

IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON,

Plaintiff-Respondent,
Respondent on Review,

v.

CATRICE PITTMAN,

Defendant-Appellant
Petitioner on Review.

Marion County Circuit
Court No. 16CN03799

CA A162950

SC S067312

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

Review of the Decision of the Court of Appeals
on Appeal from a Judgment
of the District Court for Marion County
Honorable TRACY A. PRALL, Judge

Opinion Filed: October 16, 2019
Author of Opinion: Aoyagi, Judge
Before: Hadlock, Presiding Judge, DeHoog, Judge, and Aoyagi, Judge

Continued...

ERNEST LANNET #013248
Chief Defender
Office of Public Defense Services
SARAH LAIDLAW #111188
Deputy Public Defender
1175 Court St. NE
Salem, Oregon 97301
Telephone: (503) 378-3349
Email:
sarah.laidlaw@opds.state.or.us

Attorneys for Petitioner on Review

KENDRA M. MATTHEWS # 965672
Boise Matthews Ewing LLP
1050 SW 6th Ave Ste 1400
Portland OR 97204
Telephone: (503) 228-0487
Email: kendra@boisematthews.com

Attorney for *Amici Curiae*
ACLU Foundation, ACLU of Oregon,
Inc., and Electronic Frontier
Foundation

ELLEN F. ROSENBLUM #753239
Attorney General
BENJAMIN GUTMAN #160599
Solicitor General
JONATHAN N. SCHILDT #151674
Assistant Attorney General
1162 Court St. NE
Salem, Oregon 97301-4096
Telephone: (503) 378-4402
Email:
jonathan.n.schildt@doj.state.or.us

Attorneys for Respondent on Review

FRANZ H. BRUGGEMEIER #
163533
Attorney at Law
PO Box 5248
Portland OR 97208
Telephone: (503) 867-9014
Email: fbruggemeier@ojrc.info

Attorney for *Amici Curiae*
Oregon Justice Resource Center and
Laurent Sacharoff

TABLE OF CONTENTS

INTRODUCTION	1
QUESTION PRESENTED AND PROPOSED RULE OF LAW	2
Question Presented	2
Proposed Rule of Law	3
STATEMENT OF FACTS	3
SUMMARY OF ARGUMENT	6
ARGUMENT	9
A. An order compelling a person to act may violate Article I, section 12 and the Fifth Amendment only if the act itself has a testimonial component that is not already known by the state.....	10
1. Compelling an act is impermissible only to the extent that it amounts to compelled testimony, because the right against self-incrimination does not prohibit compelling merely the production of evidence.	11
2. Compelling a person to produce evidence does not violate the right against self-incrimination when any testimonial aspect of the act is already known by the state and is thus a “foregone conclusion.”	13
3. The “foregone conclusion” principle distinguishes cases where a compelled act has true testimonial significance to the state from cases where the act is significant only as a means to access other evidence.	18
B. An order to unlock a phone by entering a password is constitutionally permissible when the state establishes that the person subject to the order knows the password.....	20
1. The act of password entry has value to the state because it provides a means to access to the contents of the phone, which are subject to a warrant and are not protected by the right against self-incrimination.....	21
2. When a state establishes that a person knows a phone password, requiring the person to enter it does not violate the right against self-incrimination.....	22
a. When the state demonstrates that a person	

knows the password to unlock a phone, the state shows that it knows the only testimony conveyed by the act of entry.....	23
b. Defendant’s arguments for a different rule misconstrue the testimonial aspect of the act of password entry.....	26
C. Defendant’s remaining arguments present no cognizable reason to adopt a rule that gives the act of unlocking a phone any greater constitutional significance.....	29
1. The authority defendant cites under Article I, section 12 does not support adopting the rule that she proposes.	30
2. Defendant’s concerns about the breadth of information that can be revealed through a cellphone search, to the extent valid, should be addressed under Article I, section 9 and the Fourth Amendment.	34
D. The trial court’s password-entry order was lawful.	37
CONCLUSION.....	39

TABLE OF AUTHORITIES

Cases Cited

<i>Commonwealth v. Gelfgatt</i> , 468 Mass 512, 11 NE3d 605 (2014).....	24
<i>Commonwealth v. Jones</i> , 481 Mass 540, 117 NE3d 702 (2019).....	21, 24, 25
<i>Doe v. United States</i> , 487 US 201, 108 S Ct 2341, 101 L Ed 2d 184 (1988)	12
<i>Fisher v. United States</i> , 425 US 391, 96 S Ct 1569, 48 L Ed 39 (1976) ..	11, 13, 14, 17, 18, 19, 20, 21, 22, 25, 28, 29, 30, 31, 32, 33, 35
<i>Kastigar v. United States</i> , 406 US 441, 92 S Ct 1653, 32 L Ed 212 (1972)	30, 31
<i>Seo v. State</i> , ___ Ind ___, 148 NE3d 952 (2020).....	36

<i>State v. Andrews</i> , ___ NJ ___, ___ A3d ___, 2020 WL 4577172 at *18 (Aug 10, 2020)..	25, 36
<i>State v. Black</i> , 150 Or 269, 42 P2d 171 (1935).....	12
<i>State v. Carcerano</i> , 238 Or 208, 390 P2d 923 (1964), <i>cert den</i> , 380 US 923 (1965)	12
<i>State v. Cram</i> , 176 Or 577, 160 P2d 283 (1945).....	12
<i>State v. Fish</i> , 321 Or 48, 893 P2d 1023 (1995).....	9, 11, 12, 13, 14, 23, 27
<i>State v. Fisher</i> , 242 Or 419, 410 P2d 216 (1966).....	12
<i>State v. Ghim</i> , 360 Or 425, 381 P3d 789 (2016).....	37
<i>State v. Hughes</i> , 252 Or 354, 449 P2d 445 (1969).....	13
<i>State v. Isom</i> , 306 Or 587, 761 P2d 524 (1988).....	34
<i>State v. Jancsek</i> , 302 Or 270, 730 P2d 14 (1986)...	16, 17, 18, 19, 20, 21, 22, 25, 29, 31, 33
<i>State v. Mansor</i> , 363 Or 185, 421 P3d 323 (2018).....	36
<i>State v. Pittman</i> , 300 Or App 147, 452 P3d 1011 (2019).....	3, 5, 28, 37
<i>State v. Soriano</i> , 68 Or App 642, 684 P2d 1220 (1984), <i>aff'd and opinion adopted</i> , 298 Or 392, 693 P2d 26 (1984).	30, 31, 33, 34
<i>State v. Tiner</i> , 340 Or 551, 135 P3d 305 (2006), <i>cert den</i> , 549 US 1169 (2007)	12
<i>State v. Tracy</i> , 246 Or 349, 425 P2d 171 (1967).....	12
<i>State v. Vondehn</i> , 348 Or 462, 236 P3d 691 (2010).....	33, 34

United States v. Hubbell,
530 US 27, 120 S Ct 2037, 147 L Ed 24 (2000) 18, 19, 32

United States v. Ponds,
454 F3d 313 (DC Cir 2006).....32

United States v. Spencer,
No. 17-cr-00259-CRB-1, 2018 WL 1964588 (ND Cal Apr 26, 2018)....20

Constitutional and Statutory Provisions

Or Const, Art I, § 9 9, 30, 34, 35, 36

Or Const, Art I, §12 1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 16, 17, 18, 20, 25, 29, 30,
..... 31, 33, 34, 35, 36, 37

US Const, Amend IV 9, 30, 34, 35, 36

US Const, Amend V ... 1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 16, 17, 18, 20, 25, 30, 31,
..... 33, 34, 35, 36, 37

Other Authorities

Orin S. Kerr,
Compelled Decryption and the Privilege Against Self-Incrimination,
97 Texas L Rev 767 (2019)..... 19, 20, 23, 25, 27, 28, 36

Orin S. Kerr,
*Executing Warrants for Digital Evidence: The Case for Use Restrictions
on Nonresponsive Data*,
48 Tex Tech L Rev 1 (2015)36

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

INTRODUCTION

The issue in this case arises from the state's efforts to execute a search warrant on a cellphone found in defendant's purse. When detectives attempted to search the phone, they discovered that a numeric password was required to access the phone's contents, which were encrypted. Because, without the password, the detectives could not execute the warrant, the state sought an order to compel defendant to unlock the phone by entering the password. In doing so, the state presented evidence that defendant knew the phone's password, and the trial court so found. The question on review is whether, under those circumstances, the trial court's order requiring defendant to unlock the phone violated her rights against self-incrimination under Article I, section 12, of the Oregon Constitution and the Fifth Amendment to the United States Constitution.

The answer is no. The state sought to compel the act of password entry to open the door to the contents of the phone, which the state had a right to access and which were not testimony protected by the privilege against self-incrimination. The privilege was implicated only because of testimony that possibly could be gleaned from performing the act, and all that entry of the password conveyed was knowledge of the phone's password. But because the

state showed that it already had independent evidence of that knowledge, the act of password entry did not provide the state with incriminating testimony to use against defendant and thus did not violate her rights against self-incrimination.

That result strikes the right constitutional balance: It safeguards the privilege against self-incrimination by ensuring that the state will not exploit the act of password entry for its testimonial value, but it also recognizes that, in cases like this one, the password presents a challenge to executing a valid warrant rather than an opportunity to gain testimony. And that balance appropriately accounts for rapid technological change: Individuals have always used locks to conceal information, but only recently has powerful encryption technology allowed anyone to create unbreakable digital locks that make it impossible to execute a warrant. Where, as here, the state establishes that entry of the password is valuable because it unlocks the phone and not because of whatever testimony it could provide, Article I, section 12 and the Fifth Amendment should not serve as an impediment to execution of the warrant.

QUESTION PRESENTED AND PROPOSED RULE OF LAW

Question Presented

When a court has issued a warrant to search a password-protected phone and the state establishes that a person knows the password, can the court compel the person to unlock the phone by entering the password?

Proposed Rule of Law

Yes. Because the testimonial aspect of the unlocking—that the person knows the password—is a foregone conclusion, an order compelling that act does not violate the right against self-incrimination.

STATEMENT OF FACTS

Defendant crashed her car into a tree, resulting in injuries to the five children and one adult who were passengers. *State v. Pittman*, 300 Or App 147, 149, 452 P3d 1011 (2019); (ER 2–3, 11–12).¹ After defendant was taken to the hospital, hospital staff and police found methamphetamine, a methamphetamine pipe, and \$1,230 in cash on defendant’s person. *Pittman*, 300 Or App at 149; (ER 3–4, 13–14). Defendant also had her purse with her, with an iPhone inside. *Pittman*, 300 Or App at 149; (ER 5, 14).

Based on evidence collected, the police suspected that defendant had operated a vehicle under the influence of intoxicants, operated a vehicle while distracted, and delivered methamphetamine. *Pittman*, 300 Or App at 149–150. The police obtained a warrant to search the iPhone in defendant’s purse. *Id.* at 150.

The police soon determined that they could not access the iPhone without a numeric password. *Id.* According to the police department’s technological

¹ The state refers to the ER attached to defendant’s brief on the merits in this court.

investigator, it would take “approximately a thousand years” using “the fastest computer we have access to” to access the information in the iPhone without the password. *Id.* And it was possible that the iPhone had been set to “delete itself” after 10 incorrect password entries, posing an additional risk. *Id.*

So that the state could execute the search warrant, the state sought to compel defendant to unlock the iPhone with the phone’s password. *Id.* Defendant refused, arguing that the court should deny the motion because complying with the court’s order would violate her right against self-incrimination under Article I, section 12 and the Fifth Amendment. Addressing that argument, the state explained that, to the extent that using a password to unlock a phone was a testimonial act—by implicitly conveying that defendant had “control” or “at least access” to the phone—the trial court nonetheless could compel the disclosure, because it was already a “foregone conclusion” that defendant had control over the phone. *Id.* The trial court ultimately agreed with the state that ordering defendant to disclose the password would not violate Article I, section 12 or the Fifth Amendment. *Id.* at 151. In doing so, it found that there was “probable cause to believe that defendant ha[d] knowledge of the passcode” for the phone. *Id.*

After granting the motion to compel, the trial court orally ordered defendant to enter the password into the phone. *Id.* at 151–52. Defense counsel asked that defendant “not be compelled to make any oral statements * * * or

any written statements.” (8/1/16 Tr 6). The trial court agreed to that, and it told defendant that “perhaps we can just hand [the phone] to you and you can unlock it without providing the information to us.” (8/1/16 Tr 7).

A detective handed defendant the phone. She entered a series of numbers that “disabled” the phone. (8/1/16 Tr 7). The detective later testified that he had seen defendant enter “123456” into the phone. (8/1/16 Tr 9). The court once again ordered defendant to enter the correct code, but defendant again entered “123456,” which again did not open the phone. (8/1/16/ Tr 17). The trial court found defendant in contempt and sentenced her to 30 days in jail. (8/1/16 Tr 18). In finding that defendant willfully violated the court’s order, the trial court necessarily found that she knew the correct password but refused to enter it. (8/1/16 Tr 16–18).

Defendant appealed and the Court of Appeals affirmed. The Court of Appeals reasoned that the act of password entry required analysis under Article I, section 12 and the Fifth Amendment because it had a “testimonial aspect,” in that it could reveal “defendant’s ‘knowledge’ of the passcode.” *Pittman*, 300 Or App at 160.² But the court explained that, when the state can already

² At the outset, the court explained that the only act at issue was the “entry of a numeric code into a smartphone”; the trial court had not ordered disclosure of a password orally or in writing, and defendant had made no argument regarding any possible distinction between entry of a password while observed or unobserved. *Pittman*, 300 Or App at 153 n 3.

establish that defendant knows the password, the act of entry has no testimonial significance to the state. Under those circumstances, the state “is not relying on a testimonial aspect” of the act to “make its case” and is instead seeking to compel action as a means to execute the warrant. *Id.* at 158, 161–62.

Because the trial court found that “defendant had knowledge of the passcode”—and defendant did not challenge any aspect of that determination on appeal—the Court of Appeals concluded that the trial court’s order compelling entry of the password was permissible under Article I, section 12 and the Fifth Amendment. *Id.* at 151, 162–63. The Court of Appeals therefore affirmed the trial court’s ruling.

SUMMARY OF ARGUMENT

Article I, section 12, of the Oregon Constitution and the Fifth Amendment to the United States Constitution prohibit the state from compelling a person to provide incriminating testimony. Courts have long recognized that an act may itself qualify as testimony. For example, a witness on the stand who nods her head in response to a question about a crime provides testimony; the physical act is meaningful only for what it says. Some acts, on the other hand, convey no testimony. The fact that a witness must open a door to walk into the courtroom does not convey her thoughts, beliefs, or knowledge.

Some acts fall somewhere in between. Consider the act required by an order to produce non-privileged documents to the state. Compliance with the

order results in physical delivery of the documents to the state; that is the point of the order. Yet there is also a risk that the act of handing over the documents could itself provide testimony to the state; when a person hands over documents, the person necessarily affirms that the documents were in her possession, for example. To safeguard against that risk—without cutting off the state’s access to the documentary or other physical evidence—courts employ a straightforward rule: An order compelling a person to act complies with Article I, section 12 and the Fifth Amendment, so long as any testimonial information the act provides is already known by the state.

That same rule applies to an order requiring a person to enter a phone password. Entering the password on a phone is significant for what it does; it provides the state access to the phone’s contents so that the state can execute a warrant. Yet there is a possibility that the state could rely on that act for what it says; when a person enters a password to unlock a phone, she also necessarily conveys that she knows the password. Accordingly, ordering password entry is constitutionally permissible when the state first demonstrates, to the court entering the order, that the person subject to the order knows the password. In doing so, the state demonstrates that it gains no testimonial advantage through performance of the act. The compelled act is significant only for what it does, not for what it says.

In this case, the state presented evidence to the trial court that defendant knew the password for the phone found in her purse, and the court credited that evidence in finding that defendant had knowledge of the password. Defendant did not challenge that finding in the Court of Appeals, and she does not challenge it on review. As a result, the trial court lawfully ordered defendant to enter the phone's password.

The arguments defendant presents on review, which reduce to three main contentions, provide no valid basis to reach a contrary conclusion.

Although defendant first argues that a person who enters a phone password provides the state with testimony that she knows, and in fact created, the contents of the phone, that argument misconstrues the testimonial significance of the act of password entry. A person who enters a phone password necessarily affirms that she knows the password; she does not affirm that she knows about, or created, the phone's contents.

Defendant otherwise urges this court to adopt a categorical rule that the foregone conclusion doctrine is "inapplicable" under Article I, section 12. But defendant acknowledges that both Article I, section 12 and the Fifth Amendment provide the same substantive protection to "testimonial" acts, and she identifies no constitutional principles unique to Article I, section 12 that support adopting the rule that she advocates.

Finally, underlying all of defendant's arguments is a contention that this court should limit the state's ability to search cellphones given the amount of information that those searches can reveal. But concerns about the breadth of cellphone searches, if valid, should be raised under Article I, section 9 and the Fourth Amendment. Article I, section 12 and the Fifth Amendment ensure that an order compelling that act does not provide the state with *testimonial* information it did not already have. Because the trial court's order gave the state no such advantage in this case, it was permissible under Article I, section 12 and the Fifth Amendment.

ARGUMENT

Under Article I, section 12, a person cannot be "compelled in any criminal prosecution to testify against himself." A nearly identical prohibition appears in the Fifth Amendment: "No person * * * shall be compelled in any criminal case to be a witness against himself[.]" As the text suggests, the substantive reach of both provisions is the same. Both provisions have the same historical origin and same animating principles, as defendant acknowledges. *See State v. Fish*, 321 Or 48, 54–56, 893 P2d 1023 (1995); (Pet Br at 9–10). And the protection under both provisions depends on the same three requirements: (1) testimony; (2) that is compelled; and (3) that is incriminating, because it could be used against the person in a criminal prosecution. *Fish*, 321 Or at 53.

The question in this case is how to apply those longstanding requirements to circumstances that result from recent technological developments: When the state obtains a warrant to search a password-protected phone and can also show that a particular person knows the password, does an order requiring that person to enter the password compel the person to provide the state with incriminating testimony?

Under both Article I, section 12 and the Fifth Amendment, the answer is no. As explained below, those provisions apply to a compelled act only if it conveys testimonial information not already known by the state through independent evidence. To the extent that the act of password entry could convey any testimony to the state, it is only that defendant knows the phone password. When the state can independently establish that fact, however, the act of entry has no testimonial significance to the prosecution; the person required to act provides the state access, not testimony. Here, given the trial court's unchallenged finding that defendant knew the password for the phone in her purse, the trial court correctly ordered defendant to enter the password for the phone, so that the state could execute a warrant to search it.

A. An order compelling a person to act may violate Article I, section 12 and the Fifth Amendment only if the act itself has a testimonial component that is not already known by the state.

The prohibition against compelled self-incriminating testimony, under both Article I, section 12 and the Fifth Amendment, extends to compelled acts.

But to apply that prohibition to acts, this court must determine the act's testimonial significance, if any. This case presents the problem arising when the act at issue is primarily valuable for what it delivers to the state: The act opens the door to physical or documentary evidence, which is not itself protected by Article I, section 12 or the Fifth Amendment. Yet, at the same time, there is at least a possibility that the state could rely on the act itself for the testimony that it implies.

The solution, first discussed in cases involving subpoenas to produce documents, is to determine whether the act at issue has any testimonial significance in the context of a particular case, apart from merely providing access to incriminating evidence, which can permissibly be compelled. When the state establishes that whatever testimony could be conveyed is already known to it, compelling the act gives the state no testimonial advantage and is constitutionally permissible. That holds true, as explained below, under Article I, section 12 and the Fifth Amendment.

- 1. Compelling an act is impermissible only to the extent that it amounts to compelled testimony, because the right against self-incrimination does not prohibit compelling merely the production of evidence.**

The state and federal constitutional protections against compelled self-incrimination extend only to evidence that is testimonial. *Fish*, 321 Or at 56 (Article I, section 12); *Fisher v. United States*, 425 US 391, 408, 96 S Ct 1569,

48 L Ed 39 (1976) (Fifth Amendment). Performing an act is not the equivalent of giving testimony, but some acts have a testimonial component that merits protection. The question is whether, by doing the act, the person must “reveal his or her thoughts” to the state. *Fish*, 321 Or at 56. In other words, does the act force a person “to disclose the contents of his own mind” in a way that conveys a “factual assertion”? *Doe v. United States*, 487 US 201, 210–11, 108 S Ct 2341, 101 L Ed 2d 184 (1988) (Fifth Amendment).

Many compelled acts—even acts that require the production of incriminating evidence—do not qualify as testimony under that test. Under Article I, section 12, the accused “may be required to stand up in court; to appear at the scene of the crime; to put on a blouse to see if it fits him; to place a handkerchief over his face; to stand up and remove his glasses; to remove his coat and shirt and permit the jury to see scars on his body and to don a shirt introduced in evidence; or to exhibit his arm so as to reveal tattoo marks thereon, which a previous witness swore were there.” *State v. Cram*, 176 Or 577, 582–83, 160 P2d 283 (1945) (citations omitted).³ Likewise, under the

³ See, e.g., *State v. Tiner*, 340 Or 551, 561–62, 135 P3d 305 (2006), *cert den*, 549 US 1169 (2007) (exposing the defendant’s tattoos to be photographed did not raise an issue of self-incrimination); *State v. Black*, 150 Or 269, 289, 42 P2d 171 (1935) (requiring a defendant to exhibit his body is not testimony about his body); *State v. Carcerano*, 238 Or 208, 215, 390 P2d 923 (1964), *cert den*, 380 US 923 (1965) (compelling the defendant to rise not testimonial); *State v. Fisher*, 242 Or 419, 422, 410 P2d 216 (1966) (handwriting

Footnote continued...

Fifth Amendment, the privilege does not extend to “the giving of blood samples,” or providing handwriting and voice exemplars, because those are acts are not “sufficiently testimonial.” *Fisher*, 425 US at 408, 411.

Those acts, to be sure, may require the actor to furnish evidence to the state that is incriminating. But none of the acts have testimonial significance because performing them does not require disclosing “beliefs, knowledge, or state of mind.” *Fish*, 321 Or at 56. Put another way, even though the act of producing evidence could give rise to an inference that the actor was involved in a crime, that does not render the act testimonial.

2. Compelling a person to produce evidence does not violate the right against self-incrimination when any testimonial aspect of the act is already known by the state and is thus a “foregone conclusion.”

The question of whether an act qualifies as testimony most often arises in a situation where the state has an interest in the act itself because of what it communicates. A person nodding her head in response to a question is a basic example. That act is significant to the state principally because of the information it communicates. In some situations, the state may seek to compel an act to gain the information that it communicates. A police officer directing a

(...continued)

exemplar could be taken without informing the defendant of right to counsel); *State v. Tracy*, 246 Or 349, 361, 425 P2d 171 (1967) (taking the defendant’s pants at arrest not testimonial); *State v. Hughes*, 252 Or 354, 355, 449 P2d 445 (1969) (handwriting not testimonial).

person to show on a map where she was driving at the time of an accident is compelling testimony because the person must “communicate information to the police about the individual’s beliefs, knowledge, or state of mind.” *Fish*, 321 Or at 60.

But this court, and other courts, also have confronted situations where the state seeks to require an act of a different sort, and for a different reason: The state asks a person to do something not because of what the act itself communicates to the state, but because the act provides a means to access other evidence. That is, the state is not interested in using the act itself as evidence to support a conviction. The facts of *Fisher* provide a classic example. In that case, IRS agents served summonses to obtain tax documents prepared by taxpayers’ accountants. The taxpayer argued that requiring him to turn over the documents violated his right against self-incrimination. In addressing that argument, the Court addressed two questions.

The Court first considered whether the evidence sought by the state was protected by the privilege against self-incrimination. The Court made clear that the answer was no. It did not matter that the documents might contain incriminating evidence, the Court explained, “for the privilege protects a person only against being incriminated by his own compelled testimonial communications.” *Fisher*, 425 US at 409. And because “the preparation of all of the papers sought * * * was wholly voluntary,” they were not “*compelled*

testimonial evidence, either of the taxpayers or of anyone else.” *Id.* at 409–10 (emphasis added).

But “the act of producing evidence in response to a subpoena” was no doubt compelled, and the Court went on to consider whether that act could provide the government with testimony independent of the documents’ content. *Id.* at 410. It could, the Court reasoned, because providing documents in response to a subpoena necessarily requires a person to assert certain beliefs—“tacit averments.” *Id.* Because a person cannot hand over documents that she does not think exists, the production necessarily conveys an affirmation of the documents’ existence. *Id.* When a person hands over the documents, she also necessarily communicates that she has “possession or control” over the documents. *Id.* And the person, who is providing the documents to comply with the summons, necessarily communicates a belief “that the papers are those described” in the summons. *Id.* Because turning over the document required the taxpayer to reveal beliefs about the documents’ existence, possession, and authenticity, it was possible that the government could use that information as implicit testimony apart from the documents themselves.

Yet that possibility did not violate the taxpayer’s right against self-incrimination because, in fact, the testimonial aspect of turning over the documents added “little or nothing to the sum total of the Government’s information.” *Id.* at 411. Given the nature of the tax documents at issue, it was

evident that the documents existed and that the taxpayer possessed them. Any implied testimony about the documents' existence or possession was a "foregone conclusion." *Id.* As for the taxpayer's implicit affirmation that the documents were what the government claimed, that did not help the government's case because the taxpayer had not prepared the document and was not competent to "vouch for their accuracy." *Id.* at 413. As a result, the government was "in no way relying on the 'truth-telling' of the taxpayer" to prove the existence, possession, or authenticity of the documents. *Id.* at 411. The "question [was] not of testimony but of surrender." *Id.* (internal quotation marks omitted).

This court came to the same conclusion when it considered a document-production order in *State v. Jancsek*, 302 Or 270, 730 P2d 14 (1986). In that case, the defendant had written a letter to Bundy saying that defendant planned to kill his wife. *Jancsek*, 302 Or at 272. The defendant carried out his plan, but by the time police learned about the letter, Bundy had already passed it along to the defendant's lawyer. *Id.* at 273. The trial court ordered the lawyer to produce the letter, rejecting the defendant's claim that doing so would violate his rights under Article I, section 12 and the Fifth Amendment. *Id.* Adopting

Fisher's reasoning under the Fifth Amendment and concluding that Article I, section 12 provided no broader protection, this court affirmed.⁴

In doing so, this court first determined that the letter itself was not protected by the privilege against self-incrimination. Echoing the reasoning of *Fisher*, this court explained that defendant's communication in the letter "had already been made," and the state did not "seek to compel defendant to make any communication." *Id.* at 285. And even if the act of turning over the letter had testimonial significance, as turning over the tax documents in *Fisher* did, that testimony told the government nothing more than it already knew. Because the state knew from Bundy about the document's existence, general content, and placement with defendant's lawyer, "compelled production of the document was not necessary to proof of its existence, nor was it any indication of defendant's belief that the letter was the document described in the state's motion and the court's order." *Id.* at 288. Ultimately, this court concluded

⁴ Although this court addressed *Fisher* in its discussion of Fifth Amendment case law, the inescapable conclusion of *Jancsek* is that Article I, section 12 provided no greater protection for the act at issue than *Fisher* recognized. The defendant in *Jancsek* argued that "analysis under Article I, section 12 would be similar and would require at least as much protection as under [*Fisher*]"—and made no principled argument for "broader" Article I, section 12 protection—but this court took up that question on its own, reasoning that the court would not address the federal constitutional claim unless the state claim failed. *Jancsek*, 302 Or at 282–83.

“that neither the state nor the federal constitution affords defendant the protection he seeks.” *Id.*

Fisher and *Jancsek* thus provide a rule in cases where the state seeks to compel a person to engage in an act that provides non-privileged evidence. Even if the act could have some testimonial character, compelling it presents no concern under Article I, section 12 or the Fifth Amendment when the state, because it has independent evidence establishing any testimonial information, already knows whatever testimonial information that the act conveys. Under those circumstances, compelling the act does not provide the state a testimonial advantage. Instead, the state seeks the physical surrender of physical evidence that the state is entitled to access; the act is just an act.

3. The “foregone conclusion” principle distinguishes cases where a compelled act has true testimonial significance to the state from cases where the act is significant only as a means to access other evidence.

Fisher and *Jancsek* both view the act at issue for what it is—a means for the government to get the documents it seeks, which are not themselves compelled testimony. At the same time, those cases recognize the risk that the state could seek to compel the production of documents not just because of what the government learns from the documents but because of what the government learns from the act. That was the case in *United States v. Hubbell*, 530 US 27, 120 S Ct 2037, 147 L Ed 24 (2000), for instance. In *Hubbell*, the

government subpoenaed a wide range of financial documents from the defendant in an effort to show that he had violated his previous commitment, as part of a plea agreement, to disclose all of his business dealings. 530 US at 30–31. Because the government had no knowledge of what documents defendant had or that they existed, the defendant’s act of assembling and producing 13,120 pages of documents allowed the government to gain that testimony to use for its case. *Id.* at 31, 45. In that circumstance, the compelled act violated the defendant’s right against self-incrimination. But when, as in *Fisher* and *Jancsek*, the implicit testimony in turning over documents was a foregone conclusion that gave the state nothing new, the act was one of “surrender,” not “testimony,” such that “no constitutional rights [were] touched.” *Fisher*, 425 US at 411 (internal quotation marks omitted).

The rule that emerges from *Fisher*, *Jancsek*, and *Hubbell* thus distinguishes between cases where a compelled act has true testimonial value to the state and cases where the act is valuable merely because it “open[s] the door” to other “treasure.” Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Texas L Rev 767, 777 (2019). “If opening the door implies incriminating testimony that the government does not already know, then the risk of compelled self-incrimination is real and the person has a privilege against opening the door that then necessarily blocks access to the treasure.” *Id.* at 778. That was the case in *Hubbell*. But if, as in

Fisher and *Jancsek*, “opening the door gives the government no prosecutorial advantage, then the risk of compelled self-incrimination is only a matter of form.” *Id.* The implicit testimony is an incidental byproduct of the act but has no substantive value: “When the testimony implicit in the door-opening is not in play, and is only an incidental matter of form rather than substance,” the privilege against self-incrimination does not block “access to the treasure.” *Id.*⁵

B. An order to unlock a phone by entering a password is constitutionally permissible when the state establishes that the person subject to the order knows the password.

The principles that the Supreme Court applied in *Fisher* and this court applied in *Jancsek* apply with the same force to the act at issue in this case: the entry of a numeric password into a phone. Ultimately, the state seeks to compel an act that provides access to other evidence—the contents of the phone, which the state has a lawful right to access under the warrant and which are not privileged under Article I, section 12 or the Fifth Amendment. But the act

⁵ *Fisher* and other decisions do not address whether, after showing that the testimonial aspect of an act is a foregone conclusion, the state could then introduce evidence at trial that a defendant performed the act. Of course, when the state has independent evidence of any testimony that the act conveys, it can present that evidence rather than evidence that defendant performed the act. And to the extent the state might attempt to introduce evidence of the act, estoppel principles may limit the state from doing so. *Kerr*, 97 Texas L Rev at 776 & n 52 (so stating); see *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (ND Cal Apr 26, 2018) (“Once [the defendant] decrypts the devices, however, the government may not make direct use of the evidence that he has done so.”).

required to access the phone creates, as a byproduct, information that the state could use because of its testimonial significance: When a person unlocks a phone by entering a password, she necessarily conveys that she knows the password. When the state already knows that information and thus has no use for it, though, requiring the act of unlocking—the act that enables execution of the warrant—does not violate the privilege against self-incrimination.⁶

- 1. The act of password entry has value to the state because it provides a means to access to the contents of the phone, which are subject to a warrant and are not protected by the right against self-incrimination.**

Like the documents at issue in *Fisher* and *Jancsek*, the content found on the phone is not itself subject to the privilege against self-incrimination. The

⁶ Although defendant acknowledges that the trial court ordered *entry* of the password into the phone and treats that as the act at issue, *amici* suggest that defendant was ordered to communicate or reveal her password to the state. (Sacharoff *Amici* Br at 4). The distinction could affect the analysis to the extent that communicating the password itself is viewed as a direct testimonial communication that presents different constitutional concerns from the act of entering the password. *See Commonwealth v. Jones*, 481 Mass 540, 547 n 9, 117 NE3d 702, 710 n 9 (2019) (noting “debate among courts and commenters” as to whether that distinction matters, but concluding that order at issue required only password entry).

Here, the trial court ordered defendant to enter the password; the trial court did not require defendant to state or write the password or display it to anyone when she entered it. To the extent that bystanders could see what defendant was typing on the phone, that is likely because defendant did not care to shield from view her act of entering “123456” rather than the password that unlocked the phone. Moreover, even if the trial court had ordered disclosure of the password, neither *amici* nor defendant explain what additional testimonial value that information would have to the state.

information on the phone, to the extent it is testimonial, did not result from state compulsion. And because the state has a warrant to search the phone, the state has a lawful right to access the phone's contents. The act of unlocking the phone provides the state with access to information that it has a right to access and that is not itself protected by the self-incrimination right.

As with the compelled act at issue in *Fisher* and *Jancsek*, then, the act of unlocking the phone has a primary utility that is not grounded in any testimony: The act is valuable not for what it tells the state but for what it allows the state to access. Just as the state subpoenas documents so that the state can access the documents' contents, the state seeks to compel password entry in order to gain access to the phone's contents. Put another way, the password entry is valuable only because it opens the door to the phone's contents.

2. When a state establishes that a person knows a phone password, requiring the person to enter it does not violate the right against self-incrimination.

The act of password entry requires further scrutiny for purposes of the self-incrimination right, however, because the act could be used for its testimonial value. As a byproduct of performing the compelled act—putting the password into the phone and unlocking it—a person necessarily communicates that she knows the password. Because there is a risk that state could make use of that implied testimony, a court must further also inquire

whether that testimony adds to the state's case. When it does not, an order compelling production does not violate the right against self-incrimination.

- a. When the state demonstrates that a person knows the password to unlock a phone, the state shows that it knows the only testimony conveyed by the act of entry.**

Entering a password into a phone provides the state with access to the phone's contents, but like the act of producing documents, the act itself must be examined to determine whether it could also provide the state with implicit testimony. Answering that question depends on what a person is ordered to do and what testimony, if any, the person implicitly asserts through the act of compliance. In this case, the trial court ordered entry of the password into the phone's password prompt. To comply, defendant had to do something—enter the password.

The act of entering the password into the phone necessarily communicates a single fact: "I know the password." Or, more specifically, compliance with an order to enter the password requires a person to affirm that fact: "If a person knows the password, he can enter it and unlock the device. If a person doesn't know the password, however, he can't enter it." Kerr, 97 Texas L Rev at 779. Because the compelled act of password entry requires disclosing "knowledge" of the password, the act gives rise to that testimony. *Fish*, 321 Or at 56.

In that respect, the act of password entry communicates less information than a response to a subpoena to produce documents. Both acts result in access to additional evidence, as explained, but what is ordered and the testimony that results are distinct. Because an order to enter a password does not direct a person to produce particular files described in an order, the subject is “not selecting documents and producing them, but merely entering a password.” *Commonwealth v. Gelfatt*, 468 Mass 512, 524 n 14, 11 NE3d 605, 615 n 14 (2014). The various beliefs that necessarily follow by complying with an order to assemble and produce identified documents do not follow from entry of the password, which does not require interaction with the contents of the phone at all. Entering a password affirms that a person knows the password, it does not affirm that a person knows the phone’s contents.

That distinction is borne out by common experience. “[F]amily members and significant others routinely know the passwords to each other’s cell phones,” for example, “and students are regularly given passwords to school-owned computers.” *Commonwealth v. Jones*, 481 Mass 540, 547 n 8, 117 NE3d 702, 710 n 8 (2019). The fact that a person can enter the passwords on the phones for her spouse, her mother, and a friend from college does not mean that she owns their phones, knows what files are on them, or created those files. It means that, at some point and for one reason or another, she gained knowledge of the password. “The fact of knowledge of a password is distinct

from the ownership or control of the device and its contents.” *Id.* For the person who unlocks the phone, the act of unlocking “would admit I know the passcode, but it wouldn’t admit that I know what is on the phone.” Kerr, 97 Texas L Rev at 779.

In sum, the act of password entry requires scrutiny under Article I, section 12, and the Fifth Amendment only to the extent it has testimonial significance. And the only testimony “conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password.” *Jones*, 481 Mass at 547, 117 NE3d at 710; *State v. Andrews*, ___ NJ ___, ___ A3d ___, 2020 WL 4577172 at *18 (Aug 10, 2020) (slip op at 40) (concluding that foregone conclusion doctrine met when state establishes the defendant’s “knowledge of the passcodes and that the passcodes enable access to the cellphones’ contents”). Accordingly, under the framework of *Fisher* and *Jancsek*, the state must establish that it already knows that testimony before the trial court may compel the act.

A straightforward rule thus results: When the state seeks an order requiring a person to enter a password so that it can execute a warrant to search a phone, the order is constitutionally permissible when the state first shows that a defendant knows the password that unlocks the phone. That showing demonstrates that any testimony that the act could provide is not “in issue” and would add nothing to the state’s case. *Fisher*, 425 US at 411–12. Under those

circumstances, the person required to act cannot avoid doing so by asserting the privilege against self-incrimination.

b. Defendant’s arguments for a different rule misconstrue the testimonial aspect of the act of password entry.

Although defendant acknowledges that a compelled act of production does not present constitutional concerns “when the state already knows and has proof of any testimonial evidence conveyed through that production,” she contends that the state must establish much more than knowledge of the password to obtain an order for password entry. (Pet Br 3). Under her view, by entering a password, a person testifies not just that she knows the password, she testifies to several “inferential communications”: I own the phone; I know the information on it; and I created and organized that information. (Pet Br 17–18). She contends that the act testifies to any “inference that the state would want a jury to draw.” (Pet Br 14). Defendant’s *amici* make a similar claim, arguing that the state must make the same showing for password entry as it does when it subpoenas documents; that is, the state must establish “that the files on the device exist, that the defendant possesses them, and that they are authentic.” (Sacharoff *Amici* Br at 5).

But only the testimonial component of the act that is subject to constitutional protection, and defendant and her *amici* misconstrue the testimony implicit in entry of a password.

For her part, defendant improperly conflates the testimony inherent in the act with what incriminating inferences that could be drawn from it. To be sure, a person who enters a password necessarily testifies that she knows the password. But performing that act does not independently testify that the person has knowledge of, or created, the phone's contents. Those are simply inferences that could be drawn from defendant's knowledge of the password. And the fact that inferences can be drawn from testimony does not mean that those inferences are themselves testimony. A person who testifies that she was present at a crime scene does not testify that she committed the crime, even if her testimony supports that inference. Kerr, 97 Texas L Rev at 780.

Defendant is thus mistaken in arguing that any incriminating inference that could be drawn from an act itself amounts to testimony. To the extent she draws that rule from *Fish*—in particular the holding that a person's refusal to perform field sobriety tests was incriminating testimony—she misreads that decision. *Fish*, 321 Or at 56. The refusal at issue in *Fish* was direct testimony, not an act, so this court did not address what testimony any *act* conveyed when it concluded that the refusal was incriminating testimony. *Fish*, 321 Or at 56. And although this court identified one inference that the state could draw from a refusal at trial, it did so in explaining why the refusal was testimonial evidence that could “be used in a criminal prosecution” against the defendant: “[T]he state wants the jury to infer from the fact of an individual's refusal that he or

she is saying, ‘I refuse to perform field sobriety tests because I believe I will fail them.’” *Id.* That an inference *could be* drawn against a defendant who refuses to perform a field sobriety test shows why the refusal is incriminating. But other inferences are possible, too, and a defendant who refuses a sobriety test does not testify to any or every inferable reason that she refused to perform the test. Put another way, the “ability to draw an inference from testimony does not amount to testimony about that inference.” Kerr, 97 Texas L Rev at 780.

Defendant’s *amici* likewise lose sight of the testimonial aspect of password entry in urging a mechanical comparison to producing subpoenaed documents. They argue that “the foregone conclusion exception applies to the documents produced because the act of producing them implicitly communicates information about their existence, who possesses them, and their authenticity,” so the same showing must be made about “the files on a device[.]” (Sacharoff *Amici* Br at 5–6). Indeed, *amici* argue that the state must identify the files on the device with “reasonably particularity” before a court can order entry of a password.

But that approach, as the Court of Appeals recognized, improperly applies “*Fisher*’s ‘existence, location, authenticity’ framework for document subpoenas to a very different context without adequately grappling with the significance of the different context.” *Pittman*, 300 Or App at 161. As already explained, the testimonial content of password entry and selection and

production of documents in response to a subpoena is different. The former act merely communicates knowledge of the password, while the latter act communicates knowledge about the documents that a person must assemble and produce. The foregone conclusion exception “applies to the documents” in subpoena cases only in the sense that complying with the subpoena requires the respondent to affirm certain facts about those documents. A person compelled to enter a password unlocks the phone so that *the state* can search it; she is not compelled to go through the phone to hand over individual files in decrypted form. Only in the latter case would compliance testify to what the person knows about the phone’s contents.

C. Defendant’s remaining arguments present no cognizable reason to adopt a rule that gives the act of unlocking a phone any greater constitutional significance.

Apart from her mistaken arguments concerning how the principles in *Fisher* and *Jancsek* should apply to the act of password entry, defendant presents two categorical arguments. Yet those arguments also miss the mark. Defendant finds no support for her contention that Article I, section 12 prohibits application of the foregone conclusion rationale—meaning that any compelled act of production would be barred, even when it has no testimonial significance in the state’s case. And defendant’s remaining argument—that this court should place limits on phone searches because of the vast information they

hold—improperly raises Article I, section 9 and Fourth Amendment questions in a case that concerns only Article I, section 12 and the Fifth Amendment.

1. The authority defendant cites under Article I, section 12 does not support adopting the rule that she proposes.

Although defendant acknowledges at the outset that the principles governing the scope of testimony covered by Article I, section 12 mirror those under the Fifth Amendment (Pet Br 9–11), she nevertheless contends that “the foregone conclusion doctrine is inapplicable under Article I, section 12.” (Pet Br 36). More specifically, defendant contends that this court’s decision in *State v. Soriano*, 68 Or App 642, 684 P2d 1220 (1984), *aff’d and opinion adopted*, 298 Or 392, 693 P2d 26 (1984), forecloses recognition of the foregone conclusion doctrine under Article I, section 12 in all circumstances. That is, defendant advocates for a rule that would create an absolute bar to any compelled act, whether a subpoena for documents or an order to enter a password, whenever the act could be ascribed some communicative content.

Defendant’s argument in support of that sweeping result proceeds in multiple steps. Defendant suggests, first, that the holding in *Fisher* relied, to some extent, on the principles of use and derivative use immunity discussed in *Kastigar v. United States*, 406 US 441, 92 S Ct 1653, 32 L Ed 212 (1972); she contends that *Fisher* and *Kastigar* rely on the same “idea.” (Pet Br 38).

Working from that premise, defendant argues that, by requiring transactional

immunity, *Soriano* rejected “the logic in *Kastigar*.”⁷ (Pet Br 38). And in doing that, defendant argues, this court implicitly rejected “the foregone conclusion doctrine in *Fisher*.” (Pet Br 38).

As an initial matter, that theory cannot be squared with this court’s application of the foregone conclusion doctrine in *Jancsek*. Two years after *Soriano*, this court in *Jancsek* applied the foregone conclusion rationale to an act of production. In doing so, this court found no Fifth Amendment violation, and it separately considered whether, for any reason, Article I, section 12 provided the defendant with broader protection. This court concluded that it did not. *Jancsek*, 302 Or 282–85. Accordingly, if *Soriano* implicitly rejected the foregone conclusion doctrine under Article I, section 12, as defendant now contends, this court ruled to the contrary in *Jancsek*.

In any event, the premise underlying defendant’s implicit-rejection theory—that *Fisher*’s analysis relies on *Kastigar*’s “logic”—is incorrect. The Court in *Fisher* did not rely on the immunity principles discussed in *Kastigar* in its analysis; the Court cited *Kastigar* along with a slew of other cases in rejecting the argument that the Fifth Amendment protects “private information”

⁷ Use and derivative use immunity permits future prosecution of a witness granted immunity but only the if state does not use the immunized testimony or any of its direct or indirect fruits, whereas transactional immunity makes the witness immune from prosecution for any offense to which the immunized testimony relates. *Soriano*, 68 Or App at 645 n 3.

even when that information does not constitute self-incriminating testimony. *Fisher*, 425 US at 400. Indeed, if *Fisher* rested on immunity principles, its result would be possible only if the government could grant immunity to any testimony inherent in the act of production and then use the documents obtained as a result of production. But the government cannot do so. *See Hubbell*, 530 US at 42–43 (so explaining in addressing derivative use immunity); *United States v. Ponds*, 454 F3d 313, 321 (DC Cir 2006) (explaining that, in *Hubbell*, the Court held that if immunity is granted for act of production, “the use of the contents of produced documents [are a] barred derivative use of the compelled testimonial act of production”).

The reason that the foregone conclusion doctrine and immunity principles operate differently is that they do not rest on the same “idea.” (Pet Br 38). The foregone conclusion doctrine reasons that, when the state *has already shown* that it has no need for any testimonial information that could be drawn from an act to produce evidence, compelling the act does not constitute compelled self-incrimination. The state has demonstrated that the act has no value as testimony and instead is valuable only because it opens the door to other, non-privileged evidence. The whole point of a grant of immunity, on the other hand, is that the state *does* need to make use of constitutionally protected testimony. A grant of immunity safeguards the testimony and prevents the state from using it going forward.

Application of the foregone conclusion doctrine is consistent with the rationale underlying *Soriano*'s adoption of transactional immunity. *Soriano* reasoned that transactional immunity is necessary to avoid the risk that a prosecutor will use immunized testimony not just for evidentiary purposes but also for non-evidentiary purposes; for example, the immunized testimony could affect the prosecutor's discretionary decisions about trial strategy and other matters. *Soriano*, 68 Or App at 662–63. But the foregone conclusion doctrine applies only if the state shows that the information that a compelled act could convey is already known. By making that showing, the state confirms—at the outset—that it need not use the testimony inherent in the act for any purposes, whether evidentiary or non-evidentiary.

In sum, *Soriano*'s requirement that the government can compel testimonial evidence only on a grant of transactional immunity, and the analysis supporting that result, does not support defendant's proposed analysis with respect to what constitutes compelled testimony under Article I, section 12. *Fisher* and *Jancsek* set out the proper framework under that provision and the Fifth Amendment. Nothing in *Soriano*, or the other Article I, section 12 decisions that defendant cites, provides a basis to conclude otherwise.⁸

⁸ Without analysis, defendant cites to other decisions under Article I, section 12—*State v. Vondehn*, 348 Or 462, 236 P3d 691 (2010), and *State v.*

Footnote continued...

2. Defendant’s concerns about the breadth of information that can be revealed through a cellphone search, to the extent valid, should be addressed under Article I, section 9 and the Fourth Amendment.

Defendant and her *amici* present one final consideration in an effort to support the rule they propose. Describing phones as “prolific devices [that] store a vast and diverse trove [of] private information,” defendant argues that “the creation and organization of information within a cellphone conveys a person’s thoughts” and thus “adds to the testimonial nature of the disclosure.” (Pet Br 1, Pet Br 17–18 (citing Fourth Amendment cases)). Defendant’s *amici* put the point more bluntly, asserting that a strict self-incrimination rule is necessary to avoid “drastic incursions on individual privacy” because “existing Fourth Amendment case law imposes virtually no limits on digital searches.” (Sacharoff *Amici* Br at 38). Whatever the merit of those arguments, they

(...continued)

Isom, 306 Or 587, 761 P2d 524 (1988). (Pet Br 36). But like *Soriano*, they do not speak to the question presented here.

Those decisions instead involve testimony that was unquestionably privileged under Article I, section 12; as a result, they do not address what statements or actions qualify as privileged self-incriminating testimony. *E.g.*, *Vondehn*, 348 Or at 466 (conceded violation of *Miranda*). And in drawing a distinction between remedies required for violations of Article I, section 12 and the Fifth Amendment, those decisions identify constitutional principles that are unique to Article I, section 12’s exclusionary rule. *See id.* at 474 (addressing unique status of *Miranda* warnings under Oregon Constitution). Defendant identifies no unique state constitutional principles applicable to the question here.

provide no reason to adopt the self-incrimination rule that defendant proposes.

That is so for two main reasons.

First, those arguments do not address the act that is at issue under Article I, section 12 and the Fifth Amendment—entry of the password to unlock the phone. Instead, those arguments concern what the state has the ability to do once it gains access to the phone’s contents. Article I, section 12 and the Fifth Amendment protect “against compelled self-incrimination, not the disclosure of private information.” *Fisher*, 425 US at 401 (internal quotation marks and brackets omitted). For purposes of those provisions, there is no distinction between a person entering a combination to open the drawer of a file cabinet and a person entering a password to open a phone; the testimonial significance of the act of entering numbers is the same. The fact that, under the authority of a warrant, the state could later discover “private” information that “convey a person’s thoughts” has no import under Article I, section 12 or the Fifth Amendment. (Pet Br 17–18). This court should not rely on concerns unique to phones as a reason to adopt a categorical rule that will apply equally to file cabinets.

Second, and relatedly, the concerns that defendant and *amici* raise, if valid, should be addressed under Article I, section 9 or the Fourth Amendment. To the extent there is a need for greater privacy protection to account for the amount of electronically stored information that is subject to search (Sacharoff

Amici Br at 38), courts can craft appropriate rules under the constitutional provisions that govern searches. *See Kerr*, 97 Texas L Rev at 797 & n 156 (suggesting that concerns about invasive searches could be addressed by “use restrictions on nonresponsive data” under the Fourth Amendment, as described in Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex Tech L Rev 1 (2015)). Indeed, this court has already done so. *See State v. Mansor*, 363 Or 185, 221, 421 P3d 323 (2018) (“We thus conclude that the state should not be permitted to use information obtained in a computer search if the warrant did not authorize the search for that information, unless some other warrant exception applies.” (Citing *Kerr*, 48 Tex Tech L Rev at 24).).

At bottom, this court should not craft Article I, section 12 rules to address Article I, section 9 concerns.⁹

⁹ The decisions cited by defendant and her *amici* not only misapply Fifth Amendment principles by misconstruing the testimonial aspect of password entry, they expressly rely on Fourth Amendment concerns about the amount of information a cellphone search can reveal to create new Fifth Amendment limitations on those searches. *See, e.g., Seo v. State*, ___ Ind ___, 148 NE3d 952, 959–60 (2020) (expressing concerns about “the unique ubiquity and capacity of smartphones” and the fact that cellphone searches are conducted “without limitation”). As the New Jersey Supreme Court has explained, “it is problematic to meld the production of passcodes with the act of producing the contents of the phones,” because “that approach imports Fourth Amendment privacy principles into a Fifth Amendment inquiry.” *State v. Andrews*, ___ NJ ___, ___ A3d ___, 2020 WL 4577172 at *17 (Aug 10, 2020) (slip op at 38).

D. The trial court's password-entry order was lawful.

The trial court lawfully ordered defendant to enter the password for the phone found in her purse. Before ordering defendant to do so, the trial court found, from the evidence presented by the state, that defendant knew the password. *Pittman*, 300 Or App at 151. As a result, the trial court's order for defendant to enter the password was permissible under the Article I, section 12 and the Fifth Amendment. That is because the state demonstrated that it would have no need to use defendant's entry of the password for its testimonial value. That act had value to the state because it allowed the state to execute the warrant to search the phone.

Because defendant is mistaken that the trial court was required to apply any different legal analysis, she presents no reason to reverse the trial court's judgment. As the Court of Appeals explained, defendant did not challenge the trial court's finding that she knew the phone's password. *Pittman*, 300 Or App at 162–63. She cannot present that argument for the first time now. *See, e.g., State v. Ghim*, 360 Or 425, 442, 381 P3d 789 (2016) (“When a party has lost in the Court of Appeals, that party cannot ask us to reverse the Court of Appeals decision on a ground that the party did not raise in that court.”). In any event, on review defendant does not challenge the trial court's finding that she knew the phone's password. Defendant contends only that evidence that “[p]olice found the cellphone in defendant's purse at the hospital after she crashed her

vehicle” was not “*strong* evidence that defendant owned the phone and accessed its contents.” (Pet Br 32–33 (emphasis added)).

Accordingly, as in the Court of Appeals, defendant presents no argument that the trial court could not permissibly find from the evidence that she knew the phone’s password. And she does not otherwise argue that the court erred in making that determination.¹⁰ As a result, defendant presents no basis to reverse the trial court’s judgment.

////

////

////

////

////

////

////

////

¹⁰ Because defendant did not challenge the trial court’s determination that she knew the phone’s password, the Court of Appeals had no occasion to address “complicated questions” concerning the proper standard of review and standard of proof for that determination. *Pittman*, 300 Or App at 163 n 10; *see United States v. Spencer*, No 17-cr-00259-CRB-1, 2018 WL 1964588 at *1–3 (ND Cal Apr 26, 2018) (addressing standard of proof). Defendant’s arguments on review again do not require resolution of those questions, which can be addressed in a future case.

CONCLUSION

For the reasons set out above, this court should affirm the decision of the Court of Appeals and the judgment of the trial court.

Respectfully submitted,

ELLEN F. ROSENBLUM

Attorney General

BENJAMIN GUTMAN

Solicitor General

/s/ Jonathan N. Schildt

JONATHAN N. SCHILDT #151674

Assistant Attorney General

jonathan.n.schildt@doj.state.or.us

Attorneys for Respondent on Review

State of Oregon

NOTICE OF FILING AND PROOF OF SERVICE

I certify that on August 11, 2020, I directed the original Brief on the Merits of Respondent on Review, State of Oregon to be electronically filed with the Appellate Court Administrator, Appellate Records Section, and electronically served upon Ernest Lannet and Sarah Laidlaw, attorneys for petitioner of review, Kendra M. Matthews, attorney for *amici curiae* ACLU Foundation and ACLU of Oregon, Inc., and Franz H. Bruggemeier, attorney for *amici curiae* Oregon Justice Resource Center and Laurent Sacharoff, by using the court's electronic filing system.

CERTIFICATE OF COMPLIANCE WITH ORAP 5.05(1)(d)

I certify that (1) this brief complies with the word-count limitation in ORAP 5.05(1)(b) and (2) the word-count of this brief (as described in ORAP 5.05(1)(a)) is 9,633 words. I further certify that the size of the type in this brief is not smaller than 14 point for both the text of the brief and footnotes as required by ORAP 5.05(3)(b).

/s/ Jonathan N. Schildt

JONATHAN N. SCHILDT #151674
Assistant Attorney General
jonathan.n.schildt@doj.state.or.us

Attorney for Respondent on Review
State of Oregon