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 Case No. 16CN03799 Court of Appeals Case No. A162950 Supreme Court Case No. S067312

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION OF OREGON, AMERICAN CIVIL LIBERTIES UNION, AND ELECTRONIC FRONTIER FOUNDATION

Review of the Decision of the Court of Appeals,
on Appeal from a Judgment of the Circuit Court for Marion County,
Hon. Tracy A. Prall, Judge

Opinion Filed: October 16, 2019
Author of Opinion: Aoyagi, J.
Before: Hadlock, P.J.; DeHoog, J.; and Aoyagi, J.

(*Counsel listed on next page*)

June 2020

Kelly Simon, OSB No. 154213
ACLU FOUNDATION OF OREGON
P.O. Box 40585
Portland, Oregon 97240
Telephone: 503-444-7015
KSimon@aclu-or.org

Attorney for Amicus Curiae
ACLU of Oregon

Kendra M. Matthews, OSB No. 965672
BOISE MATTHEWS EWING LLP
1050 SW Sixth Ave., Suite 1400
Portland, Oregon 97204
Telephone: 503-228-0487
Kendra@boisematthews.com

Attorney for Amici Curiae
ACLU of Oregon,
American Civil Liberties Union, and
Electronic Frontier Foundation

Ernest Lannet, OSB No. 013248
Chief Defender
Criminal Appellate Section
Sarah Laidlaw, OSB No. 111188
Deputy Defender
OFFICE OF PUBLIC DEFENSE SERVICES
1175 Court Street NE
Salem, Oregon 97301
Telephone: 503-378-3479
Ernest.G.Lannet@opds.or.us
Sarah.Laidlaw@opds.or.us

Attorneys for Petitioner-on-Review
Cattrice Pittman

Ellen F. Rosenblum, OSB No. 753239
Attorney General
Benjamin Gutman, OSB No. 160599
Solicitor General
Jonathan N. Schildt, OSB No. 151674
Assistant Attorney General
OREGON DEPARTMENT OF JUSTICE
1162 Court Street NE
Salem, Oregon 97301
Telephone: 503-378-4402
Jonathan.N.Schildt@doj.state.or.us

Attorneys for Respondent-on-Review
State of Oregon

Franz H. Bruggemeier, OSB No. 163433
OREGON JUSTICE RESOURCE CENTER
P.O. Box 40588
Portland, Oregon 97240
Telephone: 503-768-7321
FBruggemeier@ojrc.info

Attorney for Amici Curiae
Laurent Sacharof and
Oregon Justice Resource Center

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST

American Civil Liberties Union of Oregon ("ACLU of Oregon") is a statewide nonprofit and nonpartisan organization with over 33,000 members. As a state affiliate of the national ACLU organization, ACLU of Oregon is dedicated to defending and advancing civil rights and civil liberties for Oregonians, including the fundamental civil rights protected in the Oregon Constitution and United States Constitution. It frequently appears before this Court as *amicus curiae* in cases implicating important state and federal constitutional principles. *See, e.g.*, *State v. Link*, Supreme Court Case No. S066824 (Or. oral argument held March 12, 2020) (constitutional protections against excessive and disproportionate punishments); *State v. A.J.C.*, 355 Or. 552, 326 P.3d 1195 (2014) (constitutional protections against warrantless search and seizure); *Brumwell v. Premo*, 355 Or. 543, 326 P.3d 1177 (2014) (constitutional right to counsel).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Since its founding in 1920, the ACLU has appeared before the Supreme Court and other federal courts in numerous cases implicating Americans' right to privacy, including as counsel in

Carpenter v. United States, __ U.S. __, 138 S. Ct. 2206 (2018), and as counsel and *amicus* in various cases addressing the Fifth Amendment right against self-incrimination and the compelled decryption of digital devices, *see Commonwealth v. Davis*, 220 A.3d 534, 550 (Pa. 2019) (counsel); *Seo v. State*, No. 18S-CR-595 (Ind. oral argument held Apr. 18, 2019) (*amicus*); *State v. Andrews*, No. A-72-18 (N.J. oral argument held Jan. 22, 2020) (*amicus*).

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF is particularly interested in ensuring that individuals, and their constitutional rights, are not placed at the mercy of advancements in technology. EFF has appeared as amicus in various cases addressing the Fifth Amendment right against self-incrimination and the compelled decryption of digital devices, *Seo v. State*, No. 18S-CR-595 (Ind. oral argument held Apr. 18, 2019); *State v. Andrews*, No. A-72-18 (N.J. oral argument held Jan. 22, 2020); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012).

SUMMARY OF ARGUMENT

This case presents questions of first impression in this Court: whether either of the privileges against self-incrimination found in Article I, section 12, of the Oregon State Constitution and the Fifth Amendment to the United States Constitution preclude the state from forcing a defendant to recall from memory a passcode to enter it into her encrypted iPhone, thereby delivering the phone's contents to the state for use against her in a criminal proceeding. The Court of Appeals' ruling authorizing such compulsion under both provisions bucked centuries of legal tradition and case law holding that the state cannot compel a suspect to recall and share information that exists only in her mind to aid the state in its prosecution. *See Curcio v. United States*, 354 U.S. 118, 128 (1957) (Fifth Amendment); *State v. Soriano,* 68 Or. App. 642, 646 n 4, 684 P2d 1220 (Gillette, J.), *aff'd* 298 Or. 392, 693 P.2d 26 (1984) (Article I, section 12). The application of the privilege in this context is no technicality; it is a fundamental protection of human dignity, agency, and integrity enshrined in both the Oregon and United States constitutions.

In ruling that Ms. Pittman could be constitutionally compelled to assist in her own prosecution, the Court of Appeals relied on the so-called "foregone-conclusion" rationale to avoid the straightforward application of these fundamental protections against self-incrimination. *State v. Pittman*, 300 Or.

App. 147, 156-57, 452 P.3d 1011 (2019) (citing *United States v. Hubbell*, 530 U.S. 27, 44 (2000); *Fisher v. United States*, 425 U.S. 391, 411 (1976)); *see also Doe v. United States* (*Doe II*), 487 U.S. 201, 208 n. 6 (1988). The Court of Appeals' decision converted a narrow rule permitting the compelled production of known business records via subpoena into a super-charged power for law enforcement to enlist criminal defendants as witnesses against themselves. This Court should reverse.

First, the foregone-conclusion rationale has no basis in the Oregon Constitution. To the contrary, this Court has repeatedly recognized that Article I, section 12 protects a criminal defendant from any form of state-compelled self-incrimination, including being compelled to testify, furnish evidence, or provide the state a critical link in its effort to secure evidence. *State v. Vondehn*, 348 Or. 462, 468, 236 P.3d 691 (2010); *State v. Cram*, 176 Or. 577, 160 P.2d 283 (1945); *Soriano*, 68 Or. App. at 646 n. 4.

Second, even under the Fifth Amendment, the rationale is simply inapplicable in these circumstances. The United States Supreme Court has applied this rationale in a single case, in a specific and narrow context: the act of producing subpoenaed business documents prepared by and in the possession of third parties and the content of which was already entirely known by the

government. *See Fisher*, 425 U.S. at 391. The United States Supreme Court's conclusion that the Fifth Amendment does not provide protection in that narrow circumstance does not logically mean that criminal defendants can be compelled to incriminate themselves by reciting, writing, typing, or otherwise reproducing the contents of their minds.

Whether this Court considers the issue under the state or federal constitution, the state cannot require a defendant to remember, enter, use, or disclose the contents of her mind, such as a memorized passcode, any more than it can compel incriminating oral testimony from defendants, even when it already independently knows what they will say.

This should be the end of the analysis. Because, however, the Court of Appeals concluded that the foregone-conclusion rationale applied, that court also offered an analysis of *how* it should be applied. But that analysis was also wrong. If the rationale is to apply at all, the prosecution must demonstrate that it already knows *the evidence it will obtain*. *See United States v. Doe* (*Doe I*), 465 U.S. 605, 614 n.13 (1984); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012). In other words, in this context, the state would have to describe with reasonable particularity the

specific digital records it seeks to compel the defendant to produce. *In re Grand Jury Subpoena*, 670 F.3d at 1347 (citing *Hubbell*, 530 U.S. at 45).[1]

Under both the Fifth Amendment and Article I, section 12 of the Oregon Constitution, this Court should reverse.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Amici accept the statement of facts and the recitation of procedural history contained in the Court of Appeals' opinion, *Pittman*, 300 Or. App. at 149-52, as supplemented by Ms. Pittman's Brief on the Merits, Def. Br. at 5-8.

[1] *Amici* understand that the Court will generally "consider state constitutional claims before examining issues of federal law." *Soriano,* 68 Or. App. at 645. While the Court of Appeals followed that order of analysis in its opinion, *Pittman*, 300 Or. App. at 152, its state constitutional analysis hinged on its application and interpretation of the Fifth Amendment and United States Supreme Court opinions interpreting that provision, *id.* at 155. Accordingly, *amici* will first discuss the proper application and understanding of the Fifth Amendment, detailing how the Court of Appeals erred in its analysis under that provision and in its application of the foregone-conclusion rationale to this context. *Amici* will follow that Fifth Amendment analysis with a discussion of how Article I, section 12, provides this court with a distinct basis for reversal.

ARGUMENT

I. COMPELLED RECOLLECTION, DISCLOSURE, OR USE OF A PASSCODE BY THE TARGET OF A CRIMINAL INVESTIGATION IS TESTIMONY PRIVILEGED BY THE FIFTH AMENDMENT RIGHT AGAINST SELF-INCRIMINATION.

A. The Fifth Amendment Prohibits the Compelled Disclosure or Use of the Contents of a Suspect's Mind.

The Court of Appeals correctly recognized that by demanding decryption of Ms. Pittman's digital device, the state is seeking compelled, self-incriminating testimony—privileged under the Fifth Amendment.[2]

The Fifth Amendment guarantees that "[n]o person shall be * * * compelled in any criminal case to be a witness against himself." U.S. Const., Amend. V. To invoke the privilege, an individual must show three things: that the evidence sought is (1) compelled, (2) testimonial, and (3) self-incriminating. *Hubbell*, 530 U.S. at 34. Testimonial evidence includes the communication of any information, direct or indirect, verbal or non-verbal, that requires a person to use "the contents of his own mind" to truthfully relay facts. *Id.* at 43 (citing *Curcio*, 354 U.S. at 128); *see Pennsylvania v. Muniz*, 496 U.S. 582, 595 (1990)

[2] While the Court of Appeals analyzed the requirements for protection against self-incrimination under the Oregon Constitution, those requirements are the same as under the federal constitution. *See Pittman*, 300 Or. App. at 152-53; *see also* Def. Br. at 14-21.

(The Fifth Amendment privilege "spare[s] the accused from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government."). The testimonial nature of a communication does not turn on whether it is spoken, but whether it requires, by "word or deed," *Doe II*, 487 U.S. at 219 (Stevens, J., dissenting), a truthful expression of "the contents of an individual's mind," *Curcio*, 354 U.S. at 128; *see also Doe II*, 487 U.S. at 219 n.1 (Stevens, J., dissenting) (explaining that the Fifth Amendment protects against compelled "intrusion[s] upon the contents of the mind of the accused" because they "invade the dignity of the human mind").

B. The Fifth Amendment Prohibits Compelled Recollection and Use of a Memorized Passcode.

The trial court order violates the Fifth Amendment because it seeks to compel Ms. Pittman to provide testimony.[3] Compliance would require

[3] The trial court's order commanded Ms. Pittman to enter the passcode directly into her phone, apparently while under the observation of a law enforcement official. *See Pittman*, 300 Or. App. at 151-52 ("[T]he court orally ordered defendant to enter the passcode into 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.").

Ms. Pittman to use the contents of her mind (her recollection of the passcode), and to reveal that information by deed (typing in the passcode). Compelled entry of a password constitutes a modern but straightforward form of written testimony, which is categorically protected from compulsion under the privilege against self-incrimination.

The facts of this case show exactly how the trial court improperly sought to compel privileged testimony. When Ms. Pittman was ordered to enter her password, she was put to the classic "trilemma of truth, falsity, or silence," *Muniz*, 496 U.S. at 597. If she told the truth, she could incriminate herself. When Ms. Pittman apparently entered an incorrect password, whether she knew it was false or not, she was held in contempt. She would also have been held in contempt had she refused to enter anything. Had she proceeded to trial, her response to the order—regardless of what it was—could have been used against her. The Fifth Amendment does not allow defendants to be forced into this situation. *See id*. ("[T]he definition of 'testimonial evidence * * * must encompass all responses to questions that, if asked of a sworn suspect during a criminal trial, could place the suspect in the 'cruel trilemma.'"). The trial court's order was in error.

Reciting, writing, typing, entering, or otherwise reproducing a password from memory is testimony protected by the Fifth Amendment. Requiring a defendant to reveal incriminating information stored in her mind, however that communication is accomplished, is constitutionally off-limits. Testimony need not be verbal. Non-verbal acts such as nodding in response to a question are testimonial because they communicate the contents of the mind without speaking.[4] *See Schmerber v. California*, 384 U.S. 757, 761 n.5 (1966) ("A nod or headshake is as much a 'testimonial' or 'communicative' act in this sense as are spoken words."). The Eleventh Circuit applied this principle in a case remarkably similar to this one, holding that "the decryption * * * of the hard drives would require the use of the contents of [the accused's] mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *In re Grand Jury Subpoena*, 670 F.3d at 1346. Many other courts agree: production of computer passwords requires the suspect "to divulge through his mental processes his password." *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); *see also, e.g.*, *Commonwealth v. Davis*, 220 A.3d 534, 549 (Pa. 2019) (explaining that the Supreme Court's

[4] This is in contrast to mere physical acts that do not reveal the contents of an individual's mind, such as putting on a shirt. *Holt v. United States*, 218 U.S. 245 (1910).

cases in this area "uniformly protect information arrived at as a result of using one's mind"); *Commonwealth v. Baust*, No. CR14-1439, 2014 WL 10355635 at *4 (Va. Cir. Ct. Oct. 28, 2014); *SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644 at *3 (E.D. Pa. Sept. 23, 2015); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1061-62 (Fla. Dist. Ct. App. 2018); *In re Boucher*, No. 2:06-mj-91, 2007 WL 4246473 at *1 (D. Vt. Nov. 29, 2007).

In *Davis*, the trial court had ordered the defendant to reveal the password to decrypt data stored on a computer. In vacating the order, the Pennsylvania Supreme Court held that "revealing of a computer password is a verbal communication, not merely a physical act that would be nontestimonial in nature." 220 A.3d at 548. The court reviewed federal precedent and correctly explained that the United States Supreme Court's cases in this area "uniformly protect information arrived at as a result of using one's mind." *Id*. at 549. Based on that Fifth Amendment case law, the court held that "the compelled recollection of [a] password is testimonial in nature, and, consequently, privileged under the Fifth Amendment to the United States Constitution." *Id*. at 551.

Compelled testimony need not take great mental effort, and the government need not be interested in the import of the testimony for its own

sake. For example, in *Muniz*, the United States Supreme Court held that a motorist suspected of intoxication could not be compelled to answer a question about the date of his own sixth birthday. 496 U.S. at 598-99. Law enforcement was not interested in the date itself (in fact, they knew the date); rather, they sought his response as evidence of mental impairment. *See id.* at 599 & n.13. But the question still demanded a testimonial answer.[5] And so long as the testimony provides a "link in the chain of evidence" needed to prosecute, it is incriminating. *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *Hubbell*, 530 U.S. at 38; *Doe II*, 487 U.S. at 208 n.6.

Moreover, opening a lock with a memorized passcode is testimonial regardless of whether the state learns the combination. In *United States v. Green*, 272 F.3d 748, 753 (5th Cir. 2001), the Fifth Circuit held that there is "no serious question" that asking an arrestee to disclose the locations of and open the combination locks to cases containing firearms demands "testimonial and

[5] As explained above, the trial court's order contemplated that the state *would* learn the password entered by Ms. Pittman, because the officer was permitted to watch her enter two passcodes before Ms. Pittman was held in contempt of court. *See Pittman*, 300 Or. App. at 151-52.

communicative" acts as to his "knowledge of the presence of firearms in these cases and of the means of opening these cases."

Because compelled disclosure or entry of Ms. Pittman's passcode is both testimonial and self-incriminating, it is privileged by the Fifth Amendment and constitutionally off-limits. The analysis should end here, as it does in almost every Fifth Amendment case.

II. THE NARROW AND LIMITED FEDERAL FOREGONE-CONCLUSION RATIONALE HAS NO APPLICATION IN THIS CASE.

Even if the police know with reasonable certainty that someone committed a bank robbery, no one could credibly suggest that the suspect could then be compelled to testify orally or in writing concerning an incriminating fact because it was a foregone conclusion. That is because the Fifth Amendment does not allow the government to compel suspects to speak, write, type, or otherwise reproduce the contents of their minds to aid in their own prosecution. Notably, in neither *Muniz* nor *Green* did the courts conduct a foregone-conclusion inquiry. This was proper and frankly unsurprising, since the Fifth Amendment prohibits compelled verbal testimony, regardless of whether investigators already know the answer.

Some courts, however, including the Court of Appeals below, have erroneously concluded that the narrow foregone-conclusion inquiry permits the

state to bypass this bedrock constitutional limitation and compel witnesses to disclose or enter their memorized passcodes into digital devices. This Court should reject that conclusion.[6]

First, the foregone-conclusion analysis is exceedingly narrow, and does not reach the compelled recollection and use of a passcode to unlock a device and deliver incriminating evidence to law enforcement. Rather, it is a factor relevant to the question of whether an act of production is sufficiently testimonial to receive Fifth Amendment protection. *Fisher*, 425 U.S. at 411. The inquiry has no place outside of the context of an act of production of documents in response to a subpoena.

After *Fisher*, the Supreme Court never again allowed the government to compel a testimonial "act of production" on those grounds. *See Hubbell*, 530 U.S. at 44; *Doe I*, 465 U.S. at 612-14. In more than forty years since *Fisher*, a

[6] On this point, ACLU of Oregon, ACLU, and EFF disagree with *amici* Professor Laurent Sacharoff and Oregon Justice Resource Center. OJRC *Amicus* at 15. Saying a password and entering it are both "full-fledged testimony" because compliance means suspects must use their memories and thoughts to truthfully provide information to law enforcement and participate in their own prosecution—the "cruel trilemma." OJRC *Amicus* at 4, 9. Entering a password is not an act of production, and thus the foregone conclusion inquiry does not apply. Even if the entry of a password into a phone or computer were treated as a testimonial act of production, the foregone-conclusion analysis still does not apply to personal passwords. In either case, this Court should reverse the Court of Appeals.

handful of lower courts have considered the scope of act of production privilege and with few exceptions, have applied the foregone-conclusion rationale only in the context of court orders for the production of specified documents, the existence of which the government already knew. The Court of Appeals nonetheless joined the few courts that have found an order to recall or use a memorized password could be a foregone conclusion and therefore not privileged. *See Pittman*, 300 Or. App. at 158. In doing so, the court erroneously stretched this rationale far beyond its limits.

Second, even if the foregone-conclusion rationale could apply in cases involving passcodes, the state would have to show far more than required by the Court of Appeals. Rather than simply demonstrating that an individual had *possession and control* over a device, the state would have to show with reasonable particularity that it has independent knowledge of *any and all information disclosed* by the compelled act of production—including that the specific, identifiable files it seeks are stored on that device. Because the Court of Appeals applied a much narrower standard, even if this Court decides to expand a foregone-conclusion analysis to the compulsory entry of a memorized

password to obtain private communications, it should reverse based upon the Court of Appeals articulation of what must be shown to apply the standard.

A. The Foregone-Conclusion Analysis Applies Only to the Production of Specified, Preexisting Business Records.

The facts in *Fisher* demonstrate just how limited the foregone-conclusion rationale is to the baseline Fifth Amendment rule against self-incrimination. *Fisher*—unlike this case—did not involve compelled written or oral testimony. And law enforcement in *Fisher*—also unlike here—sought only to compel compliance with a third-party subpoena for business records.

The foregone-conclusion inquiry helps define when an act of production is testimonial. It is not a rule that overcomes the Fifth Amendment privilege for speech, writing, or testimonial acts. In *Fisher*, the United States Supreme Court for the first time acknowledged that "the 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 U.S. at 410-13. In *Fisher*, the government sought to compel the production of documents created by accountants preparing the defendants' tax records and in possession of the defendants' attorneys. 425 U.S. at 412-13. The United States Supreme Court recognized that producing records in response to a subpoena or court order can have testimonial aspects protected by the Fifth Amendment—including implicit

admissions concerning the existence, possession, and authenticity of the documents produced. *See id.* at 410. After identifying this potential testimonial nature, the *Fisher* court then had to address the "more difficult issues of whether the tacit averments * * * are both 'testimonial' and 'incriminating' for purposes of applying the Fifth Amendment." *Id.* at 410. Under the unique circumstances of the case, the Court held that the act of producing the subpoenaed documents was not testimonial since the government had independent knowledge of the existence and authenticity of documents created by accountants preparing the defendants' tax records and in possession of the defendants' attorneys. *Id.* at 412-13.

In sum, *Fisher* recognized that "[t]he act of producing evidence, specifically documents, in response to a subpoena * * * has communicative aspects," *id.* at 410, and then set out a methodology for determining whether those implicit communications rose to the level of testimony privileged under the Fifth Amendment. That methodology calls on a court to determine whether the implicit information is a foregone conclusion. The foregone conclusion analysis is a part of that methodology, and not an independent inquiry applicable in other contexts. Thus, *Fisher* stands for the proposition that if (1) a subpoena demands production of a narrow category of business and financial

documents, (2) production does not rely on or disclose the contents of one's mind, and (3) the state already has evidence of the facts communicated by the production, it may be able to compel the target's disclosure of those papers.

Unsurprisingly, given the highly specific factual circumstances in *Fisher*, in the nearly forty-three years since the case was decided, the Supreme Court has never again held that an act of production is unprotected by the Fifth Amendment because the testimony it implies is a foregone conclusion. Indeed, the Court has only even considered foregone-conclusion arguments in two other cases, and it rejected them both times. Those cases also involved the government seeking to compel the production of preexisting business or other financial records. *See Hubbell*, 530 U.S. at 44-45 (holding that the case "plainly [fell] outside of" the foregone-conclusion rationale where the government sought "general business and tax records that [fell] within the broad categories described in this subpoena" rather than specific, known files); *Doe I*, 465 U.S. at 612-14 (rejecting application of the foregone-conclusion rationale where the subpoena sought several broad categories of general business records).

Comparing *Hubbell* to *Fisher* shows how limited a foregone conclusion analysis is, demonstrating that it does not apply when the state seeks to compel witnesses to speak or act in ways that rely on their memories and cognition. In

Hubbell, the government subpoenaed broad categories of documents from the respondent. 530 U.S. at 40. The act of production established the existence, authenticity, and custody of produced documents, information the government was already able to prove, or did not need. *Id.* In other words, these matters were foregone conclusions. Nevertheless, the Court held that the Fifth Amendment privilege applied. Compliance with the subpoena required "mental and physical steps" and the obligation that the respondent "truthful[ly] reply to the subpoena. *Id*. at 42, 44. When the court stated that, "whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it," it was not because the facts implied by the act of production were as yet unknown to the prosecution. Rather, in *Hubbell*, as here (and with all forced decryption cases), the foregone-conclusion rationale does not apply because compliance requires mental effort beyond any acts of production.

That the United States Supreme Court has never applied the foregone-conclusion rationale outside of cases involving specific, preexisting business and financial records is unsurprising. These types of records constitute a unique category of material that, to varying degrees, has been subject to compelled production and inspection by the government for over a century. *See, e.g.*,

Braswell v. United States, 487 U.S. 99, 104 (1988); *Shapiro v. United States*, 335 U.S. 1, 33 (1948).

Lower courts, too, have overwhelmingly applied the rationale only in cases concerning the compelled production of specific, preexisting business and financial records. *See, e.g., United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (business and tax records); *United States v. Bright*, 596 F.3d 683, 689-90 (9th Cir. 2010) (credit-card records); *United States v. Gippetti*, 153 F. App'x 865, 868-69 (3d Cir. 2005) (bank and credit-card account records); *United States v. Bell*, 217 F.R.D. 335, 341-42 (M.D. Pa. 2003) ("tax avoidance" materials advertised on defendant business's website); *In re Grand Jury Subpoenas Served Feb. 27, 1984*, 599 F. Supp. 1006, 1012 (E.D. Wash. 1984) (business-partnership records); *cf. Burt Hill, Inc. v. Hassan*, No. CIV.A.09-1285, 2010 WL 55715 at *2 (W.D. Pa. Jan. 4, 2010) (contents of electronic storage devices used by defendants while employed by plaintiff).[7]

[7] This Court has applied *Fisher* a single time, holding that the Fifth Amendment did not bar the compelled production of a letter drafted by an accused, sent to a third party, and handed over to the accused's attorney. *State v. Jancsek*, 302 Or. 270, 285-89, 730 P.2d 14 (1986) (en banc). Notably, *Janscek* was decided before the United States Supreme Court's decision in *Hubbell*, which clarified the limited scope of the foregone-conclusion analysis. Nevertheless, in *Janscek* this Court held that the facts of that case were closer to *Fisher* than to *Doe* because "the document was in the hands of his lawyer (as in *Fisher*)" *Id*. at 288.

On the other hand, courts faced with the question have not conducted a foregone-conclusion inquiry in cases involving the compelled production of physical evidence, such as guns or drugs, because responding to such requests would constitute an implicit admission of guilty knowledge. *See, e.g.*, *Muniz*, 496 U.S. 582 (no foregone-conclusion analysis); *Green*, 272 F.3d 748 (no foregone-conclusion analysis); *Commonwealth v. Hughes*, 404 N.E.2d 1239, 1244 (Mass. 1980) ("[W]e express doubt whether a defendant may be compelled to deliver the *corpus delicti*, which may then be introduced by the government at trial, if only it is understood that the facts as to the source of the thing are withheld from the jury."); *State v. Dennis*, 558 P.2d 297, 301 (Wash. 1976) (defendant's act of producing cocaine in response to officer's urgings was testimonial, no foregone-conclusion analysis); *Goldsmith v. Superior Court*, 152 Cal. App. 3d 76, 87 (1984) (defendant's production of a gun was testimonial, and not a foregone conclusion); *see also Kirschner*, 823 F. Supp. 2d at 669 (E.D. Mich. 2010) (order to produce computer passwords requires the suspect "to divulge through his mental processes his password", no foregone-conclusion analysis).

Here, the state sought an order compelling Ms. Pittman to recall, use, and display her memorized passcode to aid law enforcement in a search of her

device. In other words, the state sought Ms. Pittman's testimony to assist it in searching the phone. That request falls outside the scope of *Fisher* and is not a mere act of production.

The Pennsylvania Supreme Court recently rejected the application of the foregone-conclusion rationale under the same circumstances. *Commonwealth v. Davis*, 220 A.3d at 550. That court acknowledged "significant and ever-increasing difficulties faced by law enforcement in light of rapidly changing technology, including encryption, to obtain evidence." *Id.* at 551. But "unlike the documentary requests under the foregone conclusion rationale, * * * information in one's mind to 'unlock the safe' to potentially incriminating information does not easily fall within this exception," and "the compulsion of a password to a computer cannot fit within this exception." *Id.*

The circumstances in which the foregone-conclusion rationale is applicable are extraordinarily limited. The Court of Appeals erred in applying it to the circumstances presented in this case.

B. Even If the Foregone-Conclusion Rationale Could Apply in this Context, the State Must Describe with Reasonable Particularity the Incriminating Files It Seeks.

For the reasons articulated above, the foregone-conclusion rationale should not be applied in this context under either Article I, section 12, or the

Fifth Amendment. Moreover, for the reasons articulated in Section III, *infra*, Article I, section 12, squarely precludes adoption of a foregone-conclusion rationale under that provision. Because, however, the Court of Appeals applied the foregone-conclusion analysis under both provisions, *amici* briefly discuss *how* that doctrine, if applicable, should be applied.

If this Court were to conclude that the foregone-conclusion rationale could be applied to an order compelling a defendant to disclose her password to decrypt a digital device, it should conclude that the state first must demonstrate knowledge of the existence, location, ownership, and authenticity of the device and also identify with reasonable particularity what files it will find stored there. *See In re Grand Jury Subpoena*, 670 F.3d at 1346. That is a far higher bar for the state to clear than merely showing that Ms. Pittman knew her password and had access to her device.

The foregone-conclusion rationale only applies where the state can show with "reasonable particularity" that it "already [knows] of the materials [it will uncover], thereby making any testimonial aspect a 'foregone conclusion.'" *See id.* at 1345 (citing *Hubbell*, 530 U.S. at 36 n.19, 38). By contrast, where an act of production reveals information the state does not already know, compelling that act would violate the Fifth Amendment. *See Hubbell*, 530 U.S. at 45 (no

foregone conclusion where government did not have "any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent").

The two federal Courts of Appeal that have applied the foregone-conclusion inquiry to password-protected digital devices have held that investigators must know and be able to describe with reasonable particularity the discrete, tangible contents of a device—not merely that the device belongs to the defendant. For example, in *In re Grand Jury Subpoena*, the Eleventh Circuit held that an order requiring the defendant to produce a decrypted hard drive would be "tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, *and* access to the encrypted portions of the drives; and of his capability to decrypt the files." 670 F.3d at 1346 (emphasis added). The government could not compel the defendant to produce the information under the foregone-conclusion rationale unless it could show with "reasonable particularity" the "specific file names" of the records sought, or, at minimum, that the government seeks "a certain file," and can establish that "(1) the file exists in some specified location, (2) the file is possessed by the target of the

subpoena, and (3) the file is authentic." *Id.* at 1347 n.28.[8] But in that case, the government did not know "the existence or the whereabouts" of the records it sought. *Id*.; *see also United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (finding the foregone-conclusion inquiry satisfied where the government had evidence *both* that contraband files existed on the devices and that the defendant could access them).

A number of other courts have similarly held that law enforcement must know with reasonable particularity what information is on an encrypted device—not merely that the suspect knows the passcode. As one division of the Florida Court of Appeals explained, "when it comes to data locked behind a passcode wall, the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall." *G.A.Q.L.*, 257 So. 3d at 1063. It is thus "not enough to know that a passcode wall exists, but rather, the state must demonstrate with reasonable particularity

[8] The Eleventh Circuit rejected the government's assertion that the use of encryption on the device in that case alone demonstrated that the suspect "was trying to hide something." *In re Grand Jury Subpoena*, 670 F.3d at 1347. Rather, it explained, "[j]ust as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all." *Id*. Indeed, encryption is designed to protect the owner from thieves, fraud, hackers, and abusive spouses. Far from creating a zone of lawlessness, encryption *prevents* crime.

that what it is looking for is in fact located behind that wall." *Id.* at 1063-64; *see Huang*, 2015 WL 5611644, at *3 (State must know what "if anything, [is] hidden behind the encrypted wall" (quoting *In re Grand Jury Subpoena*, 670 F.3d at 1349)); *see also Doe I*, 465 U.S. at 613 n.12.

Like some other courts have done, the Court of Appeals erred in concluding that the state need not meet this burden, and instead can overcome the Fifth Amendment privilege merely by showing that it has knowledge that a suspect has access to an encrypted digital device. *See Pittman*, 300 Or. App. at 161-62; *see also State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016); *United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588 at *3 (N.D. Cal. Apr. 26, 2018); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 622 (Mass. 2014) (Lenk, J., dissenting) (majority compelled defendant to enter encryption key even though "the government has not shown that it has any knowledge as to the existence or content of any particular files or documents on any particular computer"). The Court of Appeals concluded that this lower standard applies because "the testimonial aspect of entering the correct passcode into the iPhone is that it reveals [the] defendant's 'knowledge' of the

passcode." *Pittman*, 300 Or. App. at 160 (citing *State v. Fish*, 321 Or. 48, 56, 893 P.2d 1023 (1995)). But that is not the whole story.

Entering a passcode conveys not just a defendant's possession and control of a device and knowledge of the passcode, but also a wide range of information about the device's contents. In the vast majority of cases, the inescapable inference is that someone who knows the password to a device is its owner and is responsible for its *contents*—the sender or recipient of the messages it stores, the photographer of the pictures it contains, the subject of medical data, and so on. Providing a passcode is equivalent to testifying about to provenance of each photo, email, and document on the phone.

It is a fundamental tenet that the privilege against self-incrimination protects against using compulsion to derive circumstantial evidence just as much as it does direct evidence. *See, e.g.*, *Hoffman*, 341 U.S. at 486. In *Muniz*, for example, police asked the motorist the date of his sixth birthday not because they wanted to know the answer, but to generate, through his compelled mental recollection and calculations, circumstantial evidence of his intoxication. Yet the Supreme Court held the answer to be privileged. 496 U.S. 582; *Hubbell*, 530 U.S. at 38 ("[C]ompelled testimony that communicates information that may

lead to incriminating evidence is privileged even if the information itself is not inculpatory." (quotation marks omitted) (quoting *Doe II*, 487 U.S. at 208 n.6)).

Furthermore, entering the password to a device is the direct "link in the chain" that facilitates evidence about the device's contents. *Hubbell*, 530 U.S. at 42. *Hubbell* teaches that the government cannot compel the act of entering the password and proceed as if the contents of the device fell "like 'manna from heaven.'" *Id.* Hence, to get around the defendant's valid assertion of privilege, it must in the first instance provide full "use and derivative-use immunity," *id.* at 46, which would place the contents of the device off limits in this case. Even if the foregone conclusion could provide an alternative method to compel this testimony, the burden would be on the government to demonstrate it could learn of all derivative evidence through an independent, untainted source. *See, e.g.*, *Kastigar v. United States*, 406 U.S. 441, 443 (1972).

Focusing only on the passcode misses the point. In these encryption cases, law enforcement is seeking both the passcode *and* the underlying data. The Fifth Amendment prevents the state from acting as if the underlying data appears like "manna from heaven," divorced from the compelled disclosure of the password that protects this data. *In re Grand Jury Subpoena*, 670 F.3d at 1352 (quoting *Hubbell*, 530 U.S. at 33, 42). A foregone-conclusion rationale

that allows the state to force individuals to decrypt based on evidence mere possession and control of an electronic device would permit the state to compel a bonanza of incriminating personal disclosures. In the digital era, more and more evidence resides on personal digital devices, which contain "a digital record of nearly every aspect of [users'] lives." *Riley v. California*, 573 U.S. 373, 375 (2014). An "exception" to self-incrimination protections that allows law enforcement to force a suspect to reveal the contents of their device simply because they know the device belongs to the suspect would "swallow the protections of the Fifth Amendment." *G.A.Q.L.*, 257 So. 3d at 1063. Every password-protected device "would be subject to compelled unlocking since it would be a foregone conclusion that any password-protected [device] would have a passcode." *Id*.

In sum, contrary to the Court of Appeals' opinion, even if this Court were to conclude that a foregone-conclusion inquiry is appropriate, the state nevertheless cannot compel Ms. Pittman to produce the decrypted contents of her iPhone without first demonstrating with reasonable particularity that it knows what documents it will find there. The Court of Appeals' conclusion to

the contrary warrants reversal, even if this Court were to conclude that the foregone-conclusion rationale could apply in this context.

III. COMPELLED RECOLLECTION, DISCLOSURE, OR USE OF A PASSCODE BY THE TARGET OF A CRIMINAL INVESTIGATION IS PROHIBITED BY ARTICLE I, SECTION 12, OF THE OREGON CONSTITUTION.

Article I, section 12, provides: "[N]o person shall * * * be compelled in any criminal prosecution to testify against himself."[9] Although the language used in Article I, section 12, is not as broad as some other states' self-incrimination provisions, this Court has consistently held that the reference to "testify[ing]" alone should not be construed as an intention to narrow a criminal defendant's protections under the provision. *Vondehn,* 348 Or. at 468; *Cram*, 176 Or. at 579; *Soriano,* 68 Or. App. at 646 n. 4.

On the contrary, Article I, section 12, broadly protects a criminal defendant from any form of state-compelled self-incrimination, *Cram*, 176 Or. at 579, including being compelled to testify, furnish evidence, or provide the state a link in its effort to secure evidence against a defendant, *id.* at 581 (citing

[9] Like many Oregon constitutional provisions, Article I, section 12, was copied from the Indiana Constitution, and the Oregon framers did not discuss it specifically when adopting it. *See* Claudia Burton and Andrew Grade, *A Legislative History of the Oregon Constitution,* 37 Willamette L. Rev. 469, 519-520 & n. 256 (2001).

8 Wigmore on Evidence § 2263) (the privilege against self-incrimination is "not limited to testimonial utterances, but extended to prevent the compelled production of documents or chattels"); *Soriano*, 68 Or. App. at 646 n.4 ("We see no reason to construe the Oregon Constitution to give protection from testifying but not from furnishing evidence."); *Vondehn*, 348 Or. at 469-70 (Article I, section 12, imposes "no distinction between compelled statements and physical evidence derived from such statements or between the use of compelled statements to obtain evidence and as testimony at trial.").

Although the Fifth Amendment and Article I, section 12, have similar roots, "the Oregon Constitution has a content independent of that of the federal constitution," and, must be considered in the light of the values and purposes the Oregon Constitution was intended to serve. *Soriano*, 68 Or. App. at 645. Three of this Court's cases analyzing Article I, section 12—*Cram*, *Soriano*, and *Vondehn*—illustrate that an order compelling the target of a criminal investigation to recall and reveal her encrypted phone's passcode violates Article I, section 12, and that there is no basis, constitutionally or logically, to incorporate a "foregone-conclusion" exception to Article I, section 12.[10]

[10] The Court of Appeals did not cite, let alone distinguish, these cases in reaching its decision. If, after reviewing these cases, this Court nevertheless

First, in *Cram*, decided in 1945, the issue was "whether the testimony of a physician as to the alcohol content of a sample of the defendant's blood, taken from him while under arrest and in custody, violated the defendant's rights under Article I, section 12." *Vondehn*, 348 Or. at 468 (citing *Cram*, 176 Or. at 578-79). Before analyzing the proposed testimony, this Court confirmed that Article I, section 12, was intended to preclude state action compelling "testimonial utterances," which included the production of "documents and chattels." *Cram*, 176 Or. 581. It further held that physical evidence "obtained by means other than compulsion of the defendant, * * * is admissible as long as admission does not depend on the defendant being called upon to make 'any act or utterance of his own.'" *Vondehn*, 348 Or. at 468 (quoting *Cram*, 176 Or. at 582). Because "[t]he blood sample was obtained without the use of any process against him as a witness," and he was not compelled to "establish the authenticity, identity, or origin of the blood[,] those facts were proved by other

---

concludes there was room in Article I, section 12, analysis to incorporate the Fifth Amendment's so-called "foregone-conclusion" rationale, the Court should reverse for the reasons articulated in *amici's* briefing discussing the Fifth Amendment.

witnesses[,]" this Court concluded that the physician's testimony did not implicate Article I, section 12.[11] *Cram*, 176 Or. at 593.

In stark contrast, here, Ms. Pittman was compelled through an "obvious example[ ]" of state compulsion—a court order—to engage in a testimonial act herself (her recollection and typing of the passcode in front of the officer). *See Fish*, 321 Or. at 57 (identifying a court order as an obvious example of compulsion). *Cram* demonstrates that whether Ms. Pittman entered an accurate passcode (leading to an inference that she has access to the device and its contents, and forcing her to facilitate the state's efforts to gather evidence against her) or an inaccurate passcode (arguably leading to an inference that she had an incriminating reason not to want law enforcement to know what was on her phone), the trial court's *order* compelling her to make "an act or utterance" on her own violated her right against self-incrimination found in Article I, section 12.

Second, in *Soriano*, the question was whether the Oregon Constitution required the state to grant a witness "transactional" immunity before the witness

[11] The defendant in *Cram* had not contested the blood draw as unlawful search or seizure nor did he question whether "physical evidence concerning a person's identity, appearance, or physical condition implicates Article I, section 12," so those issues were expressly not resolved in the decision. *Soriano*, 348 Or. at 468 n. 4.

could be compelled to testify about potentially incriminating events or if, as is permitted by the United States Supreme Court's interpretation of the Fifth Amendment, the state could compel such testimony upon the granting of "use and derivative use" immunity.[12] *Soriano,* 68 Or. App. at 644; *see Kastigar*, 406 U.S. at 455-59 (holding use and derivative use immunity sufficient under Fifth Amendment).

As noted, this Court expressly stated that the Oregon Constitution, and Article I, section 12, in particular, had meaning independent from the United States Constitution and that it was ultimately this Court, and no other, that was the final arbiter of its meaning. *Soriano,* 68 Or. App. at 645. A core principle of Article I, section 12, is that *before* a witness can be compelled to testify, the witness must be adequately protected from the possibility that the testimony could be used in *any way* against the witness. *Id.* at 663. Because, even with the use and derivative use immunity required by the Fifth Amendment (as articulated United States Supreme Court in *Kastigar)*, the state still might find a way to use the statement against the witness, full transactional immunity was

[12] Use and derivative use immunity precludes the state from using "the immunized testimony or any of its direct or indirect fruits," but does not preclude prosecution entirely. *Soriano,* 68 Or. App. at 644 n.3. Transactional immunity immunizes the witness "from prosecution for any offense to which the immunized testimony relates." *Id.*

required to fully realize an individual's rights guaranteed by Article I, section 12:

> [W]hen a witness provides compelled statements, those statements may influence a prosecution even if they are not offered in evidence or used to obtain derivative evidence. [*Soriano*, 68 Or. App.] at 663, 684 P.2d 1220. For example, the statements may affect the discretionary decisions of a prosecutor to bring charges or to accept a plea bargain. *Id.* The [*Soriano*] court held that the state could not compel the statements of a witness without granting transactional immunity because, without protecting the witness from all evidentiary and nonevidentiary use of compelled statements, the state would not afford the witness the same protection that the constitution confers—the right to remain silent. *Id.* at 662, 684 P.2d 1220.

Vondehn, 348 Or. at 468. Like *Cram*, *Soriano* dictates reversal here for it is beyond dispute that the purpose of compelling Ms. Pittman's testimony (in the form of her recalling and entering the passcode) was to assist the state in its prosecution against her. Such compulsion is flatly prohibited by Article I, section 12.

Third, in *Vondehn*, as relevant here, the issue was whether the state's failure to issue *Miranda* warnings to a person who was subjected to custodial interrogation should result in the suppression of only the testimonial responses or, alternatively, also the physical evidence discovered as a result of those responses. While the state conceded that the statements must be excluded, the state argued that Article I, section 12, did "not prohibit the admission of

physical evidence, even physical evidence that is a 'fruit' of a defendant's compelled testimony * * *." *Vondehn*, 348 Or. at 467. After engaging in a careful analysis of its decisions in *Cram* and *Soriano*, this Court rejected the state's argument:

> [T]his court has long interpreted Article I, section 12, to impose no distinction between compelled statements and physical evidence derived from such statements or between the use of compelled statements to obtain evidence and as testimony at trial. We reject the state's argument that we should now impose those limitations on the reach of Article I, section 12.

Vondehn, 348 Or. at 469-70. Here, the court's order compelled Ms. Pittman to not only share her thoughts and beliefs about the passcode to law enforcement, but to do so for the express purpose of it facilitating its efforts to secure additional evidence against her. Compelling Ms. Pittman to respond to the order plainly violated Article I, section 12, under *Vondehn*; in the light of this analysis, there is no logical space for a foregone-conclusion inquiry in Article I, section 12, jurisprudence.

As an alternative argument in *Vondehn*, the state argued that a "mere failure" to give a *Miranda* warning was not a "constitutional violation" and, thus, the physical evidence secured in that circumstance could still be used. This Court disagreed:

> [W]e hold that when the police conduct custodial interrogation without obtaining a valid waiver of Article I, section 12, rights, they violate Article I, section 12, and the derivative physical evidence that they obtain must be suppressed.

Vondehn, 348 Or. at 467. In part, this Court reached this conclusion because in contrast to federal jurisprudence, in which the purpose of an exclusionary rule is to deter misconduct, in Oregon constitutional jurisprudence, the purpose is to ensure an individual is able to secure the full effect of his or her constitutional rights. "In the context of a criminal prosecution, the focus is on protecting the individual's rights *vis-à-vis* the government * * *." *Vondehn*, 348 Or. at 473 (quotation marks omitted) (citing *State v. Simonson*, 319 Or. 510, 512, 878 P.2d 409 (1994); *State v. Davis*, 313 Or. 246, 253-54, 834 P.2d 1008 (1992)). This concept further demonstrates the illogical nature of the Court of Appeals' decision to read a "foregone conclusion" limitation into Article I, section 12. Article I, section 12, grants Ms. Pittman the constitutional right *not* to be compelled to serve as a witness against herself, and the values underlying Oregon constitutional jurisprudence call upon the courts to take steps to ensure that she is in a position to fully-effectuate that constitutional right. The trial court's order impermissibly violated that right. The Court of Appeals erred when it concluded otherwise.

Even if this Court were to conclude, as the Court of Appeals did, that the Fifth Amendment jurisprudence was a persuasive guide as to the meaning and application of Article I, section 12, for the reasons outlined throughout *amici*'s brief, this Court should nevertheless reverse. However, a careful review of this Court's precedent provides this Court with a much more direct path for providing Ms. Pittman relief under Oregon law. Not only does Article I, section 12, preclude the state from compelling individuals to disclose their "beliefs, knowledge, or state of mind to be used in a criminal prosecution against them," *Fish*, 321 Or. at 56, it expressly draws no distinction between the state's desire to use such "testimonial" statements in trial and its desire to use such "testimonial" statements to secure additional evidence, *Vondehn*, 348 Or. at 469-70. In either circumstance, the state action compelling the statement over the defendant's objection violates Article I, section 12. Properly understood as affording individuals the fundamental right *not* to be compelled to assist the state in its prosecutorial efforts, there is simply no room for a logically derived "foregone conclusion" doctrine under Article I, section 12. To fully vindicate Ms. Pittman's rights under Article I, section 12, she could not be compelled to provide the state with the passcode to her encrypted device. The trial court and the Court of Appeals erred when they concluded otherwise.

Forced disclosure or entry of a decryption key encroaches on "the right of each individual to a private enclave where he may lead a private life." *Doe II*, 487 U.S. at 212-13 (quoting *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 55 (1964)) (quotation marks omitted). Participating in modern society requires that one expose private information to communications providers—and from there potentially to advertisers, marketers, identity thieves, blackmailers, stalkers, spies, and more. Encryption is designed to protect individuals from these threats.

Encryption may impose obstacles to law enforcement in particular cases. So do window shades. It is sometimes true that constitutional protections interfere with law enforcement investigations. Nevertheless, law enforcement can pursue other means of building its case, including securing incriminating statements by witnesses and evidence from third parties like telecommunications providers. The Oregon and United States constitutions accept that otherwise relevant evidence will sometimes be placed off-limits in order to strike a necessary balance between individual civil liberties and government power. Constitutional protections must be maintained, if not strengthened, in the digital age.

CONCLUSION

Because the disclosure of Ms. Pittman's passcodes is inherently testimonial and because the foregone-conclusion rationale does not and should not allow the government to compel disclosure of the contents of a defendant's mind, this Court should reverse the trial court's order.

Dated this 16th day of June, 2020.

Respectfully submitted,

BOISE MATTHEWS EWING LLP

/s/ Kendra M. Matthews
KENDRA M. MATTHEWS
OSB No. 965672
1050 S.W. Sixth Ave., Suite 1400
Portland, OR 97204
Telephone: 503-228-0487
Kendra@boisematthews.com

Attorney for Amici Curiae
ACLU of Oregon,
American Civil Liberties Union, and
Electronic Frontier Foundation

ACLU FOUNDATION OF OREGON

/s/ Kelly Simon
KELLY SIMON
OSB No. 154213
P.O. Box 40585
Portland, Oregon 97240
Telephone: 503-444-7015
KSimon@aclu-or.org

Attorney for Amicus Curiae
ACLU of Oregon

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the word count limitation in ORAP 5.05(1)(b)(ii)(A) because the word count of this brief (as described in ORAP 5.05(1)(d)(i)) is 8,752 words.

I 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 in ORAP 5.05(4)(f).

Dated this 16th day of June, 2020.

BOISE MATTHEWS EWING LLP

/s/ Kendra M. Matthews

KENDRA M. MATTHEWS
OSB No. 965672
1050 S.W. Sixth Ave., Suite 1400
Portland, OR 97204
Telephone: 503-228-0487
Kendra@boisematthews.com

Attorney for Amici Curiae
ACLU of Oregon,
American Civil Liberties Union Foundation,
and Electronic Frontier Foundation

CERTIFICATE OF FILING AND SERVICE

I certify that on June 16, 2020, I caused the original **BRIEF OF *AMICI CURIAE*** to be electronically filed with the State Court Administrator, Records Section, by using the Court's electronic filing system.

I further certify that June 16, 2020, I served this **BRIEF OF *AMICI CURIAE*** on the following parties using the Court's electronic filing system:

Ernest Lannet, OSB No. 013248
Chief Defender
Criminal Appellate Section
OFFICE OF PUBLIC DEFENSE SERVICES
1175 Court Street NE
Salem, Oregon 97301
Telephone: 503-378-3479
Ernest.G.Lannet@opds.or.us

Attorney for Petitioner-on-Review Cattrice Pittman

Franz H. Bruggemeier, OSB No. 163433
OREGON JUSTICE RESOURCE CENTER
P.O. Box 40588
Portland, Oregon 97240
Telephone: 503-768-7321
FBruggemeier@ojrc.info

Attorney for Amici Curiae Laurent Sacharof and Oregon Justice Resource Center

Jonathan N. Schildt, OSB No. 151674
Assistant Attorney General
OREGON DEPARTMENT OF JUSTICE
1162 Court Street NE
Salem, Oregon 97301
Telephone: 503-378-4402
Jonathan.N.Schildt@doj.state.or.us

Attorneys for Respondent-on-Review State of Oregon

Dated this 16th day of June, 2020.

BOISE MATTHEWS EWING LLP

/s/ Kendra M. Matthews

KENDRA M. MATTHEWS
OSB No. 965672
1050 S.W. Sixth Ave., Suite 1400
Portland, OR 97204
Telephone: 503-228-0487
Kendra@boisematthews.com

Attorney for Amici Curiae
ACLU of Oregon,
American Civil Liberties Union, and
Electronic Frontier Foundation