holding her in contempt for failing to unlock the phone.

In its response, the state acknowledged that the court's order compelling defendant to unlock the phone could be considered an order compelling "testimony" under Article I, section 12, and the Fifth Amendment, because the act would communicate that defendant "had control over the phone." The state argued, however, that the testimonial aspects of the act were significant only to the extent that the act communicated facts that the state did not already know.

The Court of Appeals affirmed. *Pittman*, 300 Or App at 164. The court agreed with defendant that the act of entering the passcode was testimonial, explaining that entering the passcode "requires the suspect to reveal her knowledge of the passcode and, by extension, allows a factual inference that she has access to the device and its contents." *Id.* at 153. The court then turned to the state's argument that such testimony could be compelled under the "foregone conclusion doctrine," which the state asserted had been adopted by the United States Supreme Court and discussed in two of its cases—*Fisher v. United States*, 425 US 391, 96 S Ct 1569, 48 L Ed 2d 39 (1976), and *United States v. Hubbell*, 530 US 27, 120 S Ct 2037, 147 L Ed 2d 24 (2000). *Pittman*, 300 Or App at 156-58. From those cases, the Court of Appeals concluded that that doctrine permitted the trial court's order and did not violate the either the Fifth Amendment or Article I, section 12, of the Oregon Constitution. *Id.* at 159-61.

Specifically, the court explained that "it is only the testimonial aspect of the compelled act that must be a foregone conclusion, because it is only the testimonial aspect of the compelled act that is protected under Article I, section 12." *Id.* at 160. That meant, the court reasoned, that the state need not show that it already knew the specific incriminating evidence that it would find on the phone; the act of entering the passcode did not communicate those facts. Rather, the act of entering the correct passcode "communicates *** that defendant knows the passcode and, by extension, has access to the device and its contents." *Id.* Therefore, the court explained, the court could compel defendant to enter the passcode if the state established that

it was a "foregone conclusion" that defendant could do so. *Id.* at 160-61. Because the trial court had concluded that the state had established "probable cause" of that necessary fact, and because defendant had not adequately developed an argument challenging that finding, the court held that the order compelling defendant to act violated neither the state nor the federal constitutions. *Id.* at 162-63.

Defendant sought, and we allowed, review.

II. ANALYSIS

In ordinary circumstances, when the state obtains a warrant permitting it to search for incriminating evidence in the possession of a defendant, the state has what it needs to conduct that search. For example, after obtaining a valid warrant supported by probable cause, the state is entitled to enter a defendant's home and perform the search authorized by the warrant. The state will ordinarily be capable of performing the search, including, for instance, searching a defendant's files for papers or drawers for diaries identified in the warrant. *See State v. Barnthouse*, 360 Or 403, 414, 380 P3d 952 (2019) (search is presumed unreasonable and "unlawful under Article I, section 9, unless it is supported by probable cause and a warrant"). But the circumstances in this case are not ordinary. Under these circumstances, the "novel nature of digital devices" presents an obstacle that officers cannot overcome with a search warrant. *See State v. Mansor*, 363 Or 185, 200, 421 P3d 323 (2018) (due to the "the novel nature of digital devices," courts have applied constitutional principles "in a manner somewhat different from other physical evidence"). Even with a warrant, officers cannot obtain access to the contents of a locked iPhone; as a practical matter, the state needs the assistance of a person who can unlock it. That obstacle creates a constitutional quandary. The state has a "responsibility to prosecute crime," even "in the novel and rapidly evolving context of digital evidence." *Id.* at 205. As a constitutional matter, however, a person cannot be compelled to provide incriminating, testimonial evidence. Thus, this case presents two questions of first impression: Did the court's order compel an act that would provide incriminating, testimonial evidence? If so, did the court's order violate defendant's

right against self-incrimination under the state or federal constitutions?

In answering those questions, the parties focus on *Fisher*—the decision of the United States Supreme Court that was the focus of their arguments below. Because that decision is so central to the parties' arguments, we begin by reviewing the Court's reasoning and its holding in that case.

Fisher arose out of a dispute between the IRS and three taxpayers. The IRS suspected that the taxpayers—a husband and wife and another individual—had violated various tax laws. *Fisher*, 425 US at 393-94. After being interviewed by the IRS, the taxpayers contacted their respective accountants to obtain certain tax documents that the accountants had prepared for them. *Id.* at 394. After obtaining the documents, the taxpayers gave them to their attorneys who had been hired to represent them in their dispute with the IRS. *Id.* When the IRS learned that the taxpayers had given the documents to their attorneys, the IRS served summonses on the attorneys directing them to produce the documents listed in the summons. *Id.* The attorneys did not comply, and the IRS sought court orders compelling production of the documents. *Id.* at 395. The district courts in the taxpayers' cases each entered an order to enforce the summonses, and the attorneys appealed, arguing, among other things, that if the Fifth Amendment excused the taxpayers from turning over the documents, then the attorneys who received the documents from the taxpayers should also be excused from compliance with the courts' orders.[5] *Id.* The issue, then, was whether compelling the taxpayers to produce the documents violated the taxpayers' Fifth Amendment right against self-incrimination.

The Supreme Court began its analysis by explaining that the *documents* the IRS sought did not enjoy Fifth Amendment protection. *See id.* at 109 (explaining that "the

[5] The Court agreed with the attorneys' framing of the issue. The Court explained that, if compelling a taxpayer to turn over the documents would violate the taxpayers' Fifth Amendment rights, then compelling the taxpayers' attorneys to turn over those same documents would violate the taxpayers' attorney-client privilege. *Fisher*, 425 US at 402. Thus, the Court analyzed the issue as a question of whether compelling the taxpayers to turn over the documents through their attorneys violated the taxpayers' Fifth Amendment rights. *Id.* at 405-14.

Fifth Amendment would not be violated by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications"). The documents may have contained incriminating, testimonial evidence, but the taxpayers had not been compelled to create them. The Court explained that "the preparation of all of the papers sought in these cases was wholly voluntary, and they cannot be said to contain compelled testimonial evidence, either of the taxpayers or of anyone else." *Id.* at 409-10. Therefore, the taxpayers could not "avoid compliance with the subpoena merely by asserting that the item of evidence which [they are] required to produce contains incriminating writing, whether [their] own or that of someone else." *Id.* at 410.[6]

The Court then turned to the more difficult issue of whether *the act of producing the documents*—which *was* compelled—implicated the taxpayers' Fifth Amendment rights. *Id.* The Court explained that the act of producing the documents had communicative aspects: If a taxpayer produced the documents, that act would "concede[ ] the existence of the papers demanded and their possession or control by the taxpayer. It would also indicate the taxpayer's belief that the papers are those described in the subpoena." *Id.* Nevertheless, the Court held that the act of producing the documents did not enjoy Fifth Amendment protection. *Id.* at 410-11. The Court reasoned that the government

[6] In so holding, the Court in *Fisher* took a step back from the analysis set forth in *Boyd v. United States*, 116 US 616, 68 S Ct 524, 29 L Ed 746 (1886), which had suggested, among other things, that the Fifth Amendment, like the Fourth, was concerned with privacy rights. In *Fisher*, the Court explained that it rejected *Boyd*'s analysis because the Fifth Amendment "does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a [t]estimonial [c]ommunication that is incriminating." *Fisher*, 425 US at 408; *see also* Case Comment, *The Rights of Criminal Defendants and the Subpoena Duces Tecum: The Aftermath of Fisher v. United States*, 95 Harv L Rev 683, 683-84 (1982) (noting that *Fisher* represented "a fundamental shift in [F]ifth [A]mendment jurisprudence from a concern with privacy to a focus on compulsion," and a shift from focusing on the "nature of the evidence sought" to the "process by which it was to be obtained"). Later, in *United States v. Doe*, 465 US 605, 610, 104 S Ct 1237, 79 L Ed 2d 552 (1984) (*Doe I*), the Court confirmed that understanding of the Fifth Amendment, holding that voluntarily created documents, even voluntarily created documents in an individual's possession, are not protected by the Fifth Amendment.

already knew that the documents existed, where they were located, and that the taxpayers has access to them. *Id.* at 411. The Court held that, because the communicative aspects of the act of producing the documents were a "foregone conclusion," compelling compliance with the summonses would "involve no incriminating testimony within the protection of the Fifth Amendment." *Id.* at 411, 414.

With that understanding of *Fisher*, we turn to defendant's arguments here—that the trial court's order compelling her to unlock the cell phone found in her purse violated her right against self-incrimination under both the state and federal constitutions. We begin with the Oregon Constitution and, in particular, Article I, section 12. *See State v. Campbell*, 306 Or 157, 162, 759 P2d 1040 (1988) (this court considers state law questions before turning to federal claims). Because we conclude that the trial court's order violated that state constitutional provision, we do not reach defendant's Fifth Amendment argument.

A. *The act of unlocking the phone would have provided incriminating, testimonial evidence.*

Article I, section 12, of the Oregon Constitution provides that "[n]o person shall be *** compelled in any criminal prosecution to testify against [him or herself]." "[T]o receive protection under the self-incrimination clause of Article I, section 12, a person's statement or conduct must (1) be 'testimonial' evidence, (2) be 'compelled,' and (3) be evidence that could be used against the person in a criminal prosecution." *State v. Fish*, 321 Or 48, 53, 893 P2d 1023 (1995). In this case, there is no dispute that the trial court's order compelled defendant to unlock the phone; the question is whether that compelled act qualifies as a statement that would provide incriminating, "testimonial" evidence.

Defendant argues that it would, relying on *Fish*. There, this court reasoned that acts necessary to perform certain field sobriety tests were testimonial because they "require[d] the individual to communicate information to the police about the individual's beliefs, knowledge, or state of mind." *Id.* at 60. Although we discussed the tests that the defendant performed as "acts," and observed that

statements protected by Article I, section 12, need not be verbal, the aspects of the field sobriety tests that we concluded were "testimonial" in *Fish* involved verbal communications, such as counting, answering questions relating to a person's residence and date of birth, estimating a period of time, and reciting the alphabet. *Id.* Here, the trial court's order did not require that defendant engage in any verbal communication; the court did not order defendant to state the passcode. The court's order also did not require defendant to perform an act that would expressly communicate her beliefs or knowledge—for example, by nodding her head to say, "yes," pointing to something, or translating or decoding an otherwise indecipherable statement. The court did not order the officers to observe the entry of the passcode or order defendant to permit the officers to do so. Nevertheless, defendant argues, the court's order required that she perform an act that would provide the state with incriminating, testimonial information and thus violated her right against self-incrimination under Article I, section 12.

Defendant makes two independent arguments to support her position. First, defendant argues that the act of unlocking the phone would communicate her beliefs, knowledge, or state of mind. Specifically, defendant asserts that the act of unlocking the phone would provide testimonial evidence because it would demonstrate that defendant knows the password to the phone, owns it or has access to it, and perhaps that she also knows or created the information that it contains.

Second, defendant and the American Civil Liberties Union of Oregon, the American Civil Liberties Union, and the Electronic Frontier Foundation, who appear as *amici* in support of defendant, argue more broadly that the act of unlocking the phone would provide protected "testimony," even if the act did not communicate defendant's beliefs, knowledge, or state of mind. Because of its breadth, we begin with that argument and note that it includes several interwoven strands. The first is that the state cannot compel a defendant to perform an act that serves the same function as would a compelled statement. Defendant contends that the state could not compel defendant to make a statement revealing the phone's passcode and therefore cannot compel

defendant to perform an act—unlocking the phone—that would provide the state with the same advantage.

Defendant is correct in her initial premise. The state could not compel defendant to reveal the passcode to the phone. Requiring her to do so would compel her to make an express verbal or written statement. As the state recognizes, an order requiring such a statement would be an order compelling testimonial evidence. But accepting the premise does not mean that defendant's conclusion follows. This court has made a distinction between incriminating statements—which are protected by Article I, section 12—and certain noncommunicative acts—which are not. And this court has done so even when both serve the same purpose. For example, a person cannot be compelled to make a verbal or written statement about whether the person has a tattoo, what the tattoo looks like, or where it is located, but the person may be compelled to stand up in court, permitting the observation of the tattoo. Such an act is not implicated by Article I, section 12. *See State v. Cram*, 176 Or 577, 582-83, 160 P2d 283 (1945) (explaining that a person "may be required to do many things without having [his or her] constitutional rights against self-[in]crimination invaded," including, for example, standing up in court, appearing at the scene of the crime, putting on clothing to see if it fits, removing glasses, and removing clothing so that the jury may examine scars and tattoos). We reject defendant's argument that the act of unlocking the phone is testimonial solely because it serves the same purpose as compelling defendant to reveal the passcode itself.

We also reject the strands of defendant's argument drawn from *State v. Vondehn*, 348 Or 462, 236 P3d 691 (2010), and *Cram*. According to defendant, those cases stand for the following propositions: (1) that compelled statements and the compelled production of physical evidence are entitled to equivalent constitutional protection; and (2) that defendant cannot be compelled to do an act that would lead the state to physical evidence that could be used against her.

In *Vondehn*, this court held that officers had violated the defendant's Article I, section 12, rights by failing

to give *Miranda* warnings and that both the statements that the defendant had made and the physical evidence derived from those statements must be suppressed. *Vondehn*, 348 Or at 469-70. The state had argued that Article I, section 12, "does not prohibit the admission of physical evidence, even physical evidence that is a 'fruit' of a defendant's compelled testimony; it prohibits only compelling a person to 'testify.'" *Id.* at 467. We rejected that argument, explaining that if the state illegally obtains testimony, then Article I, section 12, prohibits the admission of both "compelled statements and physical evidence derived from such statements." *Id.* at 469. Thus, defendant is correct that, for purposes of the exclusionary rule, this court generally treats illegally obtained statements and the physical evidence derived from those statements equivalently. *Vondehn* does not, however, stand for the proposition that compelled statements and acts that lead to physical evidence must always be treated the same or that a defendant can never be compelled to perform an act that aids the state in obtaining incriminating evidence. Defendant overreads *Vondehn*.

Defendant does the same with *Cram*, a case that this court discussed in *Vondehn*. In *Vondehn*, we cited *Cram* for the proposition that "the constitutional privilege against self-incrimination had generally been held to be declaratory of the common-law privilege and that that privilege was not limited to testimonial utterances, but extended to prevent the compelled production of documents or chattels." *Vondehn*, 348 Or at 468 (discussing *Cram*, 176 Or at 581-82). But the holding in *Cram* was that the admission of the testimony of a physician who took the defendant's blood sample into evidence did not violate defendant's Article I, section 12, rights, because the defendant had not been required to "establish the authenticity, identity or origin of the blood; those facts were proved by other witnesses." *Cram*, 176 Or at 593. *Cram* is therefore consistent with the analysis we undertook in *Fish*, where we looked to whether the act at issue required the defendant to communicate information about the defendant's knowledge, beliefs, or state of mind. *Fish*, 321 Or at 60. This court's prior cases do not support an argument that Article I, section 12, protects non-communicative acts which provide, lead to, or assist the state in obtaining incriminating physical evidence.

Defendant's more nuanced argument is that an act that requires mental effort is different than an act that requires only physical effort. Defendant contends that, although a person may "be forced to surrender a key to a strongbox containing incriminating documents," the person may not "be compelled to reveal the combination to a wall safe—by word or deed." The latter, defendant posits, is what she was required to do here; that is, to reveal her knowledge of the password by deed, rather than by word.

The key-combination metaphor comes from Justice Stevens's dissent in *Doe v. United States*, 487 US 201, 219, 108 S Ct 2341, 101 L Ed 2d 184 (1988) (*Doe II*). In *Doe II*, the petitioner, who was the target of a federal grand jury investigation, had invoked his Fifth Amendment privilege against self-incrimination when asked to authorize foreign banks to disclose records of his accounts. 487 US at 203-04. The banks also had been served with subpoenas commanding them to hand over the documents, but the banks, which were located in the Cayman Islands, refused to comply, citing that government's bank-secrecy laws. *Id.* at 203. The federal government sought a court order compelling the petitioner to execute a consent directive authorizing the Cayman banks to release petitioner's account information. *Id.* The district court initially denied the government's request, but the Fifth Circuit reversed that decision. *Id.* at 204-05. On remand, the district court ordered the petitioner to execute the consent directive, but he refused, and the court held him in contempt. *Id.* at 205.

The United States Supreme Court concluded that the district court's order requiring the petitioner to execute the consent directive was lawful. *Id.* at 219. Citing *Fisher*, the Court began by stating that "the contents of the foreign bank records sought by the Government are not privileged under the Fifth Amendment." *Id.* at 206. The question, then, was whether the act of executing the consent form directing the banks to release the records had "independent testimonial significance that [would] incriminate him," and whether the Fifth Amendment prohibits government compulsion of that act. *Id.* at 207. The Court noted that the "execution of the consent directive at issue in this case obviously [was] compelled, and we may assume that its execution

would have an incriminating effect." *Id.* at 207. The issue was whether executing the form was "testimonial communication." *Id.* The Court explained that whether a compelled communication was testimonial "often depends on the facts and circumstances of the particular case," and that the case before it was no exception. *Id.* at 214-15. The record in *Doe II* showed that the consent directive was drafted carefully to not reference a specific account and to speak only in the hypothetical. *Id.* at 215. That being the case, the form did not acknowledge that petitioner even had an account at the foreign bank; in fact, the form did not even identify a particular bank. *Id.* The form only allowed the government to access a potential account once the government found it by independent investigation of its own officers. *Id.* As in *Fisher*, the government was not "relying upon the 'truthtelling' of [the petitioner's] directive to show the existence of, or his control over, foreign bank account records." *Id.* (quoting *Fisher*, 425 US at 411). Consequently, the Court reasoned, the consent directive was "not testimonial in nature," and the District Court's order compelling petitioner to sign it did not violate the Fifth Amendment. *Id.* at 219.

Justice Stevens dissented. Justice Stevens's view was that the Fifth Amendment right against self-incrimination applies in any instance where a person can be compelled "to use his mind to assist the prosecution in convicting him of a crime." *Id.* at 219. Thus, a person may "be forced to surrender a key to a strongbox containing incriminating documents," but a person may not "be compelled to reveal the combination to a wall safe—by word or deed." *Id.* In Justice Stevens's view, the majority in *Doe II* was incorrect in holding that filling out a form was not protected by the Fifth Amendment because filling out a form was more akin to providing the government with the combination to a safe—both require the use of a person's mind to assist the prosecution.

In response to Justice Stevens's argument, the majority in *Doe II* also relied on the key-combination metaphor but did not accept Justice Stevens's view that the use of one's mind to assist the prosecution is what makes something testimonial. Instead, the majority stated that the "expression of the contents of an individual's mind" is what

makes something "testimonial communication for purposes of the Fifth Amendment." *Doe II*, 487 US at 210 n 9 (internal quotations omitted). Applying that test, the majority explained that it "simply disagree[d] with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind." *Id.* The majority concluded its footnote by stating that, "[i]n our view, such compulsion is more like being forced to surrender a key to a strongbox containing incriminating documents than it is like being compelled to reveal the combination to petitioner's wall safe." *Id.* (internal quotations and alterations omitted). Thus, the majority used the dissent's metaphor to spotlight the basis for its own decision. When a defendant is required to communicate beliefs or knowledge, as she does when she is compelled to reveal a safe's combination, then the defendant provides testimonial evidence. But when a defendant is required to do an act that is not similarly revelatory, that act is not testimonial simply because the act required the defendant to use her mind.

The Court adhered to that distinction, again using the key-combination metaphor, in *Hubbell*. There, the defendant was under investigation for tax evasion and other crimes relating to the Whitewater Development Corporation. *Hubbell*, 530 US at 30. During that investigation, the government served the defendant with a subpoena to appear in front of a grand jury and produce requested documents.[7] *Id.* at 31. The requested documents fell into 11 broadly described categories. *Id.* To produce the requested documents, the defendant had to examine numerous documents, and he ultimately produced 13,120 pages of material. *Id.* at 42. The Court concluded that, because the 11 different categories were described so broadly, the collection and production of the documents was "tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions." *Id.* at 41. The Court noted that, when assembling the documents into the different described categories,

[7] The defendant had initially pled guilty to tax evasion and other crimes, and when he did so, he had agreed to produce documents pertaining to the investigation. The grand jury was investigating whether the defendant had violated his first plea agreement. *Hubbell*, 530 US at 42.

> "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena. *** The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."

Id. at 43 (quoting *Curcio v. United States*, 354 US 118, 126, 77 S Ct 1145, 1 L Ed 2d 1225 (1957)).

The Court explained that, whatever the scope of the *Fisher* rationale, the case "plainly [fell] outside of it." *Hubbell*, 530 US at 44. In *Fisher*, the government "already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them." *Id.* at 44-45. By contrast, in *Hubbell*, the government had not shown "that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced." *Id.* at 45. Because the defendant's "act of production had a testimonial aspect, at least with respect to the existence and location of the documents sought," and because the government could not establish, as it had in *Fisher*, that it already knew those facts, then the Fifth Amendment prohibited the compelled production of the documents. *Id.* at 45.

In this case, as noted, defendant and her *amici* rely on the key-combination metaphor for their argument that a phone's passcode is more analogous to a safe's combination than it is with its key. That is no doubt true: A phone's passcode, like the combination to a safe, is a set of numbers that unlocks something. But, as the United States Supreme Court has used that metaphor, the important distinction is not whether the defendant will be required to *use* her mind to unlock the device, but, instead, whether the act of unlocking the device will *reveal* something about the workings of the defendant's mind. As noted, in *Doe II*, the Court appears to have accepted that, although filling out a bank form requires an individual to use his or her mind, that mental exercise alone does not make that act testimonial. Instead, the Court said, "to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Doe II*, 487 US at 210.

The Court applied that test in *Hubbell*: Because the subpoena required the defendant to use his own judgment to determine whether a particular document fell into a certain category and the act of turning over the documents would have communicated those choices, the act in *Hubbell* was more like giving testimony than it was a "act" without testimonial aspects. *Hubbell*, 530 US at 42.

We can, of course, adopt a different view in construing Article I, section 12, and hold that it is the use of the mind to assist the state that makes an act testimonial. But, to date, our decisions have been consistent with the analysis of the United States Supreme Court. In *State v. Fisher*, 242 Or 419, 422, 410 P2d 216 (1966), for example, we held that requiring a handwriting exemplar does not violate the privilege against self-incrimination. Like the act of signing a bank form, providing a handwriting exemplar requires the use of the mind, but, like the Court in *Doe II*, we did not conclude that that mental effort made that act testimonial. And in *Fish*, we, again like the Court in *Doe II*, explained the testimonial significance of conduct as stemming from what it "communicates" about a person's "beliefs, knowledge, or state of mind." *Fish*, 321 Or at 56. Today we affirm that articulation and, like most other state courts that have considered the issue,[8] decline to hold that an act is testimonial whenever its performance requires an individual to use his or her mental faculties. The information that an act

[8] We are aware of only one state trial court decision that could be understood to accept the argument that the right against self-incrimination prohibits an act that would require a defendant to use his or her mind. *See Commonwealth v. Baust*, 89 Va Cir 267, 2014 WL 10355635 at *4 (Va Cir Ct 2014) (explaining that the defendant could not "be compelled to divulge through his mental processes the passcode for entry", but, on the contrary, "[t]he fingerprint, like a key, *** does not require the witness to divulge anything through his mental processes" (internal quotation omitted)). The basis for the court's decision in *Baust* is not entirely clear, however. We cannot discern whether the government's motion was a motion to compel the defendant to unlock the cell phone or a motion to compel defendant to disclose the passcode itself, and the court seems to distinguish between an order requiring a fingerprint or requiring that the defendant "divulge" mental processes.

As we will explain, most other courts have applied a form of the *Fisher* rule to permit orders compelling criminal defendants to use passcodes to unlock cell phones or other electronic devices. The dispute among courts is not about whether to adopt such a rule, but about what the state must know to take advantage of it.

communicates, and not the uncommunicated use of the mind, is what makes an act testimonial.

For the reasons given, we reject defendant's broad argument that the act of unlocking the phone would provide testimonial evidence even if it did not communicate defendant's thoughts, beliefs, knowledge, or state of mind.[9] We return to defendant's primary argument, from the United States Supreme Court's decision in *Fisher* and this court's decision in *Fish*, that the act of unlocking the phone was protected by Article I, section 12, because it would communicate that very information.

The first step in that analysis is to determine the facts, if any, that the compelled act would communicate. As *Fisher*, *Hubbell*, and *Doe II* illustrate, that depends on the order that was given. In *Fisher*, the taxpayers were ordered to produce specified listed documents. Doing so, the Court held, would communicate that the documents existed, that the taxpayers had access to them, and that the taxpayers believed "that the papers are those described in the subpoena." *Fisher*, 425 US at 410. In *Hubbell*, the defendant was ordered to produce documents that fell within certain broadly described categories. 530 US at 42. Doing so would communicate not only that the documents existed, but that they fell into the described categories. *Id.* at 44-45. In *Doe II*, the defendant was ordered to sign bank consent forms. 487 US at 203. Doing so, the Court held, would not communicate facts of any sort. *Id.* at 215.

Here, defendant was ordered to unlock the phone using a passcode. Thus, as the state acknowledges, defendant's performance of that act would communicate that she knew the passcode. If the court had ordered defendant to do something different, what would be communicated by compliance with the order may have been different as well. For

[9] We also reject a third argument that defendant makes. Defendant asserts that she entered the passcode to the phone and that officers observed her doing so, obtaining the code and thereby obtaining testimonial evidence. We reject that argument because the trial court's order did not compel defendant to provide the passcode; it required defendant to unlock the phone. Initially, the court ordered defendant to give the state the passcode, but after defendant took issue with that, the court revised its order, stating that defendant would be handed the phone so she could "unlock it without providing the information to us."

example, had the phone been one that could be unlocked by placing a finger on the phone, and had the court ordered defendant to place her finger on the phone, then, by performing that act, defendant would communicate only that she knew how to move her finger, not that she knew how to unlock the phone. If, however, the court had ordered defendant to unlock the phone, without specifying the means she should use to do so, then any act that she performed that served to unlock the phone would communicate her knowledge—that she knew how to comply with the court's order and how to access the phone's contents. Here, as the state acknowledges, the court's order was of that ilk. It required defendant to unlock the phone using a passcode, and compliance with that order would communicate that defendant knew that passcode. We conclude that the act of unlocking the phone was an act that would provide incriminating testimonial evidence.

B. *In narrow circumstances, Article I, section 12, permits a court order requiring that a criminal defendant unlock a cell phone.*

That conclusion does not end our analysis, however. The state argues that, even if the act of unlocking a cell phone would provide testimonial evidence, its testimonial aspects are insignificant in the circumstances at issue here and, thus, are not entitled to constitutional protection. The state submits that this case is different from other instances in which the state seeks to compel testimony because, the state contends, it was not interested in having defendant unlock the phone to learn the facts that the act would communicate: The state did not seek to learn whether defendant knew the passcode to the phone; it already knew that she did. Instead, the state sought to compel defendant's act to gain access to certain information maintained on the phone. The state argues that in these circumstances, this court should construe Article I, section 12, to permit the trial court's order and rely on the United States Supreme Court's reasoning in *Fisher*.[10]

[10] The state also argues that this court already has adopted *Fisher*'s reasoning. We disagree. In the case on which the state relies, *State v. Janscek*, 302 Or 270, 285, 730 P2d 14 (1986), this court focused, as the United States Supreme

In addressing that argument, we emphasize that we are asked to apply the reasoning from *Fisher* only in the limited factual circumstances that this case presents: In this case, the state already had obtained a warrant to seize and search the cell phone and the order to unlock the phone would have required an act that communicated that defendant knows how to unlock the phone.

Both those factual circumstances are significant to our analysis. When the state has obtained a warrant that permits it to search a cell phone, the state will have been required to describe, with reasonable particularity, the evidence that it believes is on the phone and its relevance to the state's investigation. *See Mansor*, 363 Or at 216-18 (explaining that "a warrant must describe, with as much specificity as reasonably possible under the circumstances, *what* investigating officers believe will be found on the electronic devices" including, "if relevant and available, the time period during which that information was created, accessed, or otherwise used"). That requirement originates from Article I, section 9, and protects an individual's right to privacy in the contents of items that are subject to search. Thus, when the state has obtained a warrant to search a cell phone in compliance with Article I, section 9, we are assured that a defendant's right to privacy in the contents of that phone is adequately protected.

We also consider it significant that we are asked to apply the *Fisher* reasoning only to testimonial evidence that may be inferred from an act with limited testimonial significance. As we indicated at the outset, the act at issue is not an act that would expressly communicate a defendant's beliefs, knowledge, or state of mind. Instead, the act of unlocking the phone would permit a factfinder to draw an

---

Court had in *Fisher*, on whether the defendant had been compelled to create the document that the state sought. In *Janscek*, we held that a letter that the defendant had written to his employer stating that he planned to kill his wife was not protected by Article I, section 12: There was not "one bit of evidence that any representative of the state or any other governmental body in any way compelled defendant to communicate to [his employer] defendant's intent to commit an act of violence against his wife." *Id.* at 284-85. In *Janscek*, the defendant did not argue, as did the taxpayers had in *Fisher*, that the *act* of turning over the letter had a communicative aspect and was protected by Article I, section 12. We therefore had no occasion to address that issue, and we consider it afresh today.

inference about the defendant's beliefs, knowledge, or state of mind—that defendant knows its passcode—and that inference would be of limited significance. The state asks us to adopt a rule that would permit it to compel that act when it already knows the information that could be inferred from it.

Thus, the path that the state urges us to take is a narrow one, and rightly so: The obstacle the state faces is a sizable one. Generally, as the state recognizes, Article I, section 12, forbids an order compelling "testimony" without an offer of transactional immunity. *State v. Soriano*, 68 Or App 642, 684 P2d 1220 (en banc), *aff'd and opinion adopted*, 298 Or 392, 693 P2d 26 (1984) (per curiam).[11] In *Soriano*, the defendants had refused to testify before a grand jury that was investigating a crime, invoking their rights under Article I, section 12, of the Oregon Constitution. 68 Or App at 644. The trial court granted the defendants derivative-use immunity and ordered them to testify. *Id.* Derivative-use immunity typically precludes the state from using the compelled statements of a witness and the evidence derived from those statements in the prosecution of that witness. *Id.* at 644 n 3. The state argued that derivative-use immunity was a sufficient substitute for the defendants' constitutional rights against self-incrimination. *Id.* at 644-45. The United States Supreme Court had held that such immunity is sufficient because the government and the witness are left "'in substantially the same position as if the witness had claimed his privilege' in the absence of a grant of immunity." *See Kastigar v. United States*, 406 US 441, 458-59, 92 S Ct 1653, 32 L Ed 2d 212 (1972) (quoting *Murphy v. Waterfront Comm'n*, 378 US 52, 79, 84 S Ct 1594, 12 L Ed 2d 678 (1964)).

This court rejected that argument and instead held that the state could not compel the defendants to testify in front of a grand jury without providing transactional immunity. *Soriano*, 68 Or App at 662. Transactional immunity precludes a state from prosecuting the witness

[11] *Soriano* is a Court of Appeals decision that this court adopted *in toto*. *Soriano*, 298 Or at 394. Because we "agree[d] with the analysis and conclusion of the Court of Appeals and adopt[ed] its opinion as our own," *id.*, we refer to the Court of Appeals decision in *Soriano* just as we would any other opinion of this court.

for any offense relating to the compelled statements. *Id.* We explained that, in *Kastigar*, the United States Supreme Court had held that use immunity was appropriate because such immunity was a "substantial" substitute for a person's constitutional right not to be a witness against oneself. *Id.* (discussing *Kastigar*). The Court had held that the Fifth Amendment is not a complete bar to compelled testimony and that a substitute for the right could suffice because such a rule would protect a person's constitutional rights and, at the same time, would "accommodate the interests of the State and Federal Governments in investigating and prosecuting crime." *Murphy*, 378 US at 79. Although we also permitted a "substitute" for the defendant's Article I, section 12, rights, we held that the substitute must be the same in "scope and effect." *Soriano*, 68 Or App at 662 (internal quotation omitted). We reasoned that, to be the same in scope and effect, transactional immunity was necessary to protect the witness's Article I, section 12, rights: "A witness granted immunity and then required to testify has not received full value for that lost right if there is *any way the testimony can cause harm to the witness* in that prosecution." *Id.* at 664 (emphasis added). In *Soriano*, transactional immunity was necessary to ensure that the compelled statements did not affect any of the state's discretionary decisions and that the defendants would be in the same position they would have been had they not testified at all. *Id.* at 663.

Thus, under *Soriano*, the state is generally prohibited from compelling a defendant's incriminating statements without providing transactional immunity. *Id.* at 664. And, as we have concluded above, compelled testimonial conduct is generally subject to the same Article I, section 12, protections as are compelled statements. Consequently, as a general rule, the state is prohibited from compelling a defendant to perform an act that provides testimonial evidence without providing transactional immunity. The state contends that we should reach a different conclusion, however, when the state already knows the facts that such an act would communicate.

The state contends that, when it already has evidence that a defendant knows the passcode to a phone and

does not seek to have the defendant unlock the phone for the purpose of discovering that passcode, then the compelled act loses its testimonial significance. The act serves only to "open the door" to the evidence on the phone—evidence that a search warrant permits the state to obtain. Defendant responds that, even if the state already has some evidence that defendant knows the passcode to the phone, the performance of that act would provide additional, and perhaps stronger, evidence of that fact. Defendant argues that, if the state were permitted to compel her to unlock the phone, the state could benefit from that additional evidence and cause harm to the defendant, violating defendant's right against self-incrimination.

The problem is a gnarly one and both sides' interests are worthy of protection. Because it has a valid warrant, the state is entitled to search the *contents* of the phone; it is only modern technology that keeps the state from obtaining that evidence. On the other hand, forcing defendant to unlock the phone will do more than provide the state with *access* to that evidence; the act of unlocking will provide the state with evidence that has testimonial aspects, even if its significance is limited. And, because the act of unlocking a cell phone provides incriminating testimonial evidence, requiring that defendant perform that act could cause harm to defendant by providing the state with evidence that it could use in its analysis, investigation, or prosecution of the case. This particular problem is not one that the drafters of the Oregon Constitution could have anticipated, and we would benefit from its consideration in the Oregon Legislative Assembly. Although "the state and federal constitutions impose outer limits on the permissible range of authority to conduct searches and seizures," constitutions do not "define the circumstances and manner in which, within those outer constitutional limits, the authority should or should not be employed." *State v. Greene*, 285 Or 337, 346, 591 P2d 1362 (1979) (Linde, J., concurring). Those "are questions which, as far as the powers of the state and local officers are concerned, are left to state law." *Id.*

As presented, however, the question before us is one of outer constitutional limits, and we must undertake

to answer it. As we will explain, we can see our way if we understand that *Soriano* permits a "substitute" for the right against self-incrimination when the substitute places a defendant in the same position she would have been in had she not testified at all. *Soriano*, 68 Or App at 662-63 (holding that Article I, section 12, requires substitute that protects defendant to "'same extent in scope and effect'" (quoting *Counselman v. Hitchcock*, 142 US 547, 585, 12 S Ct 195, 35 L Ed 1110 (1892)). For us, the question is whether it is possible to allow a court to issue an order compelling a defendant to unlock a cell phone—thereby compelling her to communicate, by inference, that she knows the passcode and has access to that phone—while still placing her in the same position she would have been in had she not provided that communication.

To place defendant in the same position she would have been in, we must account for the two different ways in which the act of unlocking a phone could harm defendant: It could provide information that the state did not already have, or it could bolster or add to information that the state already has. In the first instance, the act, as *Soriano* warns, could significantly aid the state in its analysis, investigation, or prosecution of the case. So, for instance, if officers found a cell phone in an apartment house parking lot, an order compelling all residents of the complex to unlock the phone could provide the state with valuable information that it did not already have about the identity of the person who knows its passcode. It would be difficult to cabin the state's use of that new information without a grant of transactional immunity. If, however, the state already knows that a defendant can unlock the phone using a passcode, the fact that the defendant does so serves only to confirm the state's knowledge and the risk of harm is reduced.

The state's argument for a rule that permits it to compel defendant to unlock a cell phone is premised on its contention that it is not interested in, and does not need, the testimonial aspects of that act; all it needs, and seeks to compel, is the act itself. At trial in this case, the state informed the court that it would not use defendant's act of unlocking the phone as evidence; it would use it only to

gain access to the phone.[12] In its briefing in this court, the state appears to accept that a prohibition on other use would be imposed; the state acknowledges that judicial estoppel principles could prevent the state from offering an act in evidence after the state has argued that it has no need for the testimonial evidence that the act would provide. *See Hampton Tree Farms, Inc. v. Jewett*, 320 Or 599, 609-10, 892 P2d 683 (1995) (acknowledging that judicial estoppel has no "single, uniform formulation," but at the very least, it "preclude[s] a party from taking an inconsistent position in a later proceeding if that party has received a benefit from the previously taken position in the form of judicial success" (internal quotation omitted)). We agree with the state that a prohibition on the use of the compelled act would be appropriate; however, principles of judicial estoppel do not provide sufficient protection of the constitutional right at issue. Article I, section 12, requires sterner stuff. To comply with the Oregon Constitution, a court order compelling a defendant to unlock a cell phone so that the state may execute a valid search warrant (1) could issue only if the state already knows the information that the testimonial aspects of the act will communicate and (2) must prohibit the state from using the testimonial aspects of that act against the defendant for any purpose. Those prohibited uses would include, but not be limited to, use as evidence at the defendant's trial, use to seek additional search warrants, use to obtain an indictment, or use in sentencing. Only such a rule would protect a defendant to "the same extent in scope and effect," as the right against self-incrimination. *Soriano*, 68 Or App at 662 (internal quotation omitted).

We recognize that, if a defendant complies with an order to unlock a phone, that act will reveal the contents of the phone providing the state with evidence that it could not otherwise obtain. But, as we have explained, once the state has obtained a valid warrant to search a phone, a defendant does not have a legal right to keep the contents of the phone from the state. It is only the testimonial aspects of

[12] Below, the state asserted that the act of unlocking the phone was "not something that [the state was] going to use against [defendant]" to show that the phone was hers or that it was in her possession because the state "already [had] evidence that it was in her purse and in her possession."

the act of unlocking the phone, and not the practical result of unlocking the phone, that have constitutional significance under Article I, section 12. The testimonial aspects of the act have constitutional significance, which we must address; the access that the act provides does not.

We also recognize that, in Oregon, an individual's right against self-incrimination must be protected, no matter how weighty the state's contrary interests may be. But Article I, section 12, permits a substitute for that right that is protective to "the same extent in scope and effect," *Soriano*, 68 Or App at 663, as the right against self-incrimination and, in the circumstances that this case presents, we can craft a rule that meets those terms. There may come a day in which the state can conduct, pursuant to warrant, an appropriately limited search of a cell without compelling a defendant's assistance to unlock it. *See State v. Brown*, 301 Or 268, 278 n 6, 721 P2d 1357 (1986) ("In this modern day of electronics and computers, we foresee a time in the near future when the warrant requirement of the state and federal constitutions can be fulfilled virtually without exception."); *State v. Kurokawa-Lasciak*, 351 Or 179, 188-89, 263 P3d 336 (2011) (noting that the majority in *Brown* had suggested that its decision was "a temporary accommodation subject to change in the near future when technology would permit neutral magistrates to" issue warrants "more expeditiously"). But, today, faced with the circumstances and law as they presently exist, we construe Article I, section 12, to permit an order compelling a defendant to unlock a cell phone so long as the state (1) has a valid warrant authorizing it to seize and search the phone; (2) already knows the information that the act of unlocking the phone, by itself, would communicate; and (3) is prohibited from using defendant's act against defendant, except to obtain access to the contents of the phone.

C. *The trial court's order did not comply with Article I, section 12.*

We must now consider whether the trial court's order complied with the requirements just articulated. *See State v. Crenshaw*, 307 Or 160, 168, 764 P2d 1372 (1988) (a defendant may challenge the merits of the underlying order

in an appeal from an order of contempt where "for constitutional, statutory, or practical reasons, no other remedy, either by appeal or mandamus, was available"). As noted, there is no dispute that the first requirement—that the state have a valid warrant permitting it to search the phone—is met. Thus, we address the second and third requirements—that the state already knows the information that the act of unlocking the phone would communicate and that the order prohibits the state from using defendant's act against defendant.

Defendant begins by arguing that, to establish that the state already knows the information that the act of unlocking a phone would communicate, the state must prove not only that it already knows that defendant knows the passcode to the phone but also that it already knows what will be found when its search is conducted. For reasons we have explained above, we reject that argument. 367 Or at 524-25. As noted, the rule we have announced requires the state to establish that it already knows the information that the act of unlocking the phone would communicate. And we have explained that, because the trial court's order in this case required defendant to unlock the phone using the passcode, compliance with that order would communicate that defendant knows the passcode. Due to the nature of the court's order—defendant was asked to do something, not to produce something—compliance would not communicate that the phone contained any particular evidence.[13] *See* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex L Rev 767, 775 (2019) (explaining that there is a difference between the testimonial act of complying with an order to "do" something as opposed to complying with an order to produce something). The testimonial information that the act communicates, which, in this case, does not include information about the phone's content, is what the state must demonstrate it already knows.

[13] For this reason, we disagree with Professor Laurent Sacharoff, who appears as *amicus curiae* in this case. *See* Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone: A Response to Orin S. Kerr*, 97 Tex L Rev Online 63, 65 (2019) (arguing that government must show that it already knows what evidence will be found on the phone).

Many of the other courts that have considered the matter agree and generally require that the state establish only that it knows that the defendant knows the phone's passcode. *See State v. Andrews*, 243 NJ 447, 480, 234 A3d 1254, 1276 (2020) ("[A]lthough the act of producing the passcodes is presumptively protected by the Fifth Amendment, its testimonial value and constitutional protection may be overcome if the passcodes' existence, possession, and authentication are foregone conclusions."); *State v. Johnson*, 576 SW3d 205, 227 (Mo Ct App 2019), *cert den*, __ US __, 140 S Ct 472, 205 L Ed 2d 286 (2019) ("The facts conveyed through his act of producing the passcode were the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity."); *Commonwealth v. Jones*, 481 Mass 540, 551, 117 NE3d 702, 713, *cert den*, __ US __, 140 S Ct 545, 205 L Ed 2d 345 (2019) (explaining that the Massachusetts Constitution "requires the Commonwealth to prove that a defendant knows the password to decrypt an electronic device beyond a reasonable doubt for the foregone conclusion exception to apply").

Not all courts reason similarly, however. Others have held that, because the unlocking or decryption of a device would provide the government with the information found on the device, the government already must know what information will be found on the device. *See People v. Spicer*, 125 NE3d 1286, 1291 (Ill App 2019) (rejecting state's argument that it must show only that defendant knew the passcode and explaining that "what the State actually needed to establish with reasonable particularity was the contents of the phone, which it did not do"); *G.A.G.L. v. State*, 257 So 3d 1058, 1064 (Fla Dist Ct App 2018) (determining that the focus of the foregone conclusion doctrine should be on the evidence sought, and in a case involving the password to a cell phone, the evidence sought is not the passcode but the "actual files or evidence on the locked phone," and "[w]ithout reasonable particularity as to the documents sought behind the passcode wall, the facts of this case plainly fall outside of the foregone conclusion exception" (internal quotation omitted)); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F3d 1335, 1337, 1347 (11th Cir 2012) (government could not compel act because government did "not

know what, if anything, is held on the encrypted drives"); *cf United States v. Apple MacPro Computer*, 851 F3d 238, 248 (3d Cir 2017) (where government "provided evidence to show both that files exist on the encrypted portions of the devices and that Doe can access them," any error was not clear or obvious).

The decisions in those cases reflect privacy concerns that are echoed by defendant and her *amici*.[14] Those concerns are legitimate. The breadth of personal information maintained on cell phones is far beyond that typically inscribed in a diary or day planner. In Oregon, those concerns are addressed in Article I, section 9, of the Oregon Constitution. That provision protects the right to privacy in electronic devices and generally requires that the state obtain a warrant before searching such devices. *See State v. Munro*, 339 Or 545, 551, 124 P3d 1221 (2005) ("Article I, section 9, protects both possessory and privacy interests in effects."). That provision also requires that a warrant explain, with reasonable particularity, what evidence officers are authorized to look for and the basis for the state's conclusion that it has probable cause to believe that such evidence exists. *Mansor*, 363 Or at 216 (a warrant must describe, "with as much specificity as reasonably possible under the circumstances, *what* investigating officers believe will be found on the electronic devices," and "the 'what' is a description of the *information* related to the alleged criminal conduct which there is probable cause to believe will be found" on the device (emphases in original)). Even so, there is a potential that, when executing a warrant to search an electronic device, the state may see more than the warrant permits: "Even a reasonable search authorized by a valid warrant necessarily may require examination of at least some information that is beyond the scope of the warrant." *Id.* at 220. Consequently, this court has devised a rule that

[14] For instance, the Indiana Supreme Court noted in *Eunjoo Seo v. State*, 148 NE3d 952, 959 (Ind Sup Ct 2020), that "[t]he Supreme Court in *Fisher* (1976), *Doe I* (1984), or *Hubbell* (2000) surely could not have anticipated that such devices would become so common or imagined the breadth and depth of information they could contain." The court in *Eunjoo Seo* also expressed concerns about the workability of the *Fisher* rationale in the cell phone context, noting that compelling a person to decrypt the device would provide the state with access to more than the files it already knew existed. *Id.* at 960-61.

addresses that potential: When the state uncovers information that a warrant did not authorize it to uncover, Article I, section 9, prohibits the state from using that information at trial, unless its use comes within an exception to the warrant requirement. *Id.* at 221.

To the extent that defendant asserts that the privacy protections of Article I, section 9, must be met to satisfy Article I, section 12, we are not persuaded that today is the day to decide that issue. In this case, the state obtained a warrant to search the phone, and defendant does not argue that the trial court's order compelling defendant to unlock her phone violated Article I, section 12, because the warrant failed to state with reasonable particularity the information that the state believed would be found on the phone. To the extent that defendant asserts that the privacy protections that Article I, section 12, may afford exceed the protections of Article I, section 9, and require the state to establish greater knowledge of the contents of a cell phone than would be necessary to obtain a warrant to search it, we reject that contention.

Defendant's next argument is that, even if the state is required to establish only that it already knows the testimonial information that the act of unlocking a cell phone will impart, it failed to make that showing in this case. Here, police officers discovered the phone in defendant's purse, which they found in her hospital room. As the parties agree, the state therefore had some evidence that defendant possessed the phone. Defendant argues that that evidence is insufficient. Defendant notes that she did not admit that she owned the phone or that she knew its password, implicitly quarreling with the standard that the trial court applied in reaching its conclusion that the state's knowledge was sufficient to permit the order.

Below, the trial court determined that, because the phone was found in defendant's purse, there was "probable cause to believe that defendant ha[d] knowledge of the passcode and contents of the iPhone." In Oregon, the "probable cause" standard reflects a "substantial objective basis" to believe that, "more likely than not," something has occurred. *See* ORS 131.005(11) (defining "probable cause"). Thus, when

a court determines, for instance, that an officer had probable cause to believe that a crime occurred, the court does not determine that a crime did, in fact, occur; it determines whether there is factual basis to believe that, more likely than not, a crime occurred. Put differently, probable cause is a measure of the basis for a belief; the court determines whether an officer's belief is "objectively reasonable in the circumstances." *State v. Vasquez-Villagomez*, 346 Or 12, 23, 203 P3d 193 (2009). There is a difference, therefore, between determining whether an officer's belief that defendant knows the passcode to the phone is objectively reasonable under the circumstances, and determining, as a factual matter, whether defendant does, in fact, know the passcode. The trial court in this case concluded that there was probable cause to believe that defendant knew the passcode. As we explained above, however, Article I, section 12, requires, as a precondition for an order of this sort, that the state already know that a defendant knows the passcode to the phone, and the record does not reflect that trial court made that finding. A conclusion that the state had probable cause is not the same as a finding that the trial court, as factfinder, was persuaded by the state's evidence. Consequently, the court's order did not meet constitutional muster; defendant's conviction must be reversed, and this case must be remanded to the trial court for further proceedings. To provide guidance in future cases, we think it important to address in more detail the standard that must be met when a court conducts that necessary factfinding.

As noted, a trial court must do more than assess, as a legal matter, whether the state has submitted evidence sufficient to demonstrate a likelihood that a defendant knows the passcode to the phone and can access it. The trial court must consider that evidence and, in the role of factfinder, decide whether it is persuaded. A factfinder may, of course, have different degrees of confidence in the decisions it makes. Under the preponderance of the evidence-standard, the factfinder must determine whether the facts asserted are more likely true than false. *Riley Hill General Contractor v. Tandy Corp.*, 303 Or 390, 402, 737 P2d 595 (1987). Under the clear and convincing-evidence standard, the proponent must establish that the facts asserted are "highly probable."

Id. And, to prove facts "beyond a reasonable doubt," the proponent must establish that the facts asserted are "almost certainly true." *Id.*; *see also State v. Williams*, 313 Or 19, 37, 828 P2d 1006 (1992) (explaining that it was erroneous to describe beyond a reasonable doubt using the phrase "moral certainty" because, among other things, that phrase "'may convey the idea to the jury that absolute certainty is required'" (quoting J.P. McBaine, *Burden of Proof: Degrees of Belief*, 32 Cal L Rev 242, 258 n 35 (1944)).

Each of those standards has had its appeal to other courts that have considered the issue before us today. Under the Fifth Amendment, one federal district court applied, without discussion, the preponderance of the evidence-standard. *See United States v. Fricosu*, 841 F Supp 2d 1232, 1237 (D Colo 2012) (finding that "government has met its burden to show by a preponderance of the evidence" that the laptop at issue belonged to the person compelled to unlock it). Another federal district court, also considering the Fifth Amendment, applied a clear and convincing-evidence standard. *United States v. Spencer*, 2018 WL 1964588 (ND Cal Apr 26, 2018). That court explained that that standard was appropriate in circumstances involving decryption because the *Fisher* rule "is an exception to the Fifth Amendment's otherwise jealous protections of the privilege against giving self-incriminating testimony." *Id.* at *3.

And the Massachusetts Supreme Judicial Court held that, under its constitution, the highest standard—beyond a reasonable doubt—applies. *Jones*, 481 Mass at 551, 117 NE3d at 713 (concluding that state constitution requires the state "to prove that a defendant knows the password to decrypt an electronic device beyond a reasonable doubt for the foregone conclusion doctrine to apply"). The court noted that a standard of proof indicates to the factfinder "the degree of confidence our society thinks he [or she] should have in the correctness of [his or her] factual conclusions." *Id.* (internal quotation omitted; first alteration in original). The court explained that "some critical facts implicating a defendant's constitutional rights require proof beyond a reasonable doubt"; for example, the standard under the Massachusetts Constitution for proving the

voluntariness of a confession is beyond a reasonable doubt. *Id.* at 551, 117 NE3d at 713-14. The court also explained that, when interpreting the Massachusetts Constitution, it had "remained vigilant to safeguard against governmental conduct that could infringe upon" the privilege against self-incrimination. *Id.* at 552. Thus, the court concluded, a "high burden is necessary to ensure that the *** rights of defendants are adequately protected, and reflects our recognition that a person's right to be free from self-incrimination is a fundamental principle of our system of justice." *Id.* at 553, 117 NE3d at 714 (internal quotation omitted).

In Oregon, when measuring the voluntariness of a defendant's confession to determine admissibility, this court requires a different factfinding standard than does the Massachusetts court. For a confession to be admissible into evidence at trial, the Oregon Constitution requires the state to prove voluntariness by a preponderance of the evidence. *State v. Stevens*, 311 Or 119, 137, 806 P2d 92 (1991) ("[W]e hold that, under Article I, sections 9 and 12, the state must prove the voluntariness of a consent to search, or of a defendant's statement, by a preponderance of the evidence.").[15] But that does not conclusively establish that a confession is voluntary; the jury is still free to decide whether the confession in fact was voluntary. *See State v. Morris*, 83 Or 429, 450, 163 P 567 (1917) ("If the confession is admitted by the judge and if it comes to the jury with conflicting evidence as to whether it was voluntary, the jurors are not bound to assume that the confession was made voluntarily simply because the judge held that it was admissible."). The circumstances here are different in two ways: First, the trial

[15] The rule from *Stevens*—that Article I, section 12, requires that the state prove the voluntariness of a statement by a preponderance of the evidence—is a rule that addresses the level of confidence that a trial court must have when acting as factfinder when determining the admissibility of the evidence. *See Stevens*, 311 Or at 137 (the "threshold question of voluntariness" is a question for the court when it determines admissibility). The issue we decide today also addresses the level of confidence a trial court must have in making a factual determination. We emphasize that that issue is distinct from the issue of what standard of review should apply on appeal. *See State v. Ward*, 367 Or 188, 196-200, 475 P3d 420 (2020) (determining what standard of review should apply to other questions under Article I, section 12). We need not address the issue of what standard of review applies to the trial court's finding under these circumstances because, as we have explained, the trial court did not conduct the required factfinding before issuing its order.

court in these circumstances is not tasked with determining, after the fact, whether a confession was voluntary; the court is being asked to use its power to compel defendant to provide testimonial evidence. Second, after the trial court makes the initial factual finding that a defendant knows the passcode to the phone, that question will not go to the jury. In these circumstances, *Soriano* requires heightened vigilance. First, although we have construed Article I, section 12, to permit an order compelling a defendant to unlock a cell phone when an equivalent substitute to the supplanted right is provided, we are cognizant of the dangers inherent in such a rule. The state will be prohibited from using that act to harm a defendant, but no prohibition on use can be precisely equivalent to invoking the privilege against self-incrimination. Second, requiring proof beyond a reasonable doubt provides necessary assurance that the state really does know the facts that the act of unlocking will convey. And third, we must remember that, if a defendant does not comply with an order compelling the act, the defendant can be held in contempt, as defendant was here. Because such an order would require a defendant to choose between relinquishing his or her right against self-incrimination or, potentially, facing punitive contempt proceedings, we think it fitting to apply the same standard when issuing the order as would be applied when enforcing it. *See* ORS 33.065(9) (to impose punitive sanctions for violation of a court order, proof of contempt "shall be beyond a reasonable doubt"). We agree with the concurrence in *Jones* that "a person's right to be free from self-incrimination is a fundamental principle of our system of justice," *Jones*, 481 Mass at 562, 117 NE3d at 721 (Lenk, J., concurring), and we therefore conclude that, to obtain an order requiring a defendant to unlock a cell phone, the state must prove, beyond a reasonable doubt, that it already knows the information that that act would communicate.

In this case, we have concluded that the trial court did not conduct the necessary factfinding to determine whether the state had established that defendant knew the passcode to the phone and could access it contents, and, therefore, that the second requirement that would have permitted the court to order defendant to unlock the phone

was not met. The third requirement—that the court's order expressly prohibit the state from using the compelled act against defendant—also was absent, although we recognize that the state apparently did not dispute that such a requirement would be appropriate. We conclude that the trial court's order compelling defendant to unlock the cell phone violated Article I, section 12.[16]

III. CONCLUSION

Although Article I, section 12, permits a trial court order compelling a defendant to unlock a cell phone in certain circumstances, those circumstances are not present in this case.

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

[16] Because we reverse defendant's conviction on state constitutional grounds, we do not reach defendant's federal constitutional argument.