IN THE SUPREME COURT OF FLORIDA

No. SC20-1419

STATE OF FLORIDA

Petitioner,

v.

JOHNATHAN DAVID GARCIA

Respondent.

BRIEF OF *AMICI CURIAE* FLORIDA ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AND PROFESSOR LAURENT SACHAROFF IN SUPPORT OF RESPONDENT

/s/ Diana L. Johnson
DIANA L. JOHNSON
Florida Bar No. 35949
CHAIR, FACDL AMICUS COMMITTEE
407 N. Laura Street
Jacksonville, Florida 32202
(904) 255-4721
djohnson@pd4.coj.net

/s/ Jackie Perczek
JACKIE PERCZEK
Florida Bar No. 0042201
JEANELLE GOMEZ
Florida Bar No. 1026021
BLACK SREBNICK
201 S. Biscayne Boulevard
Suite 1300
Miami, FL 33131
(305) 371-6421
JPerczek@RoyBlack.com

TABLE OF CONTENTS

PAGE (S)

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iv

AMICI STATEMENT OF INTEREST 1

INTRODUCTION AND SUMMARY OF THE ARGUMENT 2

ARGUMENT 4

I. STATEMENTS ASSERTING A TRUE-FALSE PROPOSITION ARE ALWAYS "TESTIMONIAL" UNDER THE FIFTH AMENDMENT. 4

A. Ordering Mr. Garcia to disclose his password compels full-fledged testimony in violation of the Fifth Amendment 7

1. Disclosure of the password is incriminating because it could form a link in the chain to obtain incriminating evidence from the phone 8

2. Disclosure of the password is incriminating because of the "missile" charge in Count 1 of the Information 10

3. Disclosure of the password is not merely an "administrative" or "neutral act . . . with no value or significance" 11

B. The right against self-incrimination does not yield to the State's desire for "unencumbered access" to evidence. 12

II. WHEN THE STATE SEEKS DISCLOSURE OF A PASSWORD, THE STATE IS SEEKING FULL-FLEDGED TESTIMONY AND THE FOREGONE CONCLUSION DOCTRINE IS IRRELEVANT 16

III. IF APPLYING THE FOREGONE CONCLUSION DOCTRINE TO DISCLOSURE OF A PASSWORD, THE OBJECT OF THE FOREGONE CONCLUSION SHOULD BE THE FILES AND DATA ON THE PHONE, NOT JUST THE PASSWORD 20

CONCLUSION 23

CERTIFICATE OF SERVICE 24

CERTIFICATE OF COMPLIANCE 24

TABLE OF AUTHORITIES

FEDERAL CASES **PAGE (S)**

Doe v. United States,
487 U.S. 201 (1988)..... 4

Fisher v. United States,
425 U.S. 391 (1976)..... 2, 4, 16, 17, 21

Hoffman v. United States,
341 U.S. 479 (1951)..... 8, 10, 13, 14, 15

In re Grand Jury Subpoena,
670 F.3d 1335 (11th Cir. 2012)..... 23

Kastigar v. United States,
406 U.S. 441 (1972)..... 15

Pennsylvania v. Muniz,
496 U.S. 582 (1990)..... 5, 6, 7

United States v. Hubbell,
530 U.S. 27 (2000)..... 4, 8, 14

STATE CASES

Ex Parte Senior,
37 Fla. 1 (1896) 23

G.A.Q.L. v. State,
257 So. 3d 1058 (Fla. 4th DCA 2018) 22, 23

State v. Garcia,
302 So. 3d 1051 (Fla. 5th DCA 2020) ..... *passim*

State v. Horwitz,
191 So.3d 429 (Fla. 2016)..... 16, 23

State v. Pollard,
287 So. 3d 649 (Fla. 1st DCA 2019) 22

State v. Stahl,
206 So. 3d 124 (Fla. 2d DCA 2016) 3

OTHER AUTHORITIES

Petitioner's Initial Brief on the Merits,
State v. Garcia, No. SC-1419 (filed 03/12/21) ..... *passim*

Appendix to Petitioner's Initial Brief on the Merits,
State v. Garcia, No. SC20-1419 (filed 03/12/21).....7, 8, 12, 20

Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*,
87 Fordham L. Rev. 203 (2018)..... *passim*

Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*,
97 Texas L. Rev. Online 63 (2019)..... 9, 15

Orin Kerr, *Opinion: A revised approach to the Fifth Amendment and obtaining passcodes,*
http://tinyurl.com/3ksns87u (last visited 6-20-21)..... 19, 20

AMICI STATEMENT OF INTEREST[1]

The Florida Association of Criminal Defense Lawyers (FACDL) is a statewide organization representing more than 1,000 criminal defense practitioners. FACDL is a not-for-profit corporation whose goal is to assist in the fair administration of the Florida criminal justice system. FACDL has an interest in this case as the outcome could have a significant impact on the constitutional rights of criminal defendants in Florida.

Laurent Sacharoff is a professor of law at the University of Arkansas School of Law. Professor Sacharoff regularly writes on the topic of compelling disclosure of 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). Professor Sacharoff's interest is in the best interpretation of the Fifth Amendment and a robust recognition of individual liberties in the digital age. He joins in this brief in his personal capacity, and

[1] No party's counsel authored any part of this brief, and no one contributed money to prepare or submit this brief.

the views expressed here do not necessarily represent those of the University of Arkansas School of Law.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

The Fifth District Court of Appeal correctly held that a court violates the Fifth Amendment when it orders a person to *disclose* the password to his device to law enforcement as part of a criminal investigation. Such compulsion stands on the same unconstitutional footing as compelling a defendant to state the location of a body or the location of a bank account. It demands that the defendant make a true-false statement, and not merely that he unlock a device or produce documents. Such an order therefore compels full-fledged testimony under the Fifth Amendment with no exception for the foregone conclusion doctrine.

The Fifth District also correctly held that when the State attempts to compel such full-fledged testimony from a defendant, the foregone conclusion exception articulated for tax records in *Fisher v. United States*, 425 U.S. 391 (1976), does not apply. This case differs from an order compelling a person to *unlock* her device—where the foregone conclusion doctrine at least arguably applies to the testimony implicit in unlocking a device. By contrast, this case

involves compulsion of an actual oral or written statement—and not implicit testimony—to which the foregone conclusion doctrine cannot ever apply. Compulsion of an actual statement, unlike compulsion to open a device, bears no resemblance to the act-of-production cases that gave rise to the foregone conclusion exception in the first place. As the court below wrote, "[t]o compel a defendant … to disclose the passcode to his smartphone under this exception would … sound 'the death knell for a constitutional protection against compelled self-incrimination in the digital age.'" *State v. Garcia*, 302 So. 3d 1051, 1057 (Fla. 5th DCA 2020).

Amici agree with the thorough description of the law in Respondent's brief and in the briefs of the American Civil Liberties Union, the National Association of Criminal Defense Lawyers, and the other Amici, and will not repeat that discussion here. Amici submit that the decision of the Fifth District is correct, and that *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016), was wrongly decided.

ARGUMENT

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

In password cases, a court must distinguish two distinct scenarios. In the first scenario, the court orders a person to disclose his password so that law enforcement can open the device. As further elaborated below, this scenario compels ordinary, full-fledged testimony, enjoying the broadest protection of the Fifth Amendment.

In the second scenario, the court orders a person to *open* her device in a way that no one learns the password. In this scenario, the order to unlock the device compels *implicit* testimony and would arguably trigger the act of production doctrine and application of the foregone conclusion exception.

This case involves the first scenario.

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." *Doe v. United States*, 487 U.S. 201, 210 (1988); *United States v. Hubbell*, 530 U.S. 27, 34 (2000); *Fisher v. United States*, 425 U.S. 391 (1976); Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted*

Devices, 87 Fordham L. Rev. 203, 226 (2018) (hereinafter *Sacharoff I*).

At its core, the Fifth Amendment protects against compelling a true-false verbal statement (i.e. "my password is 1234") in part because of the underlying purposes of the Fifth Amendment. "Historically, the privilege was intended to prevent the use of legal compulsion to extract from the accused a sworn communication of facts which would incriminate him. Such was the process of the ecclesiastical courts and the Star Chamber ...." *Pennsylvania v. Muniz*, 496 U.S. 582, 595–96 (1990). "At its core," the privilege against self-incrimination "reflects our fierce unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt … wherein suspects were forced to choose between revealing incriminating private thoughts and forsaking their oath by committing perjury." *Id.* at 596.

The cruel trilemma posits that in the absence of Fifth Amendment protections, a defendant compelled to provide information is forced into an untenable position: (1) tell the truth and thereby help the State convict him, (2) lie and thereby commit perjury, or (3) remain silent and thereby suffer possible contempt and

jail. *Id.* The Fifth Amendment right to remain silent removes that oppressive coercion in relation to criminal cases. *Sacharoff I*, 87 Fordham L. Rev. at 224, 227. The cruel trilemma rests upon the assumption that the government has compelled a true-false verbal statement from the defendant. In this case, the trial court compelled a true-false statement from Mr. Garcia, who could have disclosed a true password (incrimination), a false one (perjury), or none at all (contempt).

Nearly all compelled true-false verbal statements, including the statement sought from Mr. Garcia in this case, fall under this category of full-fledged testimony that enjoys absolute Fifth Amendment protection and cannot be defeated by the foregone conclusion exception. As the United States Supreme Court said in *Muniz*, "[t]he vast majority of verbal statements … will be testimonial" because "[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts." 496 U.S. at 597. Thus, "[w]henever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or

silence, and hence the response (whether based on truth or falsity) contains a testimonial component." *Id.*

The only exception, not relevant here, are statements compelled not for their truth but to see the *manner* in which the person makes the statement. For example, does she slur her speech? But here the State seeks to compel the true-false statement from Mr. Garcia for its content.

A. Ordering Mr. Garcia to disclose his password compels full-fledged testimony in violation of the Fifth Amendment.

The State seeks the content of the password to obtain incriminating information against Mr. Garcia in two distinct ways. First, the State wants the court to order Mr. Garcia to state the password, or write it down, so that law enforcement can unlock the device and look for evidence that Mr. Garcia stalked the complainant. *Garcia*, 302 So. 3d at 1053; Petitioner's App'x at 3-5, 9-11. The State seeks data on the smartphone to link the phone to the GPS tracker found on the complainant's car. *Id.*

Second, the State has also charged Mr. Garcia with using his phone as a "missile" or deadly weapon by throwing it at the window of a home where the complainant was staying. Petitioner's App'x at

3-4, 14. The phone was recovered at the scene, near the broken glass. *Id.* at 3-5, 9-11. If Mr. Garcia supplies the password and the password unlocks the phone, Mr. Garcia has supplied evidence that the phone is likely his, thus incriminating himself and raising the inference that he is likely the person who threw the phone at the window.

These two distinct means of potential incrimination demand that the Fifth Amendment protect Mr. Garcia against compelled disclosure of the password.

1. Disclosure of the password is incriminating because it could form a link in the chain to obtain incriminating evidence from the phone.

The privilege against self-incrimination extends not only "to answers that would in themselves support a conviction … but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a … crime." *Hoffman*, 341 U.S. at 486; *Garcia*, 302 So. 3d at 1054; *see also Hubbell*, 530 U.S. at 37 ("It has, however, long been settled that [the Fifth Amendment's] protection encompasses compelled statements that lead to the discovery of incriminating evidence even though the

statements themselves are not incriminating and are not introduced into evidence").

In this case, the State wants the password to link Mr. Garcia to the "storage of evident[i]ary data pertaining to Aggravated Stalking" contained in the smartphone. IB:5. The State intends to use that data to link Mr. Garcia to the GPS tracking device found on the complainant's car. In providing the password, Mr. Garcia would communicate several incriminating facts. First, he would communicate the *content* of the password, allowing the State to unlock the phone and find the supposed incriminating evidence. The password content would provide a direct link to possibly incriminating evidence. Second, Mr. Garcia would communicate that the password works and that the phone, and the files and data on it, are likely his. Thus, disclosure of the passcode will give the State the alleged incriminating evidence *and* will link that evidence to Mr. Garcia. Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 Texas L. Rev. Online 63, 69 (2019) (hereinafter *Sacharoff II*) (describing how knowledge of a

password to a device communicates ownership or control of the device and its contents).[2]

2. Disclosure of the password is incriminating because of the "missile" charge in Count 1 of the Information.

In addition to the stalking charges, Count 1 of the Information charges Mr. Garcia with using the smartphone as a deadly missile by throwing it at the window. *Garcia*, 305 So. 3d at 1053. No one saw Mr. Garcia throw the phone nor was he arrested at the scene. The phone was not seized from Mr. Garcia's person nor among his belongings—instead, it was recovered at the scene, on the floor by the broken window. *Id.* Mr. Garcia has invoked his right to remain silent and has not admitted that he owns the phone. IB:56-57.

Compelling Mr. Garcia to reveal the password to the phone links Mr. Garcia directly to the scene of the crime and to the "missile" or

[2] When a defendant discloses his password to police, the defendant likely is also disclosing his password to other innocent devices, as well as to many of his online apps and accounts including social media, bank, and email accounts. The password thus provides law enforcement with information they can use to access other portions of the defendant's life. *Sacharoff I*, 87 Fordham L. Rev. at 224. A true password can therefore form a "link in the chain" to other incriminating evidence as well. *Hoffman v. United States*, 341 U.S. 479, 486 (1951).

the instrumentality of the crime charged in Count 1. If Mr. Garcia provides a password that unlocks the phone, the State could argue that the phone belongs to him and that Mr. Garcia is likely the person who threw it at the window. Compelled disclosure of the password would be incriminating testimony in its full-fledged form for which the Fifth Amendment provides absolute protection.

3. Disclosure of the password is not merely an "administrative" or "neutral act . . . with no value or significance."

The State contends that by disclosing the password, Mr. Garcia "*at most* communicates that he knows the passcode," which, in the State's view, is an "administrative" or "neutral act … with no value or significance." IB:28, 33 (emphasis added). This argument is wrong.

First, in disclosing the password, Mr. Garcia would reveal not only that he knows the password, but he would also reveal the *content* of the password. And it is precisely the content of the password that the State seeks in order to open the device and search for data linking the phone to the GPS tracker found on the complainant's car. Indeed, in its motion in the trial court to compel Mr. Garcia to disclose the password, the State admitted that "the

contents of the defendant's phone are relevant to how the events occurred and whether the defendant is guilty." Petitioner's App'x at 17:¶14.

Second, if Mr. Garcia provides the password that unlocks the phone, that fact *also* shows that the phone is likely his and that he is likely the person who placed the GPS tracker on the complainant's car.

Third, with respect to Count 1 charging Mr. Garcia with using the phone as a "missile," revealing a password would link Mr. Garcia directly to the instrumentality of the crime *and* to the scene itself, since the phone was recovered there.

All these facts would constitute strong evidence against Mr. Garcia, far from testimony that is "neutral" or "with no value or significance," as the State argues.

B. The right against self-incrimination does not yield to the State's desire for "unencumbered access" to evidence.

The State proposes that compelling Mr. Garcia to provide a password is not a testimonial act because "the State could care less what Respondent's passcode is, so long as police obtain

unencumbered access to the phone … This case, in other words, is about access, not testimony." IB:26-27.

To say that this case "is about access, not testimony" is also wrong. This case is about *testimony in order to obtain access*. If the State could gain access to the device without Mr. Garcia's testimony, the State would have done so already. If we are going to compare like to like, under the State's proposed interpretation of the right against self-incrimination, the State would be permitted to compel *testimony* from a defendant to answer "in which drawer is the gun?," on the theory that the State could not care less about the drawer as long as the State has "unencumbered *access*" to the gun. But of course revealing the drawer where the gun is stored does not reveal just the drawer, it also reveals the gun itself and links the defendant to the gun, to the crime under investigation, and perhaps to other offenses as well.

In saying that it does not care about the password, the State really means that once it has used the password to obtain the incriminating evidence, the State no longer has use for the password. But this argument ignores *Hoffman* and *Hubbell*, which make clear that Fifth Amendment protection is not limited only to testimony that

the State seeks to use at trial. The Fifth Amendment also protects testimony that is a lead or a step that the State can use to obtain incriminating evidence for use at trial. *Hoffman,* 341 U.S. at 487; *Hubbell,* 530 U.S. at 38.

Regardless of how much (or how little) the State cares about the password, the Fifth Amendment protects the defendant if *he* reasonably perceives that his compelled testimony will lead to incriminating evidence. As the Court said in *Hoffman*, "To sustain the privilege, it need only be evident from the implications of the question, in the setting in which it is asked, that a responsive answer to the question or an explanation of why it cannot be answered might be dangerous because injurious disclosure could result. The trial judge in appraising the claim 'must be governed as much by his personal perception of the peculiarities of the case as by the facts actually in evidence.'" 341 U.S. at 486–87.

As an alternative to compelling oral testimony, the State suggests that it could compel Mr. Garcia to write down the password and hand over that piece of paper to the State. IB:27 But such compulsion to create a new (i.e. not pre-existing) document with fresh

information is equivalent to compelled, full-fledged testimony and all the arguments above apply equally.

As a second alternative, the State argues that it could compel Mr. Garcia to enter the password directly on the phone to open the device. This alternative presents an entirely different scenario not before the Court. The certified questions before the Court involve the disclosure of a password rather than the compelled entry of a password to open a device. In *Sacharoff I* and *Sacharoff II*, Professor Sacharoff provides an extensive discussion of these issues and shows that the State cannot compel an individual to open a device unless the State can show that it knows with reasonable particularity that the particular files or data it seeks are on the device.

Finally, the State is not without methods to obtain the password and the access it seeks—the State retains the power to grant Mr. Garcia immunity. *See Hoffman*, 341 U.S. at 490; *Kastigar v. United States*, 406 U.S. 441 (1972). The State can choose not to confer immunity, which would suggest that disclosure of the password *does* have testimonial and incriminating significance. Either way, if the State chooses not to confer immunity, the tension between the right to remain silent and the State's desire for "unencumbered access"

resolves in favor of the accused. As this Court held in *State v. Horwitz*, the right to remain silent "curtail[s] and restrain[s] the power of the State. It is more important to preserve [it], even though at times a guilty man may go free, than it is to obtain a conviction by ignoring or violating [it]. The end does not justify the means. Might is not always right." 191 So. 3d 429, 438 (2016).

II. WHEN THE STATE SEEKS DISCLOSURE OF A PASSWORD, THE STATE IS SEEKING FULL-FLEDGED TESTIMONY AND THE FOREGONE CONCLUSION DOCTRINE IS IRRELEVANT.

The foregone conclusion doctrine arguably applies to an order to *open* a device, but it never applies to an order to *disclose* a password. There is a core distinction between information that a person knows in her mind and pre-existing documents or files that a person possesses. The Fifth District correctly held that *Fisher* and the entire act-of-production / foregone conclusion scaffolding apply only when the State seeks to compel production of pre-existing documents, not when the State seeks to compel testimony of what a person knows. Indeed, the Fifth District recognized the reasoning of *Fisher* that

> although compelling a taxpayer to comply with a subpoena to produce an accountant's work papers in the taxpayer's possession would undoubtedly involve

> substantial compulsion, the Fifth Amendment was not implicated because the subpoena does not compel oral testimony, nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought.

Garcia, 302 So. 3d at 1056 (citing *Fisher*, 425 U.S. at 409) (emphasis added). Thus, under *Fisher*, the State can compel the production of pre-existing documents only if it meets the requirements of the foregone conclusion exception. *Garcia*, 302 So. 3d at 1055-56; *Fisher*, 45 U.S. at 411.

But neither *Fisher* nor any other United States Supreme Court case authorize the State to compel a person to create the contents of a new document for production to the State. Nor do those cases remotely hint that the foregone conclusion doctrine applies to compel a person to disclose information such as a password, either orally or by writing it down and then "producing" it to the State. Such compulsion would compel testimony in the pure sense and would be banned by the Fifth Amendment.

The limits to *Fisher* apply with full force here. Because the trial court compelled Mr. Garcia to recollect and disclose a passcode that may unlock the phone, the order compels pure incriminating

testimony and neither the act-of-production cases nor their foregone conclusion exception apply.

To extend the foregone conclusion exception to compelled disclosures of information would eviscerate the Fifth Amendment, since the exception could then apply in even the most mundane cases. For example, if the police see, smell, and videotape a suspect smoking methamphetamine, the police obviously know and can prove that the suspect possessed methamphetamine. But the State cannot compel the suspect to answer questions about the methamphetamine, even if his possession of methamphetamine is a foregone conclusion.

Under the State's proposed application of the foregone conclusion exception, however, the State *could* compel the suspect to confess to methamphetamine possession. After all, the State already knows, and can show with particularity (the video), that the suspect possessed methamphetamine. The suspect's confession would "add little or nothing" to the State's overall information, as his possession of methamphetamine is already a foregone conclusion. But no court would countenance such coercion.

The foregone conclusion doctrine was crafted for a vastly different context involving the act of producing pre-existing business documents, not compelling testimony. The Fifth District is correct that "it would be imprudent to extend the foregone conclusion exception beyond its application as described in *Fisher*. To compel a defendant, such as Garcia, to disclose the passcode to his smartphone under this exception would, in our view, sounds the death knell for a constitutional protection against compelled self-incrimination in the digital age." *Garcia*, 302 So. 3d at 1057.

Finally, the State cites to Professor Orin Kerr multiple times, correctly referring to him as a leading scholar. IB:1,2,3,29,42,47,49. The Court should know that Professor Kerr does not support the State's argument that the foregone conclusion doctrine applies when the State seeks to compel an individual to disclose a password. In an Opinion piece in The Washington Post, Professor Kerr stated that the foregone conclusion exception does not apply to testimony:

> Jonathan Mayer has persuaded me that the . . . foregone conclusion doctrine doesn't apply . . . Jonathan argues that . . . the foregone conclusion doctrine can't apply because the government isn't asking the defendants to produce anything. The doctrine only applies to acts of production. But the government has sought an order here that the defendants have to *say* something, not turn

> something over. Because the foregone conclusion doctrine only applies to the acts of production, not direct testimony, it can't apply …
>
> After thinking it over, I tend to think that's right. The doctrine applies only to acts, not direct testimony. So now I agree with Jonathan on this point: When the government seeks disclosure of a password, the government is seeking a testimonial statement and the foregone conclusion doctrine isn't relevant.

Orin Kerr, *Opinion: A revised approach to the Fifth Amendment and obtaining passcodes*, http://tinyurl.com/3ksns87u (last visited 6-20-21) (italics in original; underline added); *see also Sacharoff I,* 87 Fordham L. Rev. at 223-24 (discussing how most scholars and many courts agree that compelling oral disclosure of a passcode enjoys full Fifth Amendment protection).[3]

III. IF APPLYING THE FOREGONE CONCLUSION DOCTRINE TO DISCLOSURE OF A PASSWORD, THE OBJECT OF THE FOREGONE CONCLUSION SHOULD BE THE FILES AND DATA ON THE PHONE, NOT JUST THE PASSWORD.

If the Court concludes that the foregone conclusion doctrine applies, the object of the foregone conclusion should be *the*

[3] Although Professor Kerr questioned whether stating a password would be incriminating in every case, that question is not relevant here because the State admitted, in its motion in the trial court, that it sought to compel Mr. Garcia to provide the password because "the contents of the defendant's phone are relevant to … whether the defendant is guilty." Petitioner's App'x at 17:¶14.

underlying data or files the State seeks, not the password to the device. That is, the State should be required to show with reasonable particularity that it already knows that the files it seeks are on the device. The soundness of this rule can be illustrated with the act of production in the physical world.

When handing over documents in the physical world in response to a subpoena, the foregone conclusion doctrine does not apply solely to that physical act; rather, the doctrine applies to *the underlying papers* that the defendant produces because the act of producing the documents implicitly communicates information about the documents: their existence, who possesses them, and their authenticity. *Fisher*, 425 U.S. at 410; *Sacharoff I*, 87 Fordham L. Rev. at 217-18. In the physical world, the court asks whether it is a foregone conclusion that *the underlying papers* exist and are in the defendant's possession, not whether it is a foregone conclusion that the defendant is physically capable of producing the documents. *Sacharoff I*, 87 Fordham L. Rev. at 237.

In the virtual world, the password produces *the underlying data or files* on the device. The Court must therefore ask whether it is a foregone conclusion that *the underlying data or files* exist on the

device. "It is not the verbal recitation of a passcode but rather the documents, electronic or otherwise, hidden by an electronic wall, that are the focus of this exception." *G.A.Q.L. v. State* , 257 So. 3d 1058, 1064 (Fla. 4th DCA 2018); *accord State v. Pollard*, 287 So. 3d 649, 657 (Fla. 1st DCA 2019) ("It is not enough for the state to infer that evidence exists—it must identify what evidence lies beyond the passcode wall with reasonable particularity").

Applying the foregone conclusion exception only to knowledge of the password would lead to drastic intrusions on individual privacy. The Fourth District recognized this when it held that unless the foregone conclusion doctrine applies *to the underlying data* and not just the password, "every password-protected phone would be subject to compelled unlocking since it would be a foregone conclusion that any password-protected phone would have a passcode. That interpretation is wrong and contravenes the protections of the Fifth Amendment." *G.A.Q.L*, 257 So. 3d at 1063.

If the Court concludes that the forgone conclusion exception should be extended to passwords, the Court can adopt the test announced by the United States Court of Appeals for the Eleventh Circuit and adopted by the Fourth District: The State must identify

with particularity the file name of the records it seeks on the device. If the file name is unknown, the State must show with some reasonable particularity "that it seeks a certain file and is aware, based on other information, 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." *In re Grand Jury Subpoena*, 670 F.3d 1335, 1347 n.28 (11th Cir. 2012); *G.A.Q.L.*, 257 So. 3d at 1063.

CONCLUSION

The decision of the Fifth District Court of Appeal is correct. The trial court's order compelling Mr. Garcia to disclose the password to the smartphone violates the Fifth Amendment. This Court has a longstanding record of providing great deference to the privilege against self-incrimination, under the Fifth Amendment and under the Florida Constitution. *Horwitz*, 191 So.3d at 439; *Ex Parte Senior*, 37 Fla. 1, 16 (1896). The Court should affirm the decision below.

Dated: June 24, 2021

Respectfully submitted,

/s/ Diana L. Johnson
DIANA L. JOHNSON
Florida Bar No. 35949
CHAIR, FACDL AMICUS COMMITTEE
407 N. Laura Street
Jacksonville, Florida 32202
(904) 255-4721
djohnson@pd4.coj.net

/s/ Jackie Perczek
JACKIE PERCZEK
Florida Bar No. 0042201
JEANELLE GOMEZ
Florida Bar No. 1026021
BLACK SREBNICK
201 S. Biscayne Boulevard
Suite 1300
Miami, FL 33131
(305) 371-6421
JPerczek@RoyBlack.com

CERTIFICATE OF SERVICE

I certify that on June 24, 2021, a true and correct copy of this brief was filed with the Clerk of Court using the Florida Courts E-Filing Portal and served via E-Service to counsel of record.

CERTIFICATE OF COMPLIANCE

I certify that this brief was prepared in 14-point Bookman font and complies with the word-count and content requirements of Rules 9.210 and 9.370.

/s/ Jackie Perczek
Jackie Perczek