IN THE COURT OF APPEALS OF THE
STATE OF OREGON

STATE OF OREGON,
Plaintiff-Respondent,
v.
CATRICE PITTMAN,
Defendant-Appellant.

Marion County Circuit Court
16CN03799; A162950

Tracy A. Prall, Judge.

Argued and submitted July 30, 2018.

Sarah Laidlaw, Deputy Public Defender, argued the cause for appellant. Also on the brief was Ernest G. Lannet, Chief Defender, Criminal Appellate Section, Office of Public Defense Services.

Jennifer S. Lloyd, Assistant Attorney General, argued the cause for respondent. Also on the brief were Ellen F. Rosenblum, Attorney General, and Benjamin Gutman, Solicitor General.

Before Hadlock, Presiding Judge, and DeHoog, Judge, and Aoyagi, Judge.

AOYAGI, J.

Affirmed.

AOYAGI, J.

This appeal presents a question of first impression for us under Article I, section 12, of the Oregon Constitution and the Fifth Amendment to the United States Constitution: whether a court ordering a suspect to enter the passcode into a smartphone, which the police have lawfully seized and have a warrant to search but are unable to access without the passcode, violates the suspect's rights against compelled self-incrimination. In this case, defendant was held in contempt after failing to comply with a court order to enter the correct passcode into a seized iPhone.

We agree with the trial court and the parties that the act of entering a passcode into a smartphone is testimonial in nature. It communicates an assertion of fact—specifically that the suspect knows the passcode and, by extension, has access to the device (as its owner or otherwise)—and therefore is subject to protection under Article I, section 12, and the Fifth Amendment. We also agree with the trial court and the parties that it was appropriate to apply the "foregone conclusion" doctrine recognized under the Fifth Amendment and, as a matter of first impression, adopt that doctrine for purposes of Article I, section 12. As for how that doctrine applies in this context, we conclude that, before the court could order defendant to enter the passcode into the iPhone, the state had to prove that defendant's knowledge of the passcode was a foregone conclusion. The state did not, however, have to prove that the contents of the iPhone were a foregone conclusion. Given the latter conclusion, defendant's challenge to the court's ruling (as presented in her opening brief) is not viable, and we affirm.

FACTS

Defendant was the suspected driver in a single-vehicle accident in which a car struck a tree. At the hospital, hospital employees found white powder, drug paraphernalia, and cash on her person, which they gave to the police. Defendant also had a purse with her at the hospital; the purse contained an iPhone.

Based on evidence collected, the police suspected that defendant had operated a vehicle under the influence

of intoxicants, operated a vehicle while distracted, delivered methamphetamine, and/or conspired to deliver methamphetamine. As relevant here, the police obtained a warrant to search the iPhone in defendant's purse. The police soon determined that they could not access the iPhone without a passcode. According to the police department's technological 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 passcode. Further, the investigator testified, an iPhone can be set to "delete itself" after 10 incorrect passcode entries, posing an additional risk.

The state moved to compel defendant to disclose the iPhone's passcode. Anticipating a constitutional challenge, the state asserted that, to the extent that disclosing a passcode is a testimonial act, in that it "inferentially communicate[s] that [defendant] ha[s] control over—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. As discussed later, "foregone conclusion" is a term of art from Fifth Amendment jurisprudence. Defendant opposed the state's motion, arguing, first, that the warrant was overbroad and, second, that compelling her to disclose the passcode to the iPhone would violate Article I, section 12, and the Fifth Amendment. On the latter issue, defendant focused on the act being testimonial in nature and did not directly address the "foregone conclusion" issue. In reply, the state defended the warrant, and it reiterated its "foregone conclusion" argument in more detail.

The trial court held a hearing on the state's motion. The state argued, consistently with its briefing, that it was a foregone conclusion that defendant knew the passcode and had access to the iPhone and that compelling her to disclose the passcode therefore would not violate Article I, section 12, or the Fifth Amendment. In response, defendant argued that the foregone conclusion doctrine did not apply because the state failed to establish that the "desired evidence" actually existed on the iPhone, that defendant was in control of the iPhone and its passcode, and that the "desired evidence" on the iPhone was authentic. Defendant asserted

that the state had to satisfy all three requirements for the doctrine to apply.[1] The state argued in rebuttal that it had established that defendant was in control of the iPhone and passcode and that requiring it to prove what was on the iPhone before searching it would "put[] the cart before the horse." In the state's view, there was no need for it to prove what was on the iPhone, beyond meeting the probable-cause requirements for the warrant.

After the hearing, the trial court issued a letter opinion, ruling in the state's favor on the "foregone conclusion" issue and also ruling, subject to certain limitations, that the warrant was not overbroad. The trial court began its analysis by making several statements about "probable cause," including that there was "probable cause to believe that defendant has knowledge of the passcode and contents of the iPhone." The court then described its understanding of the foregone conclusion doctrine in a manner consistent with defendant's argument—and inconsistent with the state's argument—but nonetheless agreed with the state as to the result, *i.e.*, that ordering defendant to disclose the passcode would not violate Article I, section 12, or the Fifth Amendment:

> "The foregone conclusion exception applies when the state can prove its independent knowledge of three elements: the documents' existence, the documents' authenticity, and respondent's possession or control of the document. The court finds, based on the evidence found and Officer Boyce's training and experience, that it is a foregone conclusion that the iPhone will contain evidence of the crimes of unlawful delivery of a controlled substance and conspiracy to commit delivery of a controlled substance."

On the same day that the trial court issued its letter opinion, the parties appeared before the court, and the court orally ordered defendant to enter the passcode into

[1] The trial court gave defendant leave to file a supplemental brief on the foregone conclusion issue after the hearing. She did so. As she had at the hearing, defendant argued in her supplemental brief that, to satisfy the foregone conclusion doctrine, the state had to prove that the information the state was seeking was on the iPhone, that the iPhone was in defendant's control or that she knew the passcode, and that the state had "*actual knowledge* of incriminating evidence on the phone." (Emphasis in original.)

the iPhone. An officer observed defendant enter "123456," which failed to unlock the iPhone. The court again ordered defendant "to enter the appropriate code," warning her that, "[i]f you enter a wrong code again, you would be in contempt of court." Defendant again entered "123456," which again failed. The court found defendant in contempt of court and sentenced her to 30 days in jail.

Defendant appeals the contempt judgment, challenging both the underlying order requiring her to disclose the passcode and the contempt judgment itself, which the state agrees is permissible under the circumstances of this case.[2] Defendant raises two assignments of error. First, she argues that the trial court erred in ordering her to enter the passcode into the iPhone, because it violated her rights under Article I, section 12, and the Fifth Amendment. We address that issue below. Second, she argues that the trial court plainly erred in holding her in contempt, because the evidence was insufficient to establish a "willful" violation. Applying the standard for plain error review, we reject the second assignment of error without written discussion.

OREGON CONSTITUTIONAL ANALYSIS

We begin with Article I, section 12, because we typically "consider[] state constitutional claims before considering federal constitutional claims." *State v. Cookman*, 324 Or 19, 25, 920 P2d 1086 (1996).

Under Article I, section 12, a person cannot be compelled to testify against himself or herself in a criminal prosecution. Or Const, Art I, § 12 ("No person shall *** be compelled in any criminal prosecution to testify against himself."). That protection applies "to any kind of judicial or nonjudicial procedure in the course of which the state seeks to compel testimony that may be used against the witness

[2] Typically, on appeal of a contempt judgment, the defendant cannot collaterally attack the underlying order. *State ex rel Mix v. Newland*, 277 Or 191, 200, 560 P2d 255 (1977). However, an exception applies when the defendant had no meaningful opportunity to obtain appellate review of the underlying order before violating it and when compliance with the order would have resulted in irremediable harm. *State v. Crenshaw*, 307 Or 160, 165-68, 764 P2d 1372 (1988). As the state notes, in this case, defendant requested a stay of the underlying order so that she could pursue mandamus, but that request was denied, and the court's order required immediate compliance.

in a criminal prosecution." *State v. Langan*, 301 Or 1, 5, 718 P2d 719 (1986). There are three requirements to trigger Article I, section 12, protection: (1) testimony; (2) that is compelled; and (3) that could be used against the person in a criminal prosecution. *State v. Fish*, 321 Or 48, 53, 893 P3d 1023 (1995). "Testimony" includes not only speech but also acts that communicate a person's "beliefs, knowledge, or state of mind." *Id.* at 56. "For an individual to reveal his or her thoughts is necessarily to make a communication, whether by words or actions." *Id.*

In this case, there is no real dispute that the three requirements for Article I, section 12, protection are met. The trial court necessarily concluded that the act of entering a passcode into an iPhone is testimonial, that a court order is compulsory, and that the state could use defendant's implicit testimony against her in a criminal prosecution—otherwise the court never would have reached the "foregone conclusion" issue. The state also appropriately concedes each of those points on appeal, and we agree. The act of entering a passcode into a smartphone is testimonial in nature, because it 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.[3] A court order is an "obvious example[]" of compulsion. *Fish*, 321 Or at 57. And there is no question that, if incriminating evidence is found on the iPhone, evidence of defendant's access to the iPhone could be used against her in a criminal prosecution.

The dispute in this case instead centers on the trial court's application of the "foregone conclusion" doctrine, a doctrine first articulated in *Fisher v. United States*, 425 US

[3] We consider in this case only the act that defendant was ordered to perform: entry of a numeric passcode into a smartphone. Most courts to consider the issue have agreed that that is a testimonial act. *See G. A. Q. L. v. State*, 257 So3d 1058, 1061 (Fla Dist Ct App 2018) (collecting cases). By contrast, the law is far less developed regarding compelling the use of a fingerprint or other biometric data to unlock an electronic device. We express no opinion on whether compelling someone to use their fingerprint or other biometric data to unlock an electronic device would implicate Article I, section 12. Because defendant has not raised the issue or made any argument regarding it, we also express no opinion as to any possible distinction between ordering someone to enter a passcode unobserved, ordering someone to enter a passcode while observed, or ordering someone to disclose a passcode orally or in writing.

391, 411, 96 S Ct 1569, 48 L Ed 2d 39 (1976), in the analogous context of the Fifth Amendment. As discussed more later, the United States Supreme Court held in *Fisher* that the compulsion of a physical act with a testimonial aspect does not violate the Fifth Amendment so long as the "testimony" at issue is a foregone conclusion. Here, the trial court concluded that there was "probable cause to believe that defendant has knowledge of the passcode and contents of the iPhone" and that it was "a foregone conclusion that the iPhone will contain evidence of the crimes of unlawful delivery of a controlled substance and conspiracy to commit delivery of a controlled substance." On that basis, the court concluded that compelling defendant to enter the passcode would not violate her rights under Article I, section 12, or the Fifth Amendment.

On appeal, defendant argues that the trial court erred in its application of the "foregone conclusion" doctrine. In her opening brief,[4] defendant contends, as she did in the trial court, that, for the doctrine to apply, the state had to establish both that the contents of the iPhone were a foregone conclusion (known to the state with "reasonable particularity") *and* that defendant's knowledge of the passcode was a foregone conclusion. Defendant argues that the trial court erred in finding that the iPhone's contents were a foregone conclusion, because, in her words, "the content of the sought evidence was unknown to police" and "[t]he state did not state with any reasonable particularity the contents of the phone." As for her knowledge of the passcode, defendant addresses that issue in only three sentences—she points out that she has never admitted to owning the iPhone, acknowledges that its presence in her purse "permitted an inference that [she] owned the phone," but asserts that typing in the passcode "would be new and stronger evidence that [she] owned the phone."

In response, the state argues that, to rely on the "foregone conclusion" doctrine, it needed to establish only that it was a foregone conclusion that defendant knew the

[4] We limit our discussion to the arguments contained in defendant's opening brief and do not address new arguments made for the first time at oral argument. *See Colton and Colton*, 297 Or App 532, 547-48, 443 P3d 1160 (2019).

passcode—and that it met that requirement. The state asserts that it was not required to prove anything about the contents of the iPhone. Thus, the state implicitly disagrees with the trial court's approach—which included determining that the contents of the iPhone were a foregone conclusion—but it defends the trial court's ultimate conclusion that ordering defendant to enter the passcode would not violate Article I, section 12.

Given the parties' arguments, we must consider whether and how the "foregone conclusion" doctrine applies under Article I, section 12. Because there is no Oregon case law on point, we begin by describing the doctrine as articulated by the United States Supreme Court for purposes of the Fifth Amendment.

Under the Fifth Amendment, like Article I, section 12, the government generally cannot compel a person to commit an act that is "testimonial" in nature and that can be used against the person in a criminal prosecution. *United States v. Hubbell*, 530 US 27, 34-35, 120 S Ct 2037, 147 L Ed 2d 24 (2000). An act is "testimonial" for Fifth Amendment purposes if it communicates "either express or implied assertions of fact or belief." *Id*. at 35. We apply a similar standard under Article I, section 12. *Fish*, 321 Or at 56 ("Facts giving rise to inferences, no less than direct statements, communicating an individual's state of mind is evidence that is subject to the right against compelled self-incrimination."). Both the United States Supreme Court and the Oregon Supreme Court have adopted a rule of thumb to identify testimonial acts: If answering a question or complying with a directive requires the person to choose between telling the truth or telling a lie, it is likely testimonial in nature. *See Pennsylvania v. Muniz*, 496 US 582, 597, 110 S Ct 2638, 110 L Ed 2d 528 (1990) ("Whenever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component." (Footnote omitted.)); *Fish*, 321 Or at 57-58 (positing the same "cruel trilemma" for purposes of Article I, section 12).

The United States Supreme Court has long held that the act of producing documents in response to a government subpoena may be sufficiently testimonial to trigger Fifth Amendment protection—and we briefly discuss that case law because it is where the "foregone conclusion" doctrine arose. The fact that the subpoenaed documents themselves may contain incriminating information is irrelevant to the Fifth Amendment analysis, because they were created voluntarily, not under compulsion. *Hubbell*, 530 US at 36. Nonetheless, "[t]he act of producing evidence in response to a subpoena *** has communicative aspects of its own, wholly aside from the contents of the papers produced." *Fisher*, 425 US at 410. The act of production may require the subpoena recipient to "communicate information about the existence, custody, and authenticity of the documents," making the act testimonial in nature. *Hubbell*, 530 US at 36-37.

In *Fisher*, the Court concluded that a government subpoena did not violate the Fifth Amendment where the existence and location of the subpoenaed documents was a "foregone conclusion," such that the act of producing them was not testimonial in nature. 425 US at 411-12. In that case, Internal Revenue Service agents served summonses on taxpayers' attorneys to obtain documents prepared by the taxpayers' accountants. *Id.* at 394. Because the IRS already knew what documents existed and where they were located, the Court concluded that any tacit admissions communicated by the act of production would "add[ ] little or nothing to the sum total of the Government's information." *Id.* at 411. The "existence and location of the papers [was] a foregone conclusion," so "[t]he question [was] not of testimony but of surrender."[5] *Id.* This is sometimes called the "foregone conclusion exception" to Fifth Amendment protection. *E.g.*, *G. A. Q. L. v. State*, 257 So3d 1058, 1063 (Fla Dist Ct App 2018) ("In general, if the state can meet the requirements of the foregone conclusion exception, it may compel otherwise ostensibly self-incriminating testimonial production of information.").

[5] We note that, in *Fisher*, the subpoena recipient's *personal knowledge* of the existence, location, and authenticity of the subpoenaed documents did not have independent significance as incriminating evidence.

By contrast, in *Hubbell*, the Court concluded that a subpoena violated the Fifth Amendment where it was written so broadly as to require the defendant to apply his own mental processes to identify and assemble responsive documents for the prosecution, in a manner akin to answering a detailed interrogatory or series of deposition questions:

> "It is apparent from the text of the subpoena itself that the prosecutor needed [the defendant's] assistance both to identify potential sources of information and to produce those sources. Given the breadth of the description of the 11 categories of documents called for by the subpoena, the collection and production of the materials demanded was tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions. The assembly of literally hundreds of pages of material in response to a request for 'any and all documents reflecting, referring, or relating to any direct or indirect sources of money or other things of value received by or provided to' an individual or members of his family during a 3-year period is the functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition."

530 US at 41-42 (internal citations omitted).

In *Hubbell*, the Court rejected the government's argument that the "foregone conclusion" doctrine applied. Referring to *Fisher*, the Court stated, "Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it." *Hubbell*, 530 US at 44. "While 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, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent." *Id.* at 44-45. Notably, in *Hubbell*, the government had an opportunity earlier in the case to demonstrate with "reasonable particularity" its independent knowledge of the requested documents' existence and authenticity, but it could not do so. *Id.* at 33.

Having examined *Fisher* and *Hubbell*, we understand the "foregone conclusion" doctrine, as articulated for Fifth Amendment purposes in the context of document subpoenas, as follows. If the existence, location, and authenticity of documents is a foregone conclusion, then compelling a person to *assemble* those documents for production does not reveal the person's mental processes and therefore is not sufficiently testimonial to trigger Fifth Amendment protection. However, if the government has minimal information about what documents exist or what they contain, the act of locating and selecting the documents to produce may require the subpoena recipient to use his or her own mental processes in a way that renders the resulting response testimonial in nature. That is why it matters whether the government has identified the documents with "reasonable particularity" in the subpoena. If it has, the government is not relying on a testimonial aspect of the person's act of production to make its case but instead is only seeking to compel the surrender of the documents. *See Fisher*, 425 US at 411.

The United States Supreme Court has never applied the "foregone conclusion" doctrine to any type of compelled act other than a document production. Nevertheless, a number of state courts and lower federal courts have applied it to other acts, including compelled decryption of electronic devices by entry of a password or passcode or otherwise. The resulting decisions are markedly inconsistent. Perhaps the most significant point of disagreement is as to *what* needs to be a foregone conclusion. At least one court has said that the password itself has to be a foregone conclusion for the doctrine to apply—while acknowledging that the government would not need it if it were.[6] Other courts have said that it is the suspect's knowledge of the password or passcode that must be a foregone conclusion.[7] Yet others have

[6] *See Commonwealth v. Baust*, 89 Va Cir 267, *4 (Va Cir Ct 2014) ("the password is not a foregone conclusion because it is not known outside of Defendant's mind," and "if the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it").

[7] *See, e.g.*, *United States v. Spencer*, No 17-cr-00259-CRB-1, 2018 WL 1964588 at *1-3 (ND Cal Apr 26, 2018) (upholding magistrate judge's order compelling the defendant to decrypt several electronic devices—where the government established that it was a foregone conclusion that the defendant had the ability to decrypt the devices—and rejecting proposition that the government also had to

required that the contents of the electronic device be a foregone conclusion.[8]

With that understanding of the genesis and current status of the "foregone conclusion" doctrine in mind, we must first decide whether the doctrine applies under Article I, section 12. Defendant and the state have assumed that it does, both in the trial court and on appeal, and the

---

prove that the contents of the devices were a foregone conclusion); *State v. Stahl*, 206 So 3d 124, 136 (Fla Dist Ct App 2016) (holding that it did not violate the Fifth Amendment to compel the defendant to produce the passcode to a cell phone, where the government established, "based upon cellphone carrier records and [the defendant's] identification of the phone and the corresponding phone number, that the phone was [his] and therefore the passcode would be in [his] possession"); *Commonwealth v. Jones*, 481 Mass 540, 548, 117 NE3d 702 (2019) (the commonwealth must "establish that a defendant knows the password to decrypt an electronic device before his or her knowledge of the password can be deemed a foregone conclusion"); *State v. Johnson*, 576 SW3d 205, 227 (Mo Ct App 2019) ("The focus of the foregone conclusion exception is the extent of the State's knowledge of the existence of the facts conveyed through the compelled act of production," and, when the state seeks to compel a suspect to produce the passcode to an iPhone, "[t]he 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."); *State v. Andrews*, 457 NJ Super 14, 18, 24-30, 197 A3d 200 (NJ Super Ct App Div 2018) (upholding order compelling the defendant to disclose the passcodes for his "lawfully-seized iPhones," because "the fact that defendant knows the passcodes to these devices 'adds little or nothing to the sum total of the Government's information,'" and rejecting argument that the state needed to prove that the contents of the iPhones were a foregone conclusion (quoting *Fisher*, 425 US at 411)).

[8] *See, e.g.*, *In re Grand Jury Subpoena*, 670 F3d 1335, 1348-49 (11th Cir 2012) (subpoena requiring the defendant to produce decrypted versions of computer hard drives violated Fifth Amendment, where the government "failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives, that [the defendant] has access to those files, or that he is capable of decrypting the files"); *In re Boucher*, 2009 WL 424718 at *3-4 (D Vt Feb 19, 2009) (subpoena to produce unencrypted hard drive did not violate Fifth Amendment, where the government already knew "of the existence and location of the Z drive and its files" and had sufficient evidence to authenticate it); *G. A. Q. L.*, 257 So3d at 1063 (production of the passcodes to a phone could be compelled where the state established the phone's contents with reasonable particularity); *People v. Spicer*, 2019 Ill App 3d 170814, ¶ 22, 125 NE3d 1286 (2019) (concluding that the state had to identify the documents on a cell phone with reasonable particularity to rely on the foregone conclusion doctrine); *see also United States v. Apple MacPro Computer*, 851 F3d 238, 248 (3d Cir 2017) (magistrate judge did not *plainly err* in rejecting Fifth Amendment challenge to subpoena requiring the defendant to produce decrypted computer hard drives, where the defendant did not contest that the drives were his and the government had a substantial amount of evidence about their contents). Notably, in some cases, such as *In re Grand Jury Subpoena*, courts have required both the defendant's knowledge of how to decrypt the device and the device's contents to be foregone conclusions.

trial court applied it without any separate discussion of Article I, section 12. Unfortunately, we have received no briefing on the issue as a result. Ultimately, however, we believe it is appropriate to recognize the doctrine under Article I, section 12. The doctrine as we understand it is grounded in logic, rather than legal principles unique to the Fifth Amendment. Moreover, other relevant aspects of our approach to Article I, section 12, have closely tracked the Fifth Amendment, as discussed earlier. We therefore agree with the trial court and the parties that the "foregone conclusion" doctrine applies under Article I, section 12.

As far as *how* the "foregone conclusion" doctrine applies in this context, both parties disagree with aspects of the trial court's decision. Defendant argues that the state had to establish both the contents of the iPhone and defendant's knowledge of the passcode as foregone conclusions, but she disagrees with the court's determination that the iPhone's contents were a foregone conclusion. For its part, the state argues that it only had to establish defendant's knowledge of the passcode as a foregone conclusion—which is not how the court approached it—but it defends the court's ultimate conclusion that compelling disclosure of the passcode would not violate Article I, section 12.

After careful consideration of the principles underlying the "foregone conclusion" doctrine, we agree with the state 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. Here, the testimonial aspect of entering the correct passcode into the iPhone is that it reveals defendant's "knowledge" of the passcode. *Fish*, 321 Or at 56 (acts that communicate a person's "beliefs, knowledge, or state of mind" are testimonial); *see also, e.g.*, *G. A. Q. L.*, 257 So3d at 1061 (the act of revealing a password "asserts a fact: that the defendant knows the password"). The act communicates to the court, the prosecution, and potentially a jury that defendant knows the passcode and, by extension, has access to the device and its contents. As such, the state had to establish that defendant's knowledge of the passcode was a foregone conclusion before the

trial court could compel defendant to reveal that knowledge through a testimonial act.

The state did not need to establish, however, that the contents of the iPhone were a foregone conclusion. In our view, the courts that have adopted that approach under the Fifth Amendment have transposed *Fisher*'s "existence, location, authenticity" framework for document subpoenas to a very different context without adequately grappling with the significance of the different context. When the government subpoenas documents, it is *not in possession* of the documents. In that context, although the Fifth Amendment does not protect against the production of the documents themselves, the defendant's act of selecting and assembling responsive documents may reveal the existence, location, and authenticity of the documents in a way that is testimonial. By contrast, when the government seeks to compel disclosure of the passcode to an electronic device that is already lawfully in its possession, the government already has possession of the data on the device. The act of entering the passcode reveals only that defendant has *access* to that data; it says nothing about the data itself. In that vein, it bears remembering that Article I, section 9, and the Fourth Amendment ensure that the seizure of the *data* itself is lawful, while Article I, section 12, and the Fifth Amendment protect only against compelled testimony. As the Court put it in *Fisher*, "the Fifth Amendment protects against compelled self-incrimination, not the disclosure of private information." 425 US at 401 (internal quotation marks and brackets omitted).

As recently and aptly stated by the Massachusetts Supreme Judicial Court, in applying both the Fifth Amendment and its own state constitution, "In the context of compelled decryption, the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device." *Commonwealth v. Jones*, 481 Mass 540, 547-48, 117 NE3d 702 (2019). As such, when the state relies on the foregone conclusion doctrine, what it must establish is that the suspect's knowledge of the passcode is a foregone conclusion, not that the contents of the

device are a foregone conclusion. *See, e.g.*, *id.* at 548; *State v. Stahl*, 206 So3d 124, 136 (Fla Dist Ct App 2016) ("To know whether providing the passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has established that it knows *** that the passcode exists, is within the accused's possession or control, and is authentic. The question is not the State's knowledge of the contents of the phone; the State has not requested the contents of the phone ***." (Underlining in original and internal citations omitted.)); *State v. Johnson*, 576 SW3d 205, 227 (Mo Ct App 2019) (similar); *State v. Andrews*, 457 NJ Super 14, 24, 197 A3d 200 (NJ Ct App Div 2018) (similar).[9]

That brings us to the disposition of this case. In her opening brief, defendant argues that "the content of the sought evidence was unknown to police," that "[t]he state did not state with any reasonable particularity the contents of the phone," and that the trial court therefore erred in ruling that the iPhone's contents were a foregone conclusion. Because we conclude that the state did not need to prove that the iPhone's *contents* were a foregone conclusion, defendant cannot obtain reversal on that basis.

At oral argument, defendant challenged a different aspect of the trial court's ruling, specifically its determination that defendant knew the passcode to the iPhone, which the court phrased in terms of "probable cause." That is not an argument that defendant makes in her opening brief. The opening brief touches only briefly on defendant's knowledge of the passcode—admitting that the iPhone's presence in her purse "permit[s] an inference that [she] owned the phone" but asserting that typing in the passcode "would be new and stronger evidence that [she] owned the phone"—and does not identify any purported error by the trial court on that issue. To the extent that defendant intended to challenge that aspect of the trial court's ruling, particularly the

[9] *See also* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Texas L Rev 767, 768-70 (2019) (reviewing nationwide case law applying the foregone conclusion doctrine in the context of court orders to decrypt electronic devices, and ultimately arguing that the doctrine should be understood such that "the Fifth Amendment poses no barrier to compelled decryption as long as the government has independent knowledge that the suspect knows the password and the government presents the password prompt to decrypt the device to the suspect").

court's use of "probable cause" language, defendant did not develop the argument sufficiently for us to consider it. *See State v. Dawson*, 277 Or App 187, 190, 369 P3d 1244 (2016) (declining to consider inadequately developed argument); *Beall Transport Equipment Co. v. Southern Pacific*, 186 Or App 696, 700 n 2, 64 P3d 1193 (2003) (it is not our proper function "to make or develop a party's argument when that party has not endeavored to do so itself"). And we will not consider arguments made for the first time at oral argument. *Colton and Colton*, 297 Or App 532, 547-48, 443 P3d 1160 (2019).[10]

We reject the first assignment of error as it pertains to Article I, section 12.

FEDERAL CONSTITUTIONAL ANALYSIS

Having rejected defendant's argument under Article I, section 12, we must next consider her argument under the Fifth Amendment to see whether the result is any different under federal law. *See* US Const, Amend V ("No person *** shall be compelled in any criminal case to be a witness against himself[.]"); *Schmerber v. California*, 384 US 757, 760, 86 S Ct 1826, 16 L Ed 2d 908 (1966) (the Fourteenth Amendment "secures against state invasion" that same privilege). Neither the Oregon Supreme Court nor the United States Supreme Court has addressed whether a court ordering a suspect to enter the passcode into an electronic device violates the Fifth Amendment, so there is no binding authority on point. *See J. M. v. Oregon Youth Authority*, 288 Or App 642, 646, 406 P3d 1127 (2017) ("The only federal court that controls over the Oregon Supreme Court on matters of federal law is the United States Supreme Court.").

In the trial court and on appeal, defendant has made the same arguments under the Oregon and federal constitutions; that is, she argues for the same analysis and

[10] We do not mean to suggest that a properly raised challenge to the trial court's passcode-knowledge determination necessarily would have been successful. To the contrary, we express no opinion on an issue that raises complicated questions—such as whether a foregone-conclusion determination is a legal ruling or a factual finding and, if it is a factual finding, what standard of proof applies—that have not been briefed.

the same result under both.[11] The state also argues that the analysis is the same. We have found no reason to interpret the Fifth Amendment differently than Article I, section 12, for present purposes. Accordingly, we independently apply the same analysis under the Fifth Amendment as we did under Article I, section 12, and reach the same result.

Affirmed.

[11] Again, we do not consider arguments made for the first time at oral argument. *Colton*, 297 Or App at 547-48.