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

CA A162950

S067312

BRIEF ON THE MERITS BY *AMICI CURIAE* LAURENT SACHAROFF AND THE OREGON JUSTICE RESOURCE CENTER IN SUPPORT OF PETITIONER PITTMAN

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

---

Court Decision Affirmed With Opinion: October 16, 2019
Before: Hadlock, P.J., DeHoog, J., and Aoyagi, J.

(Counsel Listed on the Next Page)

ERNEST G. LANNET #013248
Chief Defender
Criminal Appellate Section
SARAH LAIDLAW #111188
Deputy Defender
Office of Public Defense Services
1175 Court Street NE
Salem, OR 97301
Ernest.Lannet@opds.state.or.us
Sarah.Laidlaw@opds.state.or.us
Phone: (503) 378-3349
Attorneys for Defendant-Appellant

FRANZ H. BRUGGEMEIER, #163533
Oregon Justice Resource Center
P.O. Box 40588
Portland, Oregon 97240
Telephone: (503) 768-7321
Email: fbruggemeier@ojrc.info
LAURENT SACHAROFF
University of Arkansas School of Law
WATR 262 University of Arkansas
Fayetteville, Arkansas 72701
Telephone: (479) 575-4578
Email: lsacharo@uark.edu
Attorney and authors for Amici Curiae
Laurent Sacharoff and Oregon Justice Resource Center

ELLEN F. ROSENBLUM #753239
Attorney General
BENJAMIN GUTMAN #160599
Solicitor General
JONATHAN N. SCHILDT #151674
Assistant Attorney General
400 Justice Building
1162 Court Street NE
Salem, OR 97301
benjamin.gutman@doj.state.or.us
jonathan.n.schildt@doj.state.or.us
Phone: (503) 378-4402
Attorneys for Plaintiff-Respondent

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

///

Other Authorities

BRIEF IN SUPPORT OF PETITIONER'S BRIEF ON THE MERITS BY *AMICI CURIAE* LAURENT SACHAROFF AND THE OREGON JUSTICE RESOURCE CENTER

INTEREST OF *AMICI CURIAE*

Laurent Sacharoff is a law professor who regularly writes on the topic of compelling passwords, including *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 Fordham L Rev 203 (2018), and *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 Texas L Rev Online 63 (2019). His interest is in the best interpretation of the Fifth Amendment and a robust recognition of individual liberties in the digital age. He joins this brief in his personal capacity, and the views here do not necessarily represent those of the University of Arkansas.

The Oregon Justice Resource Center (OJRC) is a Portland-based non-profit organization founded in 2011. The OJRC works to dismantle systemic discrimination in the administration of justice by promoting civil rights and by enhancing the quality of legal representation to traditionally underserved communities. The OJRC serves this mission by focusing on the principle that our criminal justice system should be founded on fairness, accountability, and evidence-based practices. The OJRC Amicus Committee is comprised of Oregon attorneys from multiple disciplines and practice areas.

STATEMENT OF HISTORICAL AND PROCEDURAL FACTS

Amici adopt the petitioner's statement of historical and procedural facts.

QUESTIONS PRESENTED

Amici respectfully suggest the questions presented be as follows:

1. Does an order to compel an individual to disclose her password to the court or state officials compel "testimony" protected by the Fifth Amendment to the United States Constitution?
2. Should the foregone conclusion exception ever apply to such compelled disclosure?
3. When an individual is compelled to enter her password to open a device without disclosing the password, does the foregone conclusion exception apply to the password only or to the underlying files on the device as well?

SUMMARY OF ARGUMENT

In any compelled password case, courts must first distinguish two very different categories. In the first category, a court orders an individual to disclose to the government or the court her password. The court may order her to orally tell officers her password, or supply it in writing, or even enter the password in front of them such that the officers learn the contents of the password itself for possible future use.

In the second category, a court orders her to *enter* her password to open the device in a way that no one sees or learns the password itself, and the device does not record it. True, she discloses her password to the device in some metaphorical way, but the device itself, because of the magic of encryption technology, does not keep a record of the passcode entered. The government never learns the content of the password, but it does obtain access to the files on the device. The individual has essentially produced the documents just as she might in response to a subpoena.

The first category, compelling actual disclosure of a password itself to the government, presents an easy case. Nearly every court, drawing on straightforward principles from the United States Supreme Court, agrees that such compelled disclosure violates the Fifth Amendment. In this first scenario, we need not analogize to a document production or invoke the "act of production doctrine," much less use the complicated "foregone conclusion exception." Rather, compelling a person to disclose her password to others stands on the same footing as compelling her to state the location of a body or state the location of a bank account. All such orders compel full-fledged "testimony" under the Fifth Amendment.

This case falls into this first, easy category of cases. The trial court compelled petitioner to enter a passcode into her device, in open court, in view of a

watching officer. She was required, in essence, to tell her passcode to the court and state. The court did not order her to enter the password secretly to open the device, presumably because it wanted to see the actual number she entered—in this case, "123456." The content mattered, and the passcode she entered was a true-or-false statement (in this case, apparently, false). By entering a false password, petitioner exposed herself to adverse consequences.

The answer to the first question presented (as proposed by *amici*) is, therefore, simply yes. Petitioner was compelled to disclose her passcode, or a purported passcode, to a watching officer. This is full-fledged testimony under the Fifth Amendment with no exceptions, under the foregone conclusion exception or otherwise.

But many *other* password cases involve a harder question, and this court may well wish to answer the broader question. When does it violate the Fifth Amendment to compel a person to enter her password to open a device without disclosing the password to any other person? All, or nearly all, courts and scholars agree that the answer to this separate question lies in drawing an analogy to the act of production cases.

Courts are forced to find analogies because opening a device without disclosing the password to another person is part physical act and part testimonial act. Courts analogize to a person producing documents in response to a subpoena

because that act, too, has a similar hybrid character. The two scenarios are analogous because opening a device is an act that hands over the files on the device to law enforcement, just as producing documents does in response to a subpoena.

But courts differ on how they apply the analogy. Some courts hold that the testimony implicit in opening the device is limited to the fact that the person knows the password. That view is wrong. Other courts correctly hold that the act of opening a device implicitly communicates that the files on the device are in the possession of the person—exactly as the analogy would work in an ordinary act of production case.

The key lies in identifying the manner in which the Supreme Court has said the act of producing papers "implicitly communicates," and then applying that principle to devices. For ordinary document productions, the act of producing documents implicitly communicates that they exist, that the person possesses them, and that they are authentic. Similarly, when a person opens a device, that act implicitly communicates that the files on the device exist, that the defendant possesses them, and that they are authentic.

Once we have identified the way in which opening a device is testimonial, we can properly apply the foregone conclusion exception. In ordinary document production cases, the foregone conclusion exception applies to the documents produced because the act of producing them implicitly communicates information

about their existence, who possesses them, and their authenticity. Similarly, we must apply the foregone conclusion exception to the files on a device because the act of opening it communicates analogously about those files' existence, possession, and authenticity.

When we apply the foregone conclusion exception to the files on a device, we arrive at the same rule as for ordinary document productions: the government cannot compel a person to open a device unless it can show that it already knows that the files it seeks on the device exist, that the defendant possesses them, and that they are authentic. It must show that knowledge *before* it compels the person to open the device. It must also show that knowledge by describing the files with "reasonable particularity."

In this case, the state has apparently failed to show it knows of any particular files on the device and therefore could not have compelled the petitioner to open her device even if it had sought to do so without also forcing her to disclose her password to others.

The Court of Appeals mistakenly applied the foregone conclusion doctrine to knowledge of the password only. It reasoned that this case differs from ordinary act of production cases because the state already possesses the files at issue pursuant to a warrant. This brief shows why that argument is wrong. The state possesses encrypted versions of the files only. It must rely upon the testimonial

aspect of the defendant entering the password to *authenticate* the decrypted versions that it wishes to read and use. This case thus is no different from an ordinary act of production case.

This brief will use two labels to describe the two categories of cases potentially at issue before this court. The first category involves compelling an individual to disclose her password to others, as happened in this case. This category involves "full-fledged testimony" that enjoys ordinary and complete Fifth Amendment protection without any recourse to the act of production cases or the foregone conclusion exception.

The second category involves compelling a person to open her device without disclosing the password to others, the hypothetical scenario this court may wish to answer. This second category involves what this brief calls "quasi-testimony," the kind of testimony involved in the act of production cases. It is "quasi" because the United States Supreme Court has effectively afforded it a lesser status than full-fledged testimony. It can be defeated by the foregone conclusion exception, whereas full-fledged testimony cannot be. The United States Supreme Court has not adopted this terminology, but its cases have effectively created such a dichotomy.

ARGUMENT

I. STATEMENTS ASSERTING A TRUE-FALSE PROPOSITION ARE ALWAYS "TESTIMONIAL" UNDER THE FIFTH AMENDMENT.

The Fifth Amendment prohibits compelling a person to be a "witness against himself," or, as the United States Supreme Court more often formulates it, to supply "testimony." *E.g.*, *Fisher v. United States*, 425 US 391, 96 S Ct 1569, 48 L Ed 2d 39 (1976); Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 Fordham L Rev 203, 213 (2018). Under either formula, the Fifth Amendment protects against the straightforward paradigm of requiring a person to supply true-false information that sheds light on guilt. *Pennsylvania v. Muniz*, 496 US 582, 589, 110 S Ct 2638, 110 L Ed 2d 528 (1990). The statement or information need not be admissible as incriminating evidence itself; rather, to be protected, the statement can merely "furnish a link in the chain" to incriminating evidence. *Hoffman v. United States*, 341 US 479, 486, 71 S Ct 814, 818, 95 L Ed 1118 (1951).

The Fifth Amendment protects a defendant from incriminating herself, from being compelled to state a true or false type statement that is itself evidence or that can lead to evidence against her. It does so for many reasons. *See, e.g.*, *Sacharoff*, 87 Fordham L Rev at 243 (surveying justifications). The Court has said the government should shoulder the burden of proving guilt, for example. *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 US 52, 55, 84 S Ct 1594, 1597, 12 L Ed

2d 678 (1964). Some argue it protects a particular sphere of privacy. But for our purposes, the most often quoted rationale hinges on the image of the "cruel trilemma." *Muniz,* 496 US at 597 ("At its core, the privilege reflects our fierce unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt.") (internal quotation and citation omitted).

The cruel trilemma asks us to assume there is no Fifth Amendment right and describes the unfair trilemma facing the defendant that would result. The cruel trilemma involves forcing a defendant to choose one of three difficult and harmful paths: (1) telling the truth and convicting herself, (2) lying and thereby committing perjury, or (3) remaining silent and suffering a contempt order, likely resulting in jail time. The cruel trilemma depends centrally on the notion that the statement is a true-false kind of statement, one where the defendant *could* lie, or could tell the truth and incriminate herself. *Sacharoff*, 87 Fordham L Rev at 224, 227.

Put another way, the government compels a person to retrieve information from her memory and disclose that information to the government. The compulsion and the disclosure of the true-false information *coincide,* and to compel such true-false information therefore violates the Fifth Amendment.

Most testimony falls under this category of ordinary, full-fledged testimony that enjoys absolute Fifth Amendment protection, susceptible to no exceptions, including the foregone conclusion exception. As the Court said in *Muniz*, "the vast

majority of verbal statements thus will be testimonial" because they likely "convey information or assert facts." 496 US at 134.

A. The Foregone Conclusion Exception Never Applies to True-False Statements Disclosed to Others.

The foregone conclusion exception never applies to ordinary, full-fledged testimony. The foregone conclusion exception is entirely a creature of the act of production doctrine. It represents an exception the government can employ in cases that involve an *act*, such as producing documents or opening a phone. It cannot, should not, and must not apply to ordinary *statements*.

In *Fisher*, the Court created the act of production doctrine and its foregone conclusion exception. *See* 425 US 391. The premise in *Fisher* is that the Fifth Amendment does not protect the *content* of documents subpoenaed because the subpoena does not compel the person to *create* the documents but merely to surrender documents previously, and voluntarily, created. *See id.* But in compelling a person to state or otherwise disclose a true-false statement (such as a password), the government *does* compel the creation of new, fresh testimony. The principle of *Fisher* and its attendant act of production doctrine do not apply.

To apply the foregone conclusion exception to ordinary testimony would lead to absurd results. For example, if the police see and smell a suspect smoking methamphetamine, they obviously know he possesses methamphetamine. May they compel him, or may a court compel him, to admit he possessed

methamphetamine? Of course not. He enjoys an absolute Fifth Amendment right against any compelled statement that he did, or did not, possess methamphetamine.

But if we applied the foregone conclusion exception to this scenario, the government would be able to coerce a confession. After all, the government already knows he possessed methamphetamine, and it can show with reasonable particularity that it does know this fact. Were he to confess that he possessed methamphetamine, it "adds little or nothing" to the government's overall information. *See Fisher*, 425 US at 411. And yet it would be absurd to allow such coercion under the foregone conclusion exception. Indeed, even though the government already knows the fact at issue, a confession from the defendant would make conviction far easier. A jury will be far more likely to convict if the defendant confesses than if he does not and the jury must rely entirely on the testimony of a police officer.

B. The Compelled Disclosure of the Password Here Compelled Full-Fledged Testimony in Violation of the Fifth Amendment.

In this case, petitioner was compelled to enter her password within view of a watching officer who reported what she entered to the trial court. *State v. Pittman*, 300 Or App 147, 152, 452 P3d 1011 (2019), *rev all'd*, 366 Or 257, 458 P3d 1121 (2020). Petitioner was compelled to supply "testimony" in its full-fledged form, no different from being required to state the location of a body or a bank account.

The password is, of course, a true-false statement. The principles of *Muniz* apply with full force here. *See* 496 US at 134. Entering the password before court and officer amounts to answering the question, "What is your password?" It would be no different if the court had said, "What is your bank account number?" and compelled petitioner to answer. The order here compelled a true-false statement because petitioner could have typed in and disclosed her true password or a false one.

As with any true-false statement, the officer who learns the password could use it later to open the device and gain access to further incriminating evidence. Law enforcement could try the password on other devices or accounts. As in *Hoffman*, this true-false statement, if true, can form a "link in the chain" to incriminating evidence. 341 US at 486. Officers would rely on the fact that the statement was true to gain this additional information.

The compulsion here directly implicates the cruel trilemma. Petitioner was forced to choose one of three harmful paths. First, she could have entered the correct password and incriminated herself—both by opening the device and by supplying the password to the authorities who might use it to search for incriminatory evidence on other devices. Second, she could have entered a false password and suffered the penalty of perjury or some other penalty. Third, she could have refused to enter a password and suffer the penalty of contempt.

Here, petitioner entered "123456." It did not work. The trial court apparently concluded that she had entered a false password, found her in contempt, and sentenced her to 30 days in jail. *Pittman*, 300 Or App at 152. How did the court conclude the password was false? It drew its conclusion in part because it *knew the content of the password*. That is, the court first had to know that she did, in fact, enter some numbers at all, and second, that they were "123456." Those numbers in particular are significant because they seem like they could be fake. Not for sure, of course, but the content of the password here no doubt played some role in the court's conclusion.

Petitioner also faced the third prong of the cruel trilemma—refusing to answer and facing contempt for this separate reason. Here, by entering an apparently false password, petitioner supplied a separate foundation for a contempt holding—a refusal to answer the question. Petitioner did not simply say she did not remember her password but entered one that did not work. This performance apparently gave the trial court the evidence it needed to conclude that she had willfully refused to answer rather than that she had simply not remembered.

Strikingly then, these facts improperly skewered petitioner on two of the three horns of the cruel trilemma. The compulsion therefore violated petitioner's Fifth Amendment right.

One might argue that the trial court merely ordered her to open the device, and, as a byproduct, the officer and court observed her enter it. Perhaps one might argue the state and court did not have, as their purpose, to observe the content of the password. But first, no test should depend on the state's purpose in such an inscrutable way. And second, the state's and court's purposes *do* appear to have been to observe the password content as she entered it. They could easily have allowed her to enter something without looking at what she entered, and, indeed, that would be the more physically and culturally natural manner. Instead, the trial court required her to enter the password so that all could see and promptly used that information against her. It is hard to avoid the conclusion that the court compelled petitioner to disclose the content of her password, to utter a true or false statement.

II. EVEN IF PETITIONER HAD OPENED THE DEVICE WITHOUT DISCLOSING HER PASSWORD TO OTHERS, SUCH COMPULSION WOULD VIOLATE THE FIFTH AMENDMENT.

This court may well wish to answer a broader question that will affect many cases moving forward: if a court compels an individual to open her device in such a way that no one else learns the password, and the device does not record it, does that compulsion violate the Fifth Amendment? It does in many cases. Ultimately, we must answer this question by analogizing to the act of production cases.

Opening a device, even as an act, constitutes the "quasi-testimony" that parallels the act of producing documents. This act implicitly communicates that the individual possesses the files on the device, among other things. We must therefore apply the foregone conclusion exception to these files, leading us to the bottom-line test: A court can compel an individual to open her device if and only if the government *knows* the files it seeks are on the device and can describe them with reasonable particularity.

The argument proceeds in several steps. First, it justifies the analogy to the act of production cases, even though courts largely agree on this analogy. Second, it provides background on the act of production doctrine and the foregone conclusion exception in its native sphere—producing documents in response to a subpoena. Third, it applies this analogy to the act of entering a password.

A. Nature of Entering a Password

The court must first answer a threshold question: If a person enters her password to open a device such that no one else learns the password, how should we characterize that act? There are three possibilities. First, we can consider the typing of a password to be the same as ordinary Fifth Amendment testimony enjoying full protection, and we would simply default to the first argument above. Second, we can treat it more like a physical act akin to producing documents—an act that has *some* testimonial aspect sufficient to enjoy Fifth Amendment

protections, but an act to which we must apply the act-of-production analogy and case law. Third, we can treat it as a pure physical act that enjoys no Fifth Amendment protection.

Nearly every court has chosen the second path—analogizing entering a password in some way to the act of production. *See, e.g.*, *United States v. Apple MacPro Computer*, 851 F3d 238, 248 (3d Cir 2017); *In re Grand Jury Subpoena Duces Tecum Dated Mar 25, 2011*, 670 F3d 1335, 1342-46 (11th Cir 2012); *Commonwealth v. Gelfgatt*, 468 Mass 512, 522-24, 11 NE3d 605, 614-15 (2014); *see also Sacharoff*, 87 Fordham L Rev at 229. This brief argues that this is the correct path, both given the existing case law and because there is a strong logical argument that entering a password, even in a way that no one else sees, still deserves full Fifth Amendment protection. *See, e.g.*, Brief of *Amici Curiae* Electronic Frontier Foundation, *et al.*, *Seo v. Indiana*, Cause No. 18S-CR-595, 2019 WL 4573820, at *11 (Ind, Jan 31, 2019). Below, this brief first quickly makes that argument before considering the analogy to the act of production adopted by most courts.

Entering a password resembles full-fledged testimony because it requires the individual to understand the demand to open a device, use her cognitive powers to consult her memory, choose among her many passwords and passcodes the one that corresponds to this device, and transfer that information to her fingers in the

form of typing. The information she conveys is a true-false statement, albeit one that only the device can evaluate as true or false.

These cognitive steps resemble those that any witness would employ in testifying about a past event. She must listen to a question, retrieve the appropriate memory containing the requested information, and verbally disclose that information, orally or in writing. In addition, a person who enters her password to open a device has used that information as a lead for investigators to obtain incriminating information on the device. Entering the password forms, in the words of *Hoffman*, a link in the chain leading to incriminating evidence. 341 US at 486.

Were this court to adopt this reasoning, it would be amply supported by straightforward considerations of the Fifth Amendment and would enjoy the benefit of simplicity.

But the vast majority of other courts have not taken this path. Rather, they have analogized to document production in one way or another. Indeed, their disagreement hinges not on whether to adopt the analogy but rather whether to apply the foregone conclusion exception to the password only or to the underlying files as well. *Compare In re Grand Jury Subpoena Duces Tecum Dated Mar 25, 2011*, 670 F3d at 1342-46, *and Commonwealth v. Jones*, 481 Mass 540, 547, 117 NE3d 702, 710 (2019).

B. Act of Production Background

This section provides background on the act of production doctrine for documents in response to a subpoena. A later section applies those principles to opening a device.

In its act-of-production cases, the United States Supreme Court has held that the Fifth Amendment does not protect the contents of previously created documents because their *content* was not compelled. *Fisher*, 425 US at 409. Someone, perhaps the individual, voluntarily created the document at some earlier point. Now, later in time, the government compels the person to surrender the document. The Fifth Amendment does not apply because the compulsion does not coincide with the creation of the content. *Id.*

But when it announced this principle in *Fisher*, the Court also created an exception. The Court noted that the physical act of producing documents itself could constitute a type of testimony, aside from their content. By producing the documents, the person "implicitly communicates" the fact that those documents exist, that she possesses them, and that they are authentic. *Id.* at 410; *United States v. Hubbell*, 530 US 27, 36, 120 S Ct 2037, 2043, 147 L Ed 2d 24 (2000).

To take an easy example, suppose a person is served a subpoena to produce any firearms in her possession, and she physically hands a gun over to the authorities. In doing so, she has implicitly communicated that she possessed a gun

and that it is, in fact, a gun. If we further assume that she cannot legally possess a gun, then she has effectively admitted the key elements of the crime. At trial, the prosecutor could introduce into evidence the fact that she physically handed the gun over as proof she possessed it. As a consequence, she could refuse to respond to the subpoena on Fifth Amendment grounds because producing the gun would supply evidence that would incriminate her. *See Commonwealth v. Hughes*, 380 Mass 583, 592, 404 NE2d 1239, 1244 (1980) ("If the defendant should produce the revolver, he would be making implicitly a statement about its existence, location and control to which the Commonwealth says it would allude at trial to show he had possession and control at some point after the alleged crime.").

In assessing whether the act of producing documents is "sufficiently testimonial," courts examine how much the act communicates facts about the existence, possession, or authenticity of the documents or other thing produced. Courts will often also assess how central and how incriminating that fact happens to be. *Sacharoff*, 87 Fordham L Rev at 218. In the hypothetical example above, producing the gun would meet the test because the act of producing it immediately demonstrates a key element of the crime—possession of a firearm. It suffices that the production sufficiently communicates only one of the testimonial facts, in this case, possession.

Each prong—existence, possession, and authenticity—has its own attributes. The existence prong is the most complicated and least applicable here. The existence prong largely seems to involve the mental effort a witness must employ to respond to a subpoena. *Hubbell* involved the existence prong. The Court noted the act of production communicated that the requested document existed in the sense that the individual had to read the subpoena, look through his own documents, and find documents that met that requirement. *Hubbell* thus required the defendant to use his mind in this particular way. But the act of production doctrine is not limited to this type of mental effort. Indeed, the Court in *Hubbell* expressly noted that the prosecutor had disclaimed any reliance on the act of production for the purposes of proving possession or authenticity—only existence was at issue there. 530 US at 41.

For the prongs of possession and authenticity, the mere fact that the documents were physically produced by the defendant communicates the implied facts of possession and authenticity. We do not need to rely upon whether the defendant used her mind to select documents as we would in an existence case. After all, the key question is whether the *act* of producing documents implicitly communicates facts. The physical act of producing documents "implicitly communicates" both possession and authenticity as an immediate logical consequence. *Hubbell*, 530 US at 36.

The Court in *Fisher* indicated that the physical act of production implied facts about possession aside from those facts arising from the individual reading the subpoena, selecting documents, and producing them. In particular, the Court in *Fisher* said: "Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It *also* would indicate the taxpayer's belief that the papers are those described in the subpoena." 425 US at 410 (emphasis added).

United States v. Greenfield, 831 F3d 106, 118-19 (2d Cir 2016), presents a typical case. There, the government subpoenaed the defendant's bank account statements because his foreign bank refused to produce them. The defendant resisted the subpoena, arguing that merely by producing those bank statements, he would authenticate them. The Second Circuit agreed. The documents produced would have appeared to be bank records, but they would not have been self-authenticating, of course. Rather, to authenticate them at trial, the government would have had to show they came from him or his bank. *Id.*

Note that nothing in the *Greenfield* decision rests upon the argument that the defendant selected documents in response to the subpoena. We can put his judgment aside. If the documents appear to be bank statements, and they physically came from his files, those two facts alone would suffice to authenticate them. Because the act of producing the files would authenticate the bank account records,

the Second Circuit held that the Fifth Amendment protected the defendant in *Greenfield* from having to produce them.

C. Foregone Conclusion Exception

For cases where the act of production would implicitly communicate facts about the existence, possession, or authenticity of documents, the Court in *Fisher* created an exception called the foregone conclusion exception. Even if the act of production is testimonial, that act *loses* its testimonial character if the government already knows the information implicitly communicated by the act of producing the documents. If the government already knows that the document exists, or that the defendant possesses it, or that it is authentic, then it can compel production even though the production implicitly communicates those facts. *Fisher*, 425 US at 411.

The foregone conclusion exception is very strange. In no other Fifth Amendment context does government knowledge of the fact to be compelled create an exception to the Fifth Amendment allowing compulsion. But apparently, because the testimony involved in the act of production is only a secondary, quasi-testimony, the government can avoid the Fifth Amendment protections more easily.

Note that the foregone conclusion exception is not rooted in whether the testimony is incriminating. Rather, it rests in the notion that the so-called testimony

is really not sufficiently testimonial if the government already knows it. *See Fisher*, 425 US at 411. This reasoning does not make much sense, but it is apparently what the court has wrought. Perhaps for this reason, the Court in *Hubbell* appeared to cast doubt on the foregone conclusion exception entirely. *See* 530 US at 44 ("Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it.").

As for its contours, the foregone conclusion exception requires the government to show that the documents sought exist, that the defendant possesses them, and that they are authentic; moreover, it must make this showing by describing the documents with "reasonable particularity." *Hubbell*, 530 US at 30. This showing largely boils down to showing that the defendant possesses the document, since the other two prongs will likely follow from that showing. The government must make this showing before the documents have been produced, of course.

The *Greenfield* case referenced above provides a ready example of how the foregone conclusion exception works. The government sought bank account records from the defendant because the foreign bank would not produce them. The government had reason to believe the defendant, or entities he controlled, banked there, but it could not show that the defendant currently possessed the account documents. *Greenfield*, 831 F3d at 126. The foregone conclusion exception does

not apply where the government merely argues that businesspeople always possess "general business or tax records" of the broad categories described in the subpoena. *Id.* at 116 (quoting *Hubbell*, 530 US at 116).

Note how the foregone conclusion exception must match the way in which the original act of production was testimonial. If the act of producing documents implicitly communicates the existence of the documents, as in *Hubbell*, the government must show, under the foregone conclusion exception, that it knows of the existence of these documents by describing them with reasonable particularity. The government could not do that in *Hubbell*. If the act of producing them would communicate that the person possesses them, the government must show it already knows he possesses them. It could do so by showing he received monthly statements from his bank. Or that a friend had sent him a particular text. Finally, if the act communicates authenticity, then the government must show it can authenticate the documents independently. *E.g.*, *Greenfield*, 831 F3d *passim*. It might be able to call a bank employee to authenticate the bank records produced by the individual.

In *Greenfield*, the government failed to show that the defendant possessed some of the bank records and other documents at issue. True, he may once have, but time had passed for many of them. He may have thrown them out. As for the authenticity prong, the court held that the government would be unable to

authenticate the bank records independently of production because the foreign bank refused to cooperate by producing them or providing a witness to authenticate them. For this reason, too, the government failed to meet the foregone conclusion exception and the defendant could thus resist the subpoena on Fifth Amendment grounds. *Id.* at 110.

To meet the foregone conclusion exception, the government must describe the contents of the document with reasonable particularity. *Hubbell*, 530 US at 30. A bank statement from a given bank for a given month for a given account would ordinarily suffice. But this requirement does not mean the contents of the document themselves are protected by the Fifth Amendment. Rather, in showing that it already knows the individual possesses the document, for example, it must of course describe the contents of the document to show what it is the government knows he possesses.

The foregone conclusion exception thus "applies" to the documents themselves in the sense that it links the act of production to the documents. It is the act of production that does the testifying, but the implicit fact communicated is possession, say, of a particular document. It is for that reason the government must describe the document itself even though the contents are not protected. It must describe the document in order to *identify* it, in order to show it already knows the

substance of the testimony communicated by the act of production—namely, that the person possesses that *particular* document.

D. The Act of Entering a Password and Opening a Device Implicitly Testifies that the Files on the Device Exist, are Possessed by the Defendant, and are Authentic.

We must first quickly summarize what it means to "open" an electronic device. Very briefly, when a device is locked, that means two things. First, its processor will not fully function, and, second, its storage medium, such as a hard drive, is encrypted. If the storage medium were not encrypted, the government could simply remove the hard drive, mount it on a different device, and read it. Strong encryption means, however, that the hard drive cannot be decrypted without the password to the device. *Sacharoff*, 87 Fordham L Rev at 221.

When a person enters her password, it releases a chain of events that access longer encryption keys that unlock the device. Once the device is unlocked, the processor will operate, and the device can decrypt the information on the storage medium. In fact, the only way to decrypt the information on the storage medium is by way of the device itself. *Id.*

The act of opening an electronic device resembles producing documents. In opening a device, the individual has implicitly communicated that the files therein exist. Before opening the device, the hard drive or other storage medium appears to be random 0's and 1's. Maybe these are encrypted files, and maybe not. It will all

look the same until decrypted. *In re Grand Jury Subpoena Duces Tecum Dated Mar 25, 2011*, 670 F3d at 1340. Opening the device also communicates that the individual possesses the files on the device because they are on her device. Finally, those files are likely to be authentic because of their location. The testimony implicit in opening a device corresponds with that in producing documents.

To illustrate, let us take as an example a child pornography possession case, first describing how it would work with a physical document production and then how it would work with the more common scenario of an electronic device. Suppose the government subpoenas an individual to produce any physical images of child pornography in his possession, and he does so. That *act* has sunk him. The government can display the images to the jury and link them to the defendant. The government will call a witness to testify that the defendant produced the images to the government. This testimony about the production will establish possession, a key element in the crime.

True, there are other implicit testimonial facts arising from the production. The defendant read the subpoena and produced these images in response to a demand that he produce any child pornography in his possession. His production of the images is some evidence that the image does in fact depict minors engaged in sexually explicit activity and that he knows this. The latter fact is significant because it would establish *mens rea*. But this latter fact is not the only fact his

production implicitly communicates. In assessing what facts are communicated by a given production, we are not limited to those facts only that arise out of the exercise of the defendant's judgment in responding to the subpoena.

In other words, the mere fact that the defendant handed over the image, regardless of what he actually thought it was, is implicit testimony about possession. He could have produced an entire box of photographs through which he never looked, and that production would include the implicit testimony that he possessed whatever was within.

The same rules should apply to an electronic device. In the typical case, a person in a suspected child pornography case has been compelled to enter her password to open a device. If she does so, and the government finds child pornography on the device, her *act* of opening it implicitly testifies that she possessed the images on it. *E.g.*, *In re Grand Jury Subpoena Duces Tecum Dated Mar 25, 2011*, 670 F3d at 1335. The images are authenticated in the sense that they can be established as having come from her device. The encryption scramble has been unscrambled by her act. True, her opening the device does not directly show that in her judgement the images on the device are child pornography, but again, that is only one type of implicit testimony that arises from an act of production or from opening a device.

We may take the facts of this case also as an illustration with the key alteration that the trial court had ordered petitioner to open the device without disclosing her password. Had the court done so, it would still have compelled petitioner to have implicitly testified to incriminating facts. By opening the device, she would have implicitly testified that she possessed any files on the device and that those files are authentic.

For example, one of the charges involves delivery of methamphetamine. Suppose, purely as a hypothetical scenario, the state found a text sent by this phone that says, "I will sell you meth tomorrow," attaching a photo of the product. These pieces of evidence are incriminating, of course, but only if the state can tie them to defendant. The text is only incriminating if defendant wrote it.

Courts have struggled to establish tests for authenticating texts or emails, in part because more than one person can send an email from a particular device. For texts, courts often require a showing that the text came from that device (either directly or was sent from that phone number) plus other circumstantial evidence narrowing down the sender to a particular person based on content. *Commonwealth v. Koch*, 2011 PA Super 201, 39 A3d 996, 1005 (2011).

In our hypothetical scenario, the state could authenticate the text by showing it came from defendant's phone, along with other circumstantial evidence that it was she who sent it. If defendant opens the phone, this evidence tends to

authenticate any text on it, including the text we have imagined, if there are other signs that defendant wrote it. As a consequence, under the act of production cases, her opening the phone implicitly communicates testimonial facts about authenticity and thus that act of opening the phone enjoys Fifth Amendment protection.

Note that the state could establish authenticity of a particular text found on a defendant's phone without opening her device if it could retrieve that same text from the recipient instead.[1] But under the foregone conclusion doctrine, discussed below, the state would have to demonstrate its ability to authenticate particular texts independently before compelling petitioner to open her phone. It has not done so.

III. UNLOCKING A DEVICE COMMUNICATES MORE THAN KNOWLEDGE OF THE PASSWORD.

The courts are split in how to apply the act of production doctrine to devices. *Cf. In re Grand Jury Subpoena Duces Tecum Dated Mar 25, 2011*, 670 F3d at 1342-46, *and Commonwealth v. Jones*, 481 Mass at 547. Some courts hold or suggest that the password is the thing produced or that knowledge of the password is the only fact implicitly communicated by the act of opening the device. *Jones*, 481 Mass at 547; Orin S. Kerr, *Compelled Decryption and the Privilege Against*

[1] There are other ways, of course, to authenticate a text, such as testimony from the recipient who is familiar with the sender. *State v. Mulcahey*, 219 A3d 735, 740 (RI 2019).

Self-Incrimination, 97 Texas L Rev 767 (2019). They therefore apply the foregone conclusion doctrine to knowledge of the password only. This view is mistaken.

First, saying the password is the thing produced would be like saying that the defendant handed the government a box with the password inside. The act of handing over the box implicitly testifies that the piece of paper inside is, in fact, the password. It implicitly communicates that the password exists, that she possesses it, and that it is authentic. After all, she produced the piece of paper with the password on it in response to a demand that she produce the password for the device. We may infer from the fact that this is the piece of paper she handed over that it is authentically the password for this device and not some random set of numbers.

Now, to the extent that we view petitioner here as having been compelled to disclose the actual content of her password, one could argue that it has been produced, but we would also, then, default to the first argument in this brief. To compel the *content* of the password, from her mind, thus making simultaneous compulsion and disclosure to others, is to compel ordinary, full-fledged testimony. If that is the scenario, the act of production cases do not even apply.

But if we now argue, as we do in this section, that the government has compelled the person to enter her password into the device such that no one else learns it, we cannot also argue that the defendant has produced her password in any

way that is analogous to producing documents. When a person produces documents, she discloses their content to the government. That is the whole point. As a result, it makes no sense to say that the password is the thing produced when no one else learns of it. Rather, the entering of the password is merely the act that gives access to the files on the device.

The more common but mistaken argument says that the act of entering the password implicitly testifies that the defendant knows her password. True, but the act of opening the device is not *limited* to this testimonial fact. After all, in an ordinary document production case, we do not limit the implicit fact communicated to simply the fact that the defendant has the ability to produce the documents. Whether we deal with opening an electronic device or producing documents, in both cases the defendant implicitly testifies that the files on the device, or the documents produced, exist, are in her possession, and are authentic.

The foregone conclusion exception must therefore apply to the files on the device. Or, more precisely, the testimony implicit in opening a device is that the files on the device exist, that the defendant possesses them, and that they are authentic *and* that the government already knows these facts. The government must prove that it already knows that the defendant possesses the files it seeks. It can only do so by describing those files with reasonable particularity and also showing how it knows they are on the device. Again, in *Greenfield*, the court

required the government to describe the bank documents—presumably which bank, which month, etc.—and how it knew he still possessed them and had not, for example, thrown them away.

For an electronic device, the facts in *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D Vt, Feb 19, 2009) show how the government can establish the foregone conclusion exception. There, law enforcement initially searched the defendant's laptop, finding several images that appeared to be child pornography. They arrested him, seized the laptop, and shut it. Later, they could no longer access the drive with the images because it was now encrypted. The defendant refused to provide the password and later asserted his Fifth Amendment right. The court correctly held that the government had met the foregone conclusion exception and ordered him to afford them access to decrypted versions of the files. The government knew the images it sought were on the laptop because an officer had seen them, and presumably he could describe them with reasonable particularity. *Id.*

IV. THE COURT OF APPEALS MISTAKENLY APPLIED THE FOREGONE CONCLUSION DOCTRINE TO KNOWLEDGE OF THE PASSWORD ONLY.

The Court of Appeals applied the foregone conclusion exception to the password only and not to the files on the device as well. *See Pittman*, 300 Or App at 161. Under its view, the state needed only show that petitioner knew the

password to the device to satisfy the exception. It reasoned that the act of production cases apply differently here because the state already possessed the data pursuant to a search warrant. As a consequence, the "act of entering the passcode reveals only that defendant has access to that data; it says nothing about the data itself." *Id.*

The Court of Appeals is wrong. The act of entering the password says *everything* about the data itself. It says that the decrypted data *matches* the encrypted data found on the phone. After all, before the act of entering the password, the state only possesses *encrypted* data, a meaningless scramble of 0's and 1's. The act of entering a password still implicitly communicates facts about existence, possession, and, most importantly, authenticity of the files on the device. The state must, therefore, show that it can meet the requirements of the foregone conclusion doctrine as it applies to those files.

Even on a superficial level, the state does not possess the documents in any meaningful sense. The state possesses an electronic device with a storage medium such as a hard drive that is encrypted. A person who enters a password to open the device has supplied the state with meaningful new information simply by entering the password. If there are files on the device, the act of opening the device allows the state to learn this new fact. If the state did not know the files on the device existed, the fact communicated falls under the act of production doctrine.

Similarly, if petitioner opened the device, the state would then learn which files petitioner possessed, which would be new information that it did not previously know that is also protected by the Fifth Amendment via the act of production doctrine.

But when we understand that nature of strong encryption, we understand that, on a far deeper level, the reasoning by the Court of Appeals is fatally wrong. The Court of Appeals' reasoning, elaborated, essentially says this: The state already had the documents in encrypted form. If petitioner opened the device, the government would then have them in decrypted form. Having both sets of data, the encrypted set on the left and the decrypted set on the right, the state would no longer need petitioner's testimony, or any fact that arises from her opening the device. The state would not need to rely upon the testimonial aspect of petitioner's act. Instead, the state could rely entirely upon the contents of the files—the encrypted set and the decrypted set, and simply match them on their face to show the decrypted files correspond to the encrypted ones. According to the Court of Appeals, since the Fifth Amendment does not protect the content of these files, the court may compel the defendant to open the device.

This argument parallels the manna from heaven argument the government made in *Hubbell*. It argued that once it gets access to the documents themselves, it will rely entirely upon their content and no longer require use of any testimonial

aspect of the defendant's act of production. The Court in *Hubbell* actually accepted the premise of the argument—if the documents really had just magically appeared, that would have been fine. But it noted that the documents did not magically appear like "manna from heaven," and that the government was, in fact, making use of the testimonial aspects of the defendant's act of production. *Hubbell*, 530 US at 42-43.

The same occurs with an encrypted device, though in a manner different than in *Hubbell*. The state is wrong to say that once it has the decrypted files, it can simply compare the decrypted data with the encrypted data on the original phone and *match* them. The nature of strong encryption means that this is precisely what the state cannot do. There is no mathematical way, even after the data have been decrypted, to show that the decrypted data came from the encrypted data—without entering the password into the device. *Sacharoff*, 87 Fordham L Rev at 231-32. In other words, the state must still rely upon the testimonial aspect of the defendant opening the device before the state can authenticate the decrypted files as having come from that device at all. *Id.*

This brings us back to the authentication prong of the act of production doctrine. If the state finds a text on the phone it wishes to introduce at trial, it must authenticate it. It could do so, perhaps, by calling to the stand the recipient to testify she received that text. This method would satisfy the foregone conclusion

doctrine because the state had established, before compulsion, an independent way to authenticate the text, and it had shown, with reasonable particularity, that the particular text existed and was on the defendant's phone (because it is on the recipient's).

But when the state does not have this independent knowledge, the only way it can authenticate the text is to show it came from the defendant's phone. It can only make this showing, in turn, if it can show that the decrypted data match the encrypted data. It cannot do so by simply putting, side by side, the decrypted and encrypted data. It must put in evidence that the decrypted data arose after someone entered a valid password into the device. The opening of the device, by someone who knows the password—*i.e.*, the defendant—is critical testimonial evidence needed to authenticate the data and therefore the text. *Id.*

Put another way, imagine the state wanted to introduce into evidence a letter written in Japanese. It also must introduce an English translation, of course. It must authenticate the English translation. The state cannot simply put, side by side, the Japanese original and the English translation and nakedly assert they correspond or ask the jury to determine they match. Instead, the state must call to testify an expert witness who reads both English and Japanese to verify and authenticate the English translation. In the case of encrypted devices, the act of entering the password equals the testimony of the translator; that act is the only way to show that the

decrypted data match the encrypted data taken from the device. That act is essential to authenticating the file. *Id.*

Finally, as a matter of policy, applying the foregone conclusion exception to knowledge of the password only would lead to drastic incursions on individual privacy. The state will almost always be able to show that an individual knows the password to her own device. The state will also almost always be able to get a warrant to search the device. Smartphones, for example, record so much information that there will almost always be something on the phone relating to a charged crime. Under the Fourth Amendment, once law enforcement has a warrant, almost nothing limits their power to search everywhere on the phone, every folder and file, all metadata. *Id*. at 214-16.

A rule proposed by the government here is a rule that opens up a person's entire digital life, and, therefore, in some ways their entire life, simply upon an arrest for a simple crime or even an offense such as speeding. Because existing Fourth Amendment case law imposes virtually no limits on digital searches, it becomes all the more important that courts properly apply the foregone conclusion exception to devices and require some showing by the government that they know the particular files they seek are on the device.

/ / /

/ / /

CONCLUSION

Amici respectfully request that this court reverse the decisions of the Court of Appeals and trial court finding petitioner in contempt.

Respectfully submitted,

/s/ Franz H. Bruggemeier
Franz H. Bruggemeier, OSB #163533
Attorney for *Amici* Laurent Sacharoff and Oregon Justice Resource Center

CERTIFICATE OF COMPLIANCE

I certify that (1) BRIEF OF AMICUS CURIAE complies with the word count limitation in ORAP 5.05(2)(b) and (2) the word count of this brief, as described in ORAP 5.05(2)(a), is 9,044 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 by ORAP 5.05(4)(f).

CERTIFICATE OF FILING AND PROOF OF SERVICE

I certify that I electronically filed the foregoing BRIEF OF AMICI CURIAE with the State Court Administrator for the Court of Appeals of the State of Oregon by using the appellate electronic filing system on June 9, 2020.

I further certify that, upon receipt of the confirmation email stating that the document has been accepted by the eFiling system, this Amicus Brief on the Merits will be eServed pursuant to ORAP 16.45 on Ernest Lannet, #013248, attorney for Petitioner on Review, and Benjamin Gutman #160599, Solicitor General, attorney for Plaintiff-Respondent.

/s/ Franz H. Bruggemeier
Franz H. Bruggemeier, OSB #163533
Attorney for *Amici* Laurent Sacharoff and Oregon Justice Resource Center