SC20-1419

In the Supreme Court of Florida

STATE OF FLORIDA,
Petitioner,

v.

JOHNATHAN DAVID GARCIA,
Respondent.

On Petition for Discretionary Review from the
Fifth District Court of Appeal
DCA No. 5D19-590

INITIAL BRIEF ON THE MERITS

ASHLEY MOODY
Attorney General

Office of the Attorney General
The Capitol, PL-01
Tallahassee, Florida 32399
(850) 414-3300
amit.agarwal@myfloridalegal.com
jeffrey.desousa@myfloridalegal.com
christopher.baum@myfloridalegal.com
jason.hilborn@myfloridalegal.com

AMIT AGARWAL (FBN125637)
Solicitor General
JEFFREY PAUL DESOUSA (FBN110951)
Chief Deputy Solicitor General
CHRISTOPHER J. BAUM (FBN1007882)
Senior Deputy Solicitor General
JASON H. HILBORN (FBN1008829)
Assistant Solicitor General

Counsel for Petitioner

March 12, 2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Constitutional Provisions

Other Authorities

STATEMENT OF THE ISSUES

I. Whether the trial court's order compelling Respondent to grant the State access to his phone by revealing the passcode caused irreparable harm that could not be remedied on appeal, so that the district court had jurisdiction to issue a writ of certiorari.

II. Whether, assuming the district court had jurisdiction, it erred in concluding that compelled disclosure of the passcode violated the Self-Incrimination Clause of the Fifth Amendment.

STATEMENT OF THE CASE AND FACTS

1. As cellphones have become increasingly ubiquitous in modern life, the issues in this case have come to the fore. "Ninety-four percent of Americans aged eighteen to twenty-nine carry smartphones, many of which encrypt their data by default when not in use."[1] These devices—which are as much computers as they are phones—not only facilitate communication but allow the user to store videos, photos, audio, notes, and documents; to conduct commercial and banking transactions; to browse the web; and to share data.

This shift in everyday living has had a corresponding effect on

[1] Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 768 (2019).

the way people commit crime: Where once the proof and instrumentalities of criminal activity existed largely in physical form, evidence and contraband now can be found in digital-storage devices, including cellphones. For example, ledgers recording drug transactions or money laundering—previously kept on paper and stored in safes or lockboxes—are routinely stored on passcode-protected digital devices.[2] And contraband like child pornography may be entirely digital.[3]

Digital encryption is a convenient way for cellphone users to prevent theft and other intrusions. The most common forms of encryption automatically encrypt a device when it is turned off or is inactive.[4] To unlock the device, the user is prompted to input a passcode, which "serve[s] the function of [a] key[.]"[5] Some devices may also be unlocked with the use of biometric-identification

---

[2] *See* "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," U.S. DOJ, at ix (3d ed. 2009), tinyurl.com/j2ejebew.

[3] *See id.* at 5–19 (compiling examples in case law).

[4] *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L. J. 989, 990 (2018); *see generally* Daniel Garrie & Rick Borden, Encryption for Lawyers, 2016 Bus. L. Today 1–3 (June 2016).

[5] *See* Kerr & Schneier, *supra*, at 993–95.

software that recognizes fingerprints or faces,[6] although biometrics may be unavailable in a range of circumstances.[7]

Encryption presents a problem for law enforcement. The U.S. Department of Justice recently remarked on "the phenomenon of 'warrant-proof' encryption" that has resulted as "[s]ervice providers, device manufacturers, and application developers . . . deploy[] products and services with encryption that can only be decrypted by the end user or customer."[8] Encryption techniques have become so sophisticated that locked cellphones are "all but 'unbreakable,'"[9] because in "the arms race between encryption and [decryption], the mathematics overwhelmingly favors encryption."[10]

With this advent of warrant-proof encryption, police "often cannot obtain the electronic evidence and intelligence necessary to

---

[6] *See State v. Pittman*, 479 P.3d 1028, 1034 (Or. 2021).

[7] *See, e.g.*, *State v. Andrews*, 234 A.3d at 1252 (N.J. 2020) (noting that "in some cases, a biometric lock can be established only after a passcode is created"); "Apple Platform Security," Apple (last visited Mar. 12, 2021), tinyurl.com/254sfhxm (explaining that Apple iPhone's touch ID feature is unavailable if the phone has just been turned on or restarted, if the user has not unlocked the phone within the last 48 hours, after a software update, etc.).

[8] *Lawful Access*, U.S. DOJ (last updated Oct. 30, 2020), https://www.justice.gov/olp/lawful-access.

[9] *Riley v. California*, 573 U.S. 373, 389 (2014).

[10] Kerr & Schneier, *supra*, at 994.

investigate and prosecute threats to public safety and national security, even with a warrant or court order."[11]

2. The State has charged Respondent, Johnathan Garcia, with five counts: one count of throwing a deadly missile into a building; two counts of aggravated stalking with a credible threat; and two counts of criminal mischief. App'x 14–16. Respondent has a "history of documented dating violence," including a "prior case of stalking filed with the State Attorney's Office." *Id.* at 4. According to a sworn probable-cause affidavit,[12] the victim told police that Respondent's behavior after their 9-year relationship ended made her fear for her safety. *Id.* His conduct was such that the victim's then-boyfriend, Terrell, bought a firearm for protection. *Id.*

Prompting the incident that led to this case, Respondent followed the victim to a bakery where she was meeting Terrell. *Id.* Two days later, someone broke a glass window at Terrell's home at night while the victim was present. *Id.* The victim then heard a vehicle "similar to [Respondent's] leaving the scene." *Id.*

---

[11] *Lawful Access*, U.S. DOJ, *supra*.

[12] In the trial court, Respondent neither disputed the facts set out in this affidavit nor requested an evidentiary hearing to present contrary evidence.

When police responded, they found a black Samsung Galaxy Note8 cellphone near the broken window. *Id*. The victim "identified the black Samsung as belonging to [Respondent]." *Id*. To confirm that it was his, police asked the victim to call the phone number she had saved as Respondent's. *Id*. When she did, the "Samsung began to ring and the contact on the home screen read [the victim's name], with [the victim's] phone number displayed." *Id*. A sworn arrest affidavit lists Respondent's phone number as the same number that the victim dialed that night. *Compare id*. at 4, with *id*. at 8.

About a month later, police responded to Terrell's home again because the victim had discovered a "GPS tracker" on her car. *Id*. at 10. The State obtained a search warrant based in part on the GPS tracker's ability to "be tracked by electronic applications i.e. cell phones." *Id*. This fact, along with the incident on the night the phone was found, created "proba[b]le cause to believe the [phone] contains storage of evident[i]ary data pertaining to Aggravated Stalking." *Id*.

The State tried "a forensic download of the phone" but failed because the phone "requires either a passcode or the Defendant's fingerprint." *Id*. at 17. It therefore moved to compel Respondent "to

provide a passcode and/or his fingerprint to unlock his mobile phone." *Id*. In that motion, the State averred that "the Defendant's mobile phone was located on scene and collected as evidence," that the State was "unable to unlock the Defendant's phone," and that "[t]he contents of the Defendant's phone are relevant." *Id*. Respondent "object[ed] to the granting of th[e] motion," *id*., but did not dispute that the State could show those three facts.

In ruling on the motion, the circuit court analyzed whether the Fifth Amendment's Self-Incrimination Clause protected Respondent from disclosing his passcode. By way of background, this analysis involves determining whether disclosing a passcode is compelled, testimonial, and incriminating, which in turn implicates two inquiries: the act-of-production exception and the foregone-conclusion doctrine. In assessing the act-of-production exception, a court looks to what information the defendant conveys to the State by performing the act of producing whatever the State seeks to compel. In turn, in assessing the foregone-conclusion doctrine, the court asks whether the State already knows that information. If it does, the Self-Incrimination Clause does not prevent the State from

compelling the act of production at issue.

At the time of the motion-to-compel hearing, the Fourth District in *G.A.Q.L. v. State*, 257 So. 3d 1058 (Fla. 4th DCA 2018), had split with the Second District's decision in *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016), over how to apply the act-of-production exception and foregone-conclusion doctrine to the compelled production of digital devices.[13] The Second District in *Stahl* held that the Self-Incrimination Clause does not prevent the State from requiring a defendant to provide the State access to an encrypted device because doing so is not "testimonial" and is thus outside the Self-Incrimination Clause's reach. 206 So. 3d at 134–35. And even if it were testimonial, the Second District held that disclosing a passcode conveys only that the defendant knows the passcode, which is all the State must show to meet the foregone-conclusion doctrine. *Id*. at 135–36. By contrast, in *G.A.Q.L.*, the Fourth District held that disclosing a passcode is testimonial and that the State must show not only that it already knows that the defendant knows the

[13] The First District later sided with the Fourth District. *See Varn v. State*, No. 1D19-1967, 2020 WL 5244807 (Fla. 1st DCA Sept. 3, 2020); *Pollard v. State*, 287 So. 3d 649, 651 (Fla. 1st DCA 2019).

passcode, but also that it knows the contents on the phone to which the passcode grants access. 257 So. 2d at 1061–65.

At the motion-to-compel hearing here, the State explained that it had "filed a motion to compel the Defendant's phone passcode" and that the State "ha[d] the Defendant's cellphone in custody, in evidence." App'x 22. Respondent did not assert that the phone or passcode was not his. He instead argued that, under *G.A.Q.L.*, "compelling the Defendant . . . to disclose or provide his password would be testimonial and would be in violation of the Fifth Amendment." *Id.* at 23–24. The circuit court disagreed, electing to follow *Stahl*, and "direct[ed] that [Respondent] turn over his passcodes." *Id.* at 24–25.

3. Before trial, Respondent petitioned the Fifth District for a writ of certiorari under Florida Rule of Appellate Procedure 9.030(b)(3), challenging the trial court's order granting the State's motion to compel. Citing *G.A.Q.L.*, the Fifth District issued the writ of certiorari and quashed the order. App'x 38, 40.

The Fifth District held that Respondent's disclosing his passcode would be testimonial. *Id.* at 36. And it reasoned that "it

would be imprudent to extend the foregone conclusion exception" from documents to passcodes because of the risk to defendants' protections against self-incrimination posed by the "digital age." *Id.* at 39. "[O]ther than in those limited circumstances when a defendant's ownership of the smartphone was in question, it would necessarily be a 'foregone conclusion' that a defendant . . . would have knowledge of or have otherwise memorized his or her passcode." *Id.* Thus, the court determined that compelling Respondent to disclose his passcode would "contravene the protections afforded by the Fifth Amendment." *Id.*

The Fifth District certified two questions of great public importance:

First, may a defendant be compelled to disclose orally the memorized passcode to his or her smartphone over the invocation of privilege under the Fifth Amendment to the United States Constitution?

Second, if orally providing the passcode to a passcode-protected smartphone is a "testimonial communication" protected under the Fifth Amendment, can the disclosure of the passcode nevertheless be

compelled under the foregone conclusion exception or doctrine when there is no dispute that the defendant is the owner of the passcode-protected phone? App'x 40.

This Court accepted jurisdiction.[14]

SUMMARY OF ARGUMENT

I. Modern encryption now gives criminals the tools to hide the evidence and instrumentalities of their offenses from law enforcement—even when police have a valid warrant. The trial court's order granting the State access to that evidence here does not cause Respondent irreparable harm that cannot be remedied on appeal. *First*, no Fifth Amendment violation occurs until the State introduces evidence obtained in violation of the Fifth Amendment at trial, which has not occurred yet here. Even if a Fifth Amendment violation occurs earlier, the possibility of obtaining reversal and a suppression order shows that any harm is not irreparable. *Second*, the district court's resort to civil cases finding irreparable harm was misplaced. The district court therefore lacked jurisdiction to issue a writ of

[14] Facts like those here have also prompted the same Fifth Amendment issue in two "tag" cases before this Court. *See Varn v. State*, SC20-1383; *State v. Hager*, SC20-1421. The State seeks to compel access to a password-protected phone in both cases.

certiorari.

II. A. On the merits, the Fifth Amendment does not prevent the State from compelling Respondent to provide access to his phone. Disclosing a passcode is not testimonial. That act—like unlocking a front door—merely grants access. After the door is opened, the State must then conduct its own search under a valid search warrant constricting what and where the State may search. The passcode itself has no value or significance and does not speak to Respondent's guilt—it merely grants access.

B. Even if granting access to Respondent's phone were testimonial, the foregone-conclusion doctrine allows the State to compel Respondent to do so. Providing his passcode tells the State one thing: That Respondent knows the passcode and thus controls the phone on some level. If the State already knows that—as it does here—the act of production is unprotected.

Any holding to the contrary would prove disastrous to law enforcement. For centuries, and particularly at the time of the Framing, so long as the State had a valid search warrant it could access evidence in homes or lockboxes—the "king's keys" opened all

doors. But technological advancements have changed that reality. Modern encryption has shifted the balance between criminals and law enforcement in favor of crime by allowing criminals to hide evidence in areas the State physically cannot access. The Fifth Amendment should not be interpreted to now allow criminals to use it as a shield in ways never understood by the Framers.

The State must show that it already knows that Respondent has control or possession of the phone by a preponderance of the evidence. It has done so. And Respondent has never affirmatively argued that the phone is not his nor has he ever requested an evidentiary hearing to prove otherwise. Under the foregone-conclusion doctrine, then, the Fifth Amendment Self-Incrimination Clause does not prevent the State's compelling Respondent to grant access to his phone by producing his passcode.

STANDARD OF REVIEW

This Court reviews questions of law de novo. *See Kopel v. Kopel*, 229 So. 3d 812, 815 (Fla. 2017). And it reviews "[m]ixed questions of law and fact that ultimately determine constitutional rights . . . using a two-step approach, deferring to the trial court on questions of historical fact but conducting a de novo review of the constitutional issue." *City of Fort Lauderdale v. Dhar*, 185 So. 3d 1232, 1234 (Fla. 2016).

ARGUMENT

I. THE DISTRICT COURT LACKED JURISDICTION TO GRANT CERTIORARI BECAUSE RESPONDENT HAS NOT SUFFERED IRREPARABLE HARM.

At the outset, the district court lacked jurisdiction because Respondent did not face any risk of irreparable harm, an indispensable element of certiorari. District courts of appeal have discretionary jurisdiction to issue writs of certiorari. Art. V, § 4(b)(3), Fla. Const. Certiorari review, though, "is an extraordinary remedy," *Jaye v. Royal Saxon, Inc.*, 720 So. 2d 214, 214 (Fla. 1998), that "should not be used to circumvent the interlocutory appeal rule" permitting appeals from only select non-final orders. *Id.* at 214–15. That is because "[p]iecemeal review of nonfinal trial court orders . . .

impede[s] the orderly administration of justice." *Id.* at 215. So "before certiorari can be used to review non-final orders, the appellate court must focus on the threshold jurisdictional question: whether there is a material injury that cannot be corrected on appeal, otherwise termed as irreparable harm." *Citizens Prop. Ins. Corp. v. San Perdido Ass'n, Inc.*, 104 So. 3d 344, 351 (Fla. 2012).

Respondent argued below that unlocking his phone would irreparably harm him because doing so would (1) "violat[e] his Fifth Amendment right" against self incrimination, which (2) would then "be compounded by whatever evidence the State acquires." Am'd Pet. for Writ of Cert., No. 5D19-590, at *7 (Mar. 7, 2019). These injuries, Respondent asserted, have "no adequate remedy on direct appeal." *Id*.

But as the U.S. Supreme Court has explained, a Self-Incrimination Clause violation does not occur until trial, so requiring him to grant access to his phone before trial would cause no Fifth Amendment injury at all. And the district court's theory of irreparable harm was likewise unavailing.

A. A self-incrimination violation occurs, if at all, only at trial.

Respondent's theory of irreparable harm was that his rights against self-incrimination were about to be violated, and that the fruits of that violation would compound the injury. He is incorrect. As reflected in U.S. Supreme Court precedent, the Fifth Amendment's text, and its historical purpose, the Self-Incrimination Clause is limited to preventing the State from using compelled statements to convict or punish defendants. Because generally it is only *at trial* when defendants face conviction or punishment, the Self-Incrimination Clause is a "trial right." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990). And, at a minimum, any pretrial violation of the Fifth Amendment is not irreparable.

1. a. To begin with, the U.S. Supreme Court has consistently referred to the Self-Incrimination Clause as a "trial right," *Withrow v. Williams*, 507 U.S. 680, 692 (1993), that protects a defendant from "stand[ing] as a witness against himself," *Brady v. United States*, 397 U.S. 742, 748 (1970).

That theme permeates the Court's decisions. "[T]he core protection afforded by the Self-Incrimination Clause," the Court has

said, "is a prohibition on compelling a criminal defendant to testify against himself *at trial*." *United States v. Patane*, 542 U.S. 630, 637 (2004) (plurality op.) (emphasis added). "Although conduct by law enforcement officials prior to trial may ultimately impair that right, a constitutional violation occurs only *at trial*." *Verdugo-Urquidez*, 494 U.S. at 264 (emphasis added); *see also Chavez v. Martinez*, 538 U.S. 760, 767 (2003) (plurality op.) ("Statements compelled by police interrogations of course may not be used against a defendant *at trial*." (emphasis added)). As a result, if the State "acquire[s] incriminating evidence in violation of the Fifth Amendment," the defendant is "at most . . . entitled to suppress the evidence and its fruit if they [a]re sought to be used against him *at trial*." *United States v. Blue*, 384 U.S. 251, 255 (1966) (emphasis added).[15]

Given those precedents, several federal appellate courts have declined to recognize self-incrimination violations before trial, *see*,

[15] The U.S. Supreme Court has even blessed using compelled testimony in pretrial proceedings. In *Estelle v. Smith*, the Court went out of its way to explain that "no Fifth Amendment issue would have arisen" if the statements in that case "had been confined to" "a routine competency" proceeding "to ensur[e] that respondent understood the charges against him and was capable of assisting in his defense." 451 U.S. 454, 465 (1981).

e.g., *Renda v. King*, 347 F.3d 550, 552 (3d Cir. 2003); *Burrell v. Virginia*, 395 F.3d 508, 514 (4th Cir. 2005); *Murray v. Earle*, 405 F.3d 278, 285 (5th Cir. 2005), though others have taken a broader view. *See Vogt v. City of Hays, Kansas*, 844 F.3d 1235, 1240 (10th Cir. 2017) (discussing split).

b. The text of the Self-Incrimination Clause supports the trial-centric approach. It provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const., amend. V. This text, particularly the use of "witness" and "in any criminal case," "suggests that 'its coverage [is limited to] compelled testimony that is used against the defendant in the trial itself." *Patane*, 542 U.S. at 638 (plurality op.). More specifically, "[t]he text . . . focuses on the *courtroom use* of a criminal defendant's compelled, self-incriminatory testimony." *Chavez*, 538 U.S. at 777 (Souter, J., concurring) (emphasis added). Indeed, "[w]itness here is used in its natural sense, meaning someone whose testimony, or utterances, are introduced at trial." Akhil R. Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 Mich. L. Rev. 857, 900 (1995).

Interpreting the Fifth Amendment's use of "witness" this way accords with how the Framers used the same word in the Sixth Amendment. The Sixth Amendment provides that "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him." U.S. Const., amend. VI. "Ordinarily, a witness is considered to be a witness 'against' a defendant for purposes of the [Sixth Amendment] only if his testimony is part of the body of evidence that the jury may consider in assessing his guilt." *Cruz v. New York*, 481 U.S. 186, 190 (1987).

c. This trial limitation is confirmed by the Self-Incrimination Clause's history and purpose, which reveals a focus on reliable conviction and punishment—all of which occur at trial or sentencing.[16] At the time of the Framing, "many innocent defendants in noncapital cases could not afford lawyers and were not furnished lawyers by the government." Amar & Lettow, *supra*, at 923. And defendants historically had faced "methods of proof [that] relied entirely on the behavior of the defendant, under the threat of a

[16] The U.S. Supreme Court has held that the Self-Incrimination Clause also applies at sentencing proceedings, which stems from concerns over "severity of . . . *punishment*." *Mitchell v. United States*, 526 U.S. 314, 327 (1990) (emphasis added).

penalty, to determine *guilt*." *United States v. Gecas*, 120 F.3d 1419, 1437 (11th Cir. 1997) (en banc) (emphasis added).

Against this backdrop, the Self-Incrimination Clause serves to ensure the "correct ascertainment of *guilt*" (and corresponding punishment). *Withrow*, 507 U.S. at 692 (emphasis added). Although correctly ascertaining guilt "is critical at trial"—"where final decisions are made"—it is "not so critical . . . in pretrial proceedings" when the goal is "to gather as much relevant information as possible." Amar & Lettow, *supra*, at 910 n.229. It thus makes sense for the Self-Incrimination Clause to apply only at trial.

All told, these considerations show that a self-incrimination violation does not occur until compelled testimony is introduced at trial. Respondent therefore cannot claim injury from any perceived violation of the Fifth Amendment.

2. Assuming Respondent could make out a constitutional injury, that injury is not irreparable. For a district court to have jurisdiction to issue a writ of certiorari, a defendant's injury must be of the sort "that cannot be corrected on appeal, otherwise termed as irreparable harm." *Rodriguez v. Miami-Dade Cty.*, 117 So. 3d 400,

404 (Fla. 2013).

But a criminal defendant "always has the right of appeal from a conviction in which he can attack any [allegedly] erroneous interlocutory orders," *see State v. Pettis*, 520 So. 2d 250, 253 n.2 (Fla. 1988), and the fruit-of-the-poisonous-tree doctrine applies to compelled statements. *Patane*, 542 U.S. at 639. An appellate court that determines on direct appeal that any statement was unlawfully compelled may therefore reverse and order the compelled statement and its fruits suppressed on retrial—repairing any harm. *See* § 914.04, Fla. Stat. (providing that, when a person has been compelled to provide testimony or to produce documents, "no testimony so given or evidence so produced shall be received against the person upon any criminal investigation or proceeding").

In other words, "[n]o irreparable injury" to Respondent "has yet occurred, and none is certain to follow." *State Farm Fla. Ins. Co. v. Seville Place Condo. Ass'n, Inc.*, 74 So. 3d 105, 108 (Fla. 3d DCA 2011). Indeed, it is not even clear that prosecutors will try to introduce any fruits of the compelled disclosure of Respondent's

passcode at trial.[17]

B. No other harms are implicated here.

For its part, the Fifth District believed it had jurisdiction to issue a writ of certiorari because "certiorari lies in *civil* cases to review an order compelling discovery over an objection asserting that the order violates the Fifth Amendment." App'x 34 (emphasis added); *see also Aguila v. Frederic*, 306 So. 3d 1166, 1172 (Fla. 3d DCA 2020). That circumstance is quite different.

When a civil litigant is forced to respond in a way that may incriminate him, he risks subsequent prosecution by law-enforcement officials who previously lacked a basis to bring charges. That bell—and any ensuing investigation spawned by the compelled testimony—arguably cannot be un-rung. Here, however, Respondent is already under prosecution. Should further evidence of guilt come to light, any harm can be rectified with a suppression order. *Supra*

[17] The story is different when the State seeks a writ of certiorari to correct the denial of a motion to compel access to a phone. Such a ruling would "effectively negate [the State's] ability to prosecute" and the State would be "totally deprived of the right of appellate review" because, "[s]hould the defendant be acquitted, the principles of double jeopardy [would] prevent the state from seeking review." *Pettis*, 520 So. 2d at 253.

at 20.

At any rate, and to the State's knowledge, this Court has never endorsed the approach that a litigant is categorically harmed by an order compelling him to reveal potentially incriminatory information, and this Court's opinions on isolated instances of reviewing orders compelling discovery—usually in civil cases—are inapposite. The Court has reasoned that information "that could be used to injure another person or party outside the context of the litigation" "may" cause irreparable harm. *Allstate Ins. Co. v. Langston*, 655 So. 2d 91, 94 (Fla. 1995). The same is true for "material protected by privilege, trade secrets, work product, or involving a confidential information." *Id*.

It makes sense that releasing information that a party could use to physically harm someone or that could reveal confidential business information could cause irreparable harm. Take trade secrets. The rules governing discovery balance the judicial system's interest "in the fair and efficient resolution of disputes" while seeking to avoid "discovery [that] will result in undue invasion of privacy." *Alterra Healthcare Corp. v. Estate of Shelley*, 827 So. 2d 936, 945 (Fla.

2002). When courts compel the release of private, confidential information that may injure the litigant outside the confines of litigation, the "cat"—at least arguably—"is out of the bag" because the release of the private information is the very harm to a party's privacy that is irreparable upon release. One litigant, for example, might use erroneously compelled trade secrets to harm another's business interests.

Likewise, any pretrial encroachment on the priest-penitent, psychotherapist-patient, attorney-client, or spousal privileges may give rise to a freestanding injury to the relationships those privileges are designed to protect. If, for instance, spouses learn that their private conversations may be unprotected, they are less likely to communicate openly and to experience the marital benefits that flow from that, thereby undermining the purpose of the privilege. *See, e.g.*, *Lynch v. State*, 2 So. 3d 47, 65 & n.10 (Fla. 2008).

But here, the State seeks only access to Respondent's phone, a device it already has a warrant to search. That eliminates any privacy interests. Thus, any harm that might flow from a Self-Incrimination Clause violation in this setting differs from the harm that flows from

a privacy violation.

Regardless, this Court has cautioned that "not every erroneous discovery order creates certiorari jurisdiction because some orders are subject to adequate redress by plenary appeal from a final judgment." *Allstate*, 655 So. 2d at 94. So too here. Even if this Court were to conclude that a Self-Incrimination Clause violation can occur before trial, Respondent can obtain full relief on appeal. Absent irreparable harm, the Fifth District should have dismissed his petition for a writ of certiorari.

II. THE SELF-INCRIMINATION CLAUSE DOES NOT PROTECT RESPONDENT FROM PROVIDING ACCESS TO HIS PHONE.

If the Court reaches the merits, it should conclude that the Self-Incrimination Clause does not shield Respondent from providing access to his unencrypted phone for at least two reasons. *First*, Respondent's disclosing his passcode is not testimonial—a prerequisite to seeking relief under the Fifth Amendment. Instead, revealing the passcode merely grants access to property police have the right to search. *Second*, even if it were testimonial, the U.S. Supreme Court has held that the Self-Incrimination Clause is not violated when a court compels information that is a foregone

conclusion, as that information lends nothing to the sum total of the prosecution's case. Here, the State knows that Respondent has access to the phone because it knows the phone belongs to him, a point he did not dispute in the trial court. That is all Respondent's disclosure conveys to the State, and so compelling disclosure does not trigger the Self-Incrimination Clause.

A. Disclosing a passcode is not testimonial.

As a threshold matter, disclosing a cellphone passcode is not testimonial and thus is unprotected by the Fifth Amendment. The Self-Incrimination Clause provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." It grants a right against self-incrimination that applies only when the State (1) compels a communication that is (2) incriminating and (3) testimonial. *Fisher v. United States*, 425 U.S. 391, 410 (1976).

"[T]o be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210 (1988) ("*Doe II*"). If the defendant is "force[d] . . . to disclose the contents of his own mind" or "required 'to disclose any knowledge he might have,' or 'to speak his guilt,'" his statement is testimonial. *Id.* at 211 (citation

omitted).

By contrast, it is not testimonial to: (1) repeat a statement made by a suspect, *United States v. Wade*, 388 U.S. 218, 222–23 (1967); (2) create a handwriting exemplar, *Gilbert v. California,* 388 U.S. 263, 266–67 (1967); (3) execute consent forms to grant access to contents of bank records, *Doe II,* 487 U.S. at 206; (4) don articles of clothing, *Holt v. United States*, 218 U.S. 245, 252 (1910); (5) produce blood, *Schmerber v. California*, 384 U.S. 757, 765 (1966); (6) produce abused children, *Baltimore City Dep't of Soc. Servs. v. Bouknight,* 493 U.S. 549, 551 (1990); and (7) stop at an accident and give a name and address, *California v. Byers*, 402 U.S. 424, 431–32 (1971). And most courts agree that compelling defendants to unlock their phones with biometrics like fingerprint and facial recognition also does not involve testimonial communication. *See, e.g., Stahl,* 206 So. 3d at 135.

Here, the State could care less what Respondent's passcode is, so long as police obtain unencumbered access to the phone. The contents of Respondent's mind are therefore relevant only insofar as he alone can unlock the device, and he certainly is not asked to

"speak his guilt." This case, in other words, is about *access*, not *testimony*.

Imagine a search of a home. If police have a warrant, the Supreme Court has said that it is "constitutionally reasonable to require [a suspect] to open his doors to the officers of the law." *Payton v. New York*, 445 U.S. 573, 602–03 (1980). No one could fairly claim that in requiring a suspect to unlock his front door so that police could execute a search warrant, police compelled the suspect to testify against himself. He has merely been required to grant access.

In the cellphone context, revealing the passcode is one way to grant access. But whether the trial court ordered Respondent to speak his passcode aloud, to write it down, or to enter it into the phone so that police could permanently disable the device's encryption, the result remains: The State does not seek testimony, it seeks access.

Doe II is instructive. The U.S. Supreme held there that compelling a defendant to execute consent forms granting the Government access to the contents of his bank accounts was not testimonial. *Doe II*, 487 U.S. at 202–06, 219. While "the executed

form allows the Government access to a potential source of evidence," it reasoned, the form "itself does not point the Government toward hidden accounts or otherwise provide information that will assist the prosecution in uncovering evidence." *Id.* at 215. Instead, the Government "must locate that evidence by the independent labor of its officers." *Id.* (quotation marks omitted). The consent form, at most, unlocked the door to evidence police had already discovered. Unlocking a phone is no different.

In this sense, disclosing the passcode is administrative: It allows the State to execute a valid warrant. Like disclosing a name and address at the scene of an accident, disclosing the passcode is a "neutral act," *Byers*, 402 U.S. at 432, with no "value or significance." *Stahl*, 206 So. 3d at 134. Indeed, it is not unlike "routine booking question[s] . . . exempt[ed] from *Miranda*'s coverage . . . to secure biographical data necessary to complete booking." *Pennsylvania v. Muniz*, 496 U.S. 582, 601 (1990) (plurality op.). When a question "appear[s] reasonably related to the police's administrative concerns," it is permissible in view of the Fifth Amendment. *Id.* at 601–02.

Permitting suspects like Respondent to take shelter in the Fifth Amendment would frustrate the legitimate judicial processes that underly search warrants. A warrant tells police that they may search or seize the items, places, or persons described therein. *See* U.S. Const., amend. IV. To accept Respondent's rule, however, would leave it to *private individuals* to decide if and when police can search digital devices. As the Supreme Court has observed, modern encryption means that a locked phone is "all but 'unbreakable.'" *Riley v. California*, 573 U.S. 373, 389 (2014). That is because, in "the arms race between encryption and [decryption], the mathematics overwhelmingly favors encryption." Kerr & Schneier, *supra*, at 994. In light of that technological barrier, Respondent's rule would leave police beholden to the suspect they are investigating. And it would permit suspects to defy with impunity the judge who signed the warrant and authorized the search.

In other words, "[i]nvestigators ordinarily don't seek to compel decryption because they want testimony." Kerr, *supra*, at 794. They seek to compel decryption because there may be "no other way to execute searches." *Id.*

Moreover, allowing suspects to hide behind the Fifth Amendment would predicate the execution of warrants on happenstance, "provid[ing] greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use their fingerprint" or other biometrics "as the passcode." *Stahl*, 206 So. 3d at 135. But it stands to reason that "the particular type of technology used to protect the information sought is not dispositive of whether the Fifth Amendment applies." *G.A.Q.L.*, 257 So. 3d at 1062 n.1.

The courts that disagree place too much weight on Justice Stevens' dissent in *Doe II*. Again, that case held that the Government could compel the defendant to execute certain bank-consents forms releasing his financial records. *Doe II*, 487 U.S. at 206. Justice Stevens disagreed. He compared a key to a strongbox with the combination to a wall safe to describe the contours of the Fifth Amendment's application to compelling the production of incriminating documents. *Id.* at 219 (Stevens, J., dissenting). A key to a strongbox full of incriminating evidence, he said, could be compelled with no problem. *Id.* But, Justice Stevens thought,

providing the combination to a wall safe would require the use of one's mind, and thus trigger the Fifth Amendment as a testimonial communication. *Id*.

This key-combination analogy presents a distinction without a difference. "[I]dentifying the key which will open the strongbox" and "telling an officer the combination" are functional equivalents, particularly as "technology advances." *Stahl*, 206 So. 3d at 134–35. Both require the defendant to use his mind either in finding the key to turn over or in remembering the combination to disclose. So "using the mind" cannot be the dispositive factor.

And "accepting the analogy to the combination-protected safe, whether a person who receives a subpoena for documents may invoke the Fifth Amendment would hinge on whether he kept the documents at issue in a combination safe or a key safe." *United States v. Spencer*, No. 17-cr-00259, 2018 WL 1964588, at *2 (N.D. Cal. 2018). But "that should make no difference," *id*.—in either event, the State seeks access. Thus, that a phone key takes the form of "a series of characters without independent evidentiary significance," *Andrews*, 234 A.3d at 1274, rather than a piece of metal with a series of jagged

edges is irrelevant to whether disclosing that key is testimonial under the Fifth Amendment.

This access-versus-testimony distinction accords with the original public meaning of the Self-Incrimination Clause. "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." *Doe II*, 487 U.S. at 212. The Clause addressed the Framers' concern with the "process of the ecclesiastical courts and the Star Chamber," which used "the inquisitorial method of putting the accused upon his oath and compelling him to answer questions designed to uncover uncharged offenses, without evidence from another source." *Id*. It was therefore thought to prevent "the cruel trilemma of self-accusation, perjury or contempt." *Id*. (quoting *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 55 (1964)). But the privilege against self-incrimination had nothing to say about law enforcement's execution of valid search warrants. At the time of the Framing, the State was physically and technologically able to conduct most, if not all, "[]reasonable" searches authorized by the Fourth Amendment. U.S. Const., amend.

IV. Indeed, it was understood that "[t]he king's keys unlock[ed] all doors." *Payton*, 445 U.S. at 604. A valid search warrant thus originally meant *access*. If Respondent is correct, encryption has altered that fundamental reality.

* * *

At bottom, the State asks Respondent not for *testimony*, but for *access* to a device it has a warrant to search. Because the compelled act is not functionally different than requiring a defendant to unlock the door to a home or turn over the key to a lockbox, no testimony is involved. For that reason alone, Respondent cannot refuse to disclose his passcode.

B. Alternatively, compelling the passcode is permitted by the foregone-conclusion doctrine.

Even if providing access were testimonial, Respondent's disclosure of his passcode at most communicates that he knows the passcode, a fact already known to the State. The foregone-conclusion doctrine therefore applies and renders any "testimony" unprotected by the Fifth Amendment.

1. Under the foregone-conclusion doctrine, compelled acts are not protected if the State already knows the information conveyed.

A person "may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents [i]s not 'compelled' within the meaning of the privilege." *United States v. Hubbell*, 530 U.S. 27, 35–36 (2000); *see also Fisher*, 425 U.S. at 409 (holding Government can compel production of incriminating information). That is, a defendant required to turn over documents is not forced to "be a witness against himself," U.S. Const., amend. V, because the documents already exist. Thus, "the fifth amendment privilege does not protect the contents of [those] voluntarily prepared documents." Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. Pitt. L. Rev. 27, 77 (1986). And defendants generally "cannot avoid compliance with . . . subpoena[s] merely by asserting that the item of evidence which [they are] required to produce contains incriminating writing." *Fisher*, 425 U.S. at 410.

The "act of production" exception is an exception to that rule. It provides that while the Self-Incrimination Clause does not protect documents and their contents, the act itself of producing the

documents "has communicative aspects of its own, *wholly aside from the contents of the papers produced*." *Id.* (emphasis added). This act can be testimonial if it "implicitly communicate[s] 'statements of fact.'" *Hubbell*, 530 U.S. at 36.

The "act of production" in the context of producing documents "tacitly concedes" three pieces of information: (1) "the existence of the papers demanded," (2) "their possession or control" by the defendant, and (3) the suspect's or defendant's "belief that the papers are those described in the subpoena" (*i.e.*, authentication). *Fisher*, 425 U.S. at 410; *see also Hubbell*, 530 U.S. at 36 (act of production may "admit that the papers existed, were in [the defendant's] possession or control, and were authentic"). If this information is compelled, incriminating, and testimonial, the Self-Incrimination Clause protects the defendant from disclosure.

This exception has its limits. Under the foregone-conclusion doctrine, if the State can show that it already sufficiently knows the information conveyed by the act of production—that the produced item "exist[s]," that the defendant "possess[es] or control[s]" it, and that it is authentic, *Fisher*, 425 U.S. at 410, compelling the defendant

to produce that item does not violate the Self-Incrimination Clause.

Fisher explains this principle. That case involved IRS summonses for certain taxpayer documents that had been prepared by the taxpayers' accountants. *Fisher*, 425 U.S. at 393–94. The Court reasoned that it was "confident" that "however incriminating" the documents might be, "the act of producing them"—which was "the only thing which the [accused] [wa]s compelled to do"—"would not itself involve testimonial self-incrimination." *Id.* at 410–11. That was because the accused "adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers" when "[t]he existence and location of the papers are a foregone conclusion." *Id.* at 411.

The existence and location of the papers in *Fisher* were a "foregone conclusion" because, among other things, the Government already knew to whom they belonged and by whom they were prepared, as well as that they were of "the kind usually prepared" by that type of person. *Id.* "Under these circumstances," the Court wrote, "no constitutional rights are touched" and "[t]he question is not of testimony but of surrender." *Id.* at 411 (citation and quotations

omitted). Put differently, if the act itself communicates no information that the State does not already know, the act lacks any "testimonial significance" and does not trigger the Self-Incrimination Clause. *See Doe II*, 487 U.S. at 215; *see also United States v. Doe*, 465 U.S. 605, 614 n.13 (1984) ("*Doe I*") (noting Government could "rebut[] respondent's claim by producing evidence that possession, existence, and authentication were a 'foregone conclusion'").

2. In this context, the foregone-conclusion doctrine asks whether the State already knows the defendant has the passcode.

As the Second District has properly held, the foregone-conclusion analysis asks whether the testimonial aspects of the act of production—that is, granting access to the phone by revealing the passcode—include only facts already known to the State. *See Stahl*, 206 So. 3d at 136. The First, Fourth, and Fifth Districts take a different approach. The First and Fourth Districts have required the State to show not only that the State sufficiently knows that the passcode exists and that the defendant controls or possesses it, but also that the State already knows the phone's contents. *See, e.g.*, *Varn v. State*, No. 1D19-1967, 2020 WL 5244807, at *3–4 (Fla. 1st DCA Sept. 3, 2020); *Pollard v. State*, 287 So. 3d 649, 651 (Fla. 1st

DCA 2019); *G.A.Q.L.*, 257 So. 3d at 1064. The Fifth District went a step further and held that the foregone-conclusion doctrine does not even apply to producing passcodes. App'x 39. Those holdings are wrong and will prove disastrous to law-enforcement efforts.

i. Supreme Court precedent supports this view.

In applying the foregone-conclusion doctrine to compelled passcodes, courts should focus on the information conveyed by the actual act of producing the passcode—the key that decrypts the phone. This act, like all other acts of production, conveys at most that this key exists, that the defendant possesses or controls it, and that it is authentic. *Fisher,* 425 U.S. at 410. And thus the foregone-conclusion's focus is limited to whether the State already knows those same three bits of information. Indeed, because the passcode's existence is readily apparent and the passcode "self-authenticate[s]" by working, *Andrews*, 234 A.3d at 1275, the only real inquiry is whether the State sufficiently knows that the defendant possesses or controls it.

This central focus on the *passcode,* not the phone's *contents*, follows from the U.S. Supreme Courts cases involving the foregone-

conclusion doctrine. These cases show that when analyzing whether an act of production is testimonial, the sole consideration is the testimonial significance of the information conveyed by the act itself—not to what informational content the act may lead. Otherwise, the act-of-production exception would swallow the general rule that courts can compel suspects "to produce specific documents even though they contain incriminating assertions of fact or belief." *Hubbell*, 530 U.S. at 35.

In *Fisher*, the Court explained that the Self-Incrimination Clause did not protect the actual documents sought by the Government even though their contents "might incriminate" the defendant. 425 U.S. at 409. Because the defendant prepared the content voluntarily, the documents could not "be said to contain *compelled* testimonial evidence." *Id.* at 409–10 (emphasis added). Instead, the Court explained, "the *only* thing compelled is the act" of producing the documents. *Id.* at 410 n.11 (emphasis added). That act "has communicative aspects of its own, *wholly aside* from the *contents* of the papers produced." *Id.* at 410 (emphases added). Though the Self-Incrimination Clause might cover the act of

producing preexisting, voluntarily created documents, it "does not shield the *contents*" of those documents. Alito, *supra*, at 29, 44 (emphasis added).

Thus, when the *Fisher* Court conducted its foregone-conclusion-exception analysis, it did not look to the contents of the compelled documents. The Court instead looked to whether the Government already knew the documents existed, who possessed or controlled them, and their authenticity. *Fisher*, 425 U.S. at 410–13.

The Court confirmed this distinction in *Doe I*. Even though the contents of the documents sought there were incriminating—and although the Government had failed to do so—the Government could have "rebutted" the self-incrimination claim "by producing evidence that possession, existence, and authentication [of the documents] were a 'foregone conclusion.'" *Doe I*, 465 U.S. at 614 n.13. The Court did not include the "contents" of the compelled documents in this analysis.

The Court in *Doe II* reemphasized the distinction between information conveyed by the act of production itself and the informational content to which the compelled act might lead. The *Doe*

II petitioner argued that the Government could not compel him to execute consent forms to foreign banks "to release records as to which the banks believe[d] he has the right of withdrawal." 487 U.S. at 207. The Court rejected this argument. In doing so, it limited its analysis to the compelled act of executing the consent forms. That executing the consent forms would "allow[] . . . access to a potential source of evidence" did not matter. *Id.* at 215. "If a compelled statement is not testimonial and for that reason not protected by the privilege," the Court explained, "it cannot become so because it will lead to incriminating evidence." *Id.* at 208 n.6.

The most recent United States Supreme Court case on compelled acts tracks this distinction. *Hubbell*, 530 U.S. 27. In *Hubbell*, the Court reiterated *Fisher*'s and *Doe*'s holdings that "a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege." *Hubbell*, 530 U.S. at 35–36. And the Court again clarified that courts should not look to the contents of the documents produced to determine whether the act of producing those

documents is testimonial: "The 'compelled testimony' that is relevant is *not* to be found in the contents of the documents produced . . . . It is, rather, the testimony inherent in the act of producing those documents." *Id.* at 40. The content to which a compelled production grants access, then, does not affect whether the compelled act is testimonial, even if it is incriminating.

Interpreting these decisions, most state supreme courts have focused their inquiry on whether the State already knows the defendant has the power to grant access—that is, knows the passcode.[18] Several federal courts[19] and intermediate state appellate courts[20] have held the same. And that is the view of the leading scholar in this area.[21]

---

[18] *See, e.g.*, *Pittman*, 479 P.3d 1028 at 1044; *Andrews*, 234 A.3d at 1273; *Commonwealth v. Jones*, 117 N.E.3d 702, 710 (Mass. 2019).

[19] *See, e.g.*, *United States v. Gavegnano*, 305 F. App'x 954, 956 (4th Cir. 2009); *Spencer*, 2018 WL 1964588, at *3; *In re Search of a Residence in Aptos*, No. 17-MJ-70656-JSC-1, 2018 WL 1400401, at *6 (N.D. Cal. Mar. 20, 2018); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1236–37 (D. Colo. 2012) (similar); *cf. United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n. 7 (3d Cir. 2017).

[20] *See, e.g., Stahl*, 206 So. 3d at 136; *State v. Johnson*, 576 S.W.3d 205, 227 (Mo. Ct. App. 2019).

[21] *See* Kerr, *supra*, at 779 ("'I know the password' is the only assertion implicit in unlocking the device . . . the act of unlocking the device does not communicate knowledge about the device's contents.").

This makes sense. If the Self-Incrimination Clause categorically does not apply to pre-existing content within documents, then that content should not factor into whether the act itself of producing the documents with that content is testimonial. Nothing supports changing this settled law by "meld[ing] the production of passcodes with the act of producing the contents of the phones." *Andrews*, 234 A.3d at 1274.

Even if producing a phone's passcode gives the State "access to a potential source of evidence" in the phone's content, *Doe II*, 487 U.S. at 215, and even if that content is incriminating, the State did not compel the creation of that content, so the Self-Incrimination Clause does not apply to it, *see Hubbell*, 530 U.S. at 35–36; *Fisher*, 425 U.S. at 409–10. That is, the contents of a document are unprotected by the Fifth Amendment—it is only what the act of production may reveal that can be testimonial. And, as Judge Winokur has observed, "[i]n no other context does the foregone-conclusion analysis focus on evidence other than the evidence being compelled." *Pollard*, 287 So. 3d at 661 (Winokur, J., dissenting). Here, the only testimony being compelled is the act of producing the

key to the phone, and "[t]here is no reason to shift the focus now." *Id*.

ii. A contrary approach improperly conflates the Fourth and Fifth Amendments.

The U.S. Supreme Court has interpreted the Fourth Amendment to require three things for the issuance of a warrant: (1) a neutral and detached magistrate; (2) probable cause; and (3) particularity as to the things to be seized and place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979). There is no dispute here that police obtained a valid warrant. *See* App'x 9–13.

But the courts that focus their foregone-conclusion inquiry on the contents of the phone conflate the Fourth and Fifth Amendments by reading into the Fifth Amendment its own particularity requirement. In *G.A.Q.L.*, for instance, the Fourth District asked whether the State already knew with "reasonable particularity"—a Fourth Amendment concept—"the data the state seeks behind the passcode wall." 257 So. 3d at 1063. That is, the Fourth District required the State, under the Fifth Amendment, to demonstrate a super-charged form of particularity: It was not enough that police convinced a magistrate that there was probable cause to believe a particular item—the phone—contained evidence of a crime, the State

also had to show that it knew the *contents* of that evidence before the search could even occur.[22]

That would be incorrect in all events because the Fourth Amendment contains no such heightened requirement. Even if it did, however, the Supreme Court has never accepted the view that the Fifth Amendment contains its own particularly requirement.

Indeed, in *Fisher* the Court held that the Self-Incrimination Clause does not "serve as a general protector of privacy." 425 U.S. at

---

[22] The *G.A.Q.L.* court also relied on the Eleventh Circuit's decision in *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335 (11th Cir. 2012), which held that the Government in that case had not met the foregone-conclusion doctrine. But the Government had sought to compel the defendant both to decrypt his device *and to produce the files* that the Government sought. *In re Grand Jury*, 670 F.3d at 1337 n.1. *In re Grand Jury* thus involved *two* compelled acts: the act of decrypting the files and the act of producing the files. It therefore is not remarkable that the Eleventh Circuit applied the foregone-conclusion doctrine not just to the passcode but also to the files. The additional compelled act to produce altered the analysis from looking only to the testimony in the act of decrypting the files (that the defendant knew the passcode) to the testimony conveyed in the added act of producing *the files* (that the requested files existed and that the defendant possessed them). The compelled production of the actual files also makes *In re Grand Jury* like *Hubbell*, where the Government unsuccessfully sought to compel the defendant to identify and produce thousands of incriminating documents. *Hubbell*, 530 U.S. at 41–42. The opposite is true here, where the State seeks only access to the device.

401. Privacy is "not mentioned in" the Self-Incrimination Clause's text, and is instead "directly addressed in the Fourth Amendment." *Id*. "Insofar as private information not obtained through compelled self-incriminating testimony is legally protected," the Court reasoned, "its protection stems from other sources" like "the Fourth Amendment's protection against seizures without warrant or probable cause," protections "against subpoenas which suffer from too much indefiniteness or breadth in the things required to be 'particularly described,' . . . or evidentiary privileges such as the attorney-client privilege." *Id*. (citations and quotations omitted).

iii. Policy considerations counsel against creating phone-specific exceptions to the foregone-conclusion doctrine.

A rule forbidding law enforcement from compelling a defendant's cellphone passcode would be disastrous. For centuries, law enforcement could simply break a lock to gain access to hidden evidence. *See, e.g.*, *Semayne's Case*, 5 Co. Rep. 91a, 91b, 77 Eng. Rep. 194, 195 (K.B. 1603) ("[W]hen the King is party, the sheriff (if the doors be not open) may break the party's house, either to arrest him, or do other execution of the King's process, if otherwise he cannot enter."). The Framers understood this. They included in the

Bill of Rights the *Fourth* Amendment to prevent sprawling, unjustified searches for evidence. *See* George C. Thomas III, *Stumbling Toward History: The Framers' Search and Seizure World*, 43 Tex. Tech. L. Rev. 199, 206–210 (2010). When the Fourth Amendment's protections are satisfied, the Framers would not have understood the Self-Incrimination Clause to nevertheless permit defendants to shield evidence from search.[23] *See, e.g.*, *Fisher*, 425 U.S. at 399. At the time of the Framing, such a tactic was not even technologically feasible.

But it is now. Technological advancements have shifted the balance of power between criminals and law enforcement in favor of crime, *see* Kerr & Schneier, *supra*, at 994, as encrypted devices are now "all but 'unbreakable.'" *Riley*, 573 U.S. at 389. And even if states could overcome the mathematics to break passcodes by "brute force," technology companies often limit the number of unsuccessful attempts, deleting a phone's data if the would-be decoder reaches that number. *See, e.g.*, *Seo v. State*, 109 N.E.3d 418, 425 (Ind. Ct. App.), *vacated sub nom. Seo v. State*, 148 N.E.3d 952 (Ind. 2020).[24]

---

[23] This understanding is another reason that granting access to a phone is not testimonial to begin with.

[24] Some companies claim they can defeat all forms of

This elbow on the scale for encryption, combined with the First and Fourth District's impossibly iterative test of requiring the State to show that it already knows the contents that it seeks to search, or the Fifth District's holding that passcodes do not even qualify for the foregone-conclusion doctrine, would mean that any time a suspect password-protected a device or a file, it would be impossible to force him to unlock it—even with a warrant. This reading of the Self-Incrimination Clause would lead to "unpoliceable zone[s] of lawlessness." *Seo*, 109 N.E.3d at 443 (May, J., dissenting), not contemplated by the Fourth Amendment.

And it does "not follow that the constitutional values protected by [the Fifth Amendment] are of such overriding significance that they compel substantial sacrifices . . . where the pursuit of [governmental] objectives requires the disclosure of information which will undoubtedly significantly aid in criminal law

---

encryption. *E.g.*, Cellebrite, https://www.cellebrite.com/en/law-enforcement/lab/ (last visited Mar. 12, 2021). But these services are expensive (ranging from $9,000 to $15,999), SC Media, *Cellebrite UFED Series*, https://www.scmagazine.com/review/cellebrite-ufed-series/ (Oct. 1, 2015), and have failed in the past, *e.g.*, *Johnson*, 576 S.W.3d at 218 n.4. And with the rapid pace of technology, a decryption method that works today may not work tomorrow.

enforcement." *Byers*, 402 U.S. at 448 (Harlan, J., concurring). Thus, the Supreme Court has sometimes "balanc[ed] the public need" with "the individual claim to constitutional protections." *Id.* at 427 (plurality op.).

The public need here is surpassing: If Respondent is correct, then police are powerless to uncover child pornography on an encrypted phone or hard drive; to confirm that a suspect has been dealing drugs with help from a cellphone; or to prove that a defendant used his cellphone as the trigger for a bomb. And that would be so simply because a criminal had the wherewithal to passcode-protect his devices, an option that is already the default setting on many devices. *See* Kerr, *supra,* at 768. But defendants should not receive greater Fifth Amendment protection simply because they now use phones to communicate, store records, take photographs, and undertake any number of other activities, some lawful, some not.[25]

[25] Another balancing consideration is the option to require the State to offer use immunity for the act of disclosing a passcode. The State usually can compel testimony only if it offers the defendant use *and* derivative-use immunity. *See Hubbell*, 530 U.S. at 38–39; *Kastigar v. United States*, 406 U.S. 441, 453 (1972). If the Court were not satisfied that meeting the foregone-conclusion exception eliminates all testimonial significance of the act of Respondent's

At the time of the Framing, those acts would not have been encrypted, and thus would have been accessible to a law-enforcement agent with a warrant.

Moreover, the Fifth District was wrong to conclude that "it would be imprudent to extend the foregone conclusion exception" to "compel[ing[oral testimony" in the digital context. App'x 39. To begin with, the State does not truly seek "oral testimony." It seeks access to the unlocked phone, and, like asking a suspect to open the door to his house, asking Respondent to produce his passcode is simply the most expedient method of achieving that. If the trial court ordered Respondent to manually unlock the phone by entering his passcode, the practical effect would be the same, and that would surely not be oral testimony. Indeed, although less preferable,[26] the State could

---

producing his passcode, an alternative would be to hold that the State could still compel Respondent to produce his passcode and make derivative use of that act—accessing Respondent's phone. But the State, under this alternative, could not use the act of Respondent's producing his passcode at trial. One federal district court has reached this conclusion. *See Spencer*, 2018 WL 1964588, at *3. That would accommodate the often-competing interests of the criminal justice system and individuals who come before it.

[26] Two practical difficulties make this a less workable option. First, having a suspect manually enter his passcode into a phone requires giving the suspect temporary possession of the device, which

manage to execute warrants if this Court were to hold that it could require suspects to enter—rather than turn over—passcodes.

At any rate, the act-of-production exception places compelled physical acts on the same potentially self-incriminating footing as compelled oral acts. The doctrine makes it so the State cannot get around compelling oral testimony simply by compelling a defendant to physically act in a way that conveys the same information as if the State were to compel a defendant to speak. Contrary to the Fifth District's conclusion, whether the compelled act is oral or physical does not affect whether the State already knows the information conveyed by that oral or physical testimony. Orally conveying a passcode does not somehow reveal more information than physically conveying a passcode. Whether orally conveyed, physically conveyed on a slip of paper, or entered directly into a phone, producing a passcode conveys its existence, who possesses or controls it, and that it is authentic. Each of these compelled acts are "governed by the same Fifth Amendment analysis." *G.A.Q.L.*, 257 So. 3d at 1062 n.1.

---

creates the risk that he will attempt to destroy or tamper with it. Second, turning over the passcode ensures that, should technical issues arise after the suspect has unlocked the phone, police will be able to regain access.

Thus, if the State already knows that information, the foregone-conclusion doctrine removes the compelled act—oral or physical—from the Fifth Amendment's protection.

3. The preponderance of the evidence standard applies.

Courts applying the foregone-conclusion analysis from *Fisher* have sometimes referred to a "particularity" standard—that is, whether the State has shown that it already knows "with reasonable particularity" that the information compelled exists, is within the accused's possession or control, and is authentic. The D.C. Circuit, for example, adopted this standard in *Hubbell*. *United States v. Hubbell*, 167 F.3d 552, 579 (D.C. Cir. 1999). But because the Supreme Court determined that the Government in that case could not meet the foregone-conclusion doctrine, *Hubbell*, 530 U.S. at 44–45, the Court did not opine on the correct standard.

A few courts, though, have rejected the reasonable-particularity test in the context of passcodes and have instead looked to traditional evidentiary burdens. *See, e.g.*, *Fricosu*, 841 F. Supp. 2d 1232, 1236–37; *Spencer*, 2018 WL 1964588, at *3; *Jones*, 117 N.E.3d at 712 n.11. Reasonable particularity comes from the Fourth Amendment, which

requires that warrants "particularly describ[e]" the place or things to be searched. U.S. Const., amend. IV; *see also Dean v. State*, 478 So. 2d 38, 41 (Fla. 1985) (explaining that the Fourth Amendment "protects against subpoenas which suffer from too much indefiniteness or breadth in the things to be particularly described" (quotations and citations omitted)). That standard is inapplicable to testimony. This Court thus should follow these courts in looking to traditional evidentiary burdens rather than applying a "reasonable particularity" test.

The preponderance of the evidence standard applies here. This standard often applies to questions, like this one, of a preliminary nature. "[W]hen preliminary facts are disputed," this Court has explained, "the offering party must prove them by a 'preponderance of the evidence.'" *Romani v. State*, 542 So. 2d 984, 985 n.3 (Fla. 1989).

That requirement holds true for an alleged Self-Incrimination Clause violation. For example, when determining "the voluntariness of a defendant's statement," this Court has held that "[t]he fifth amendment privilege against self-incrimination . . . requires the

government to prove [that voluntariness] by a preponderance of the evidence." *Balthazar v. State*, 549 So. 2d 661, 662 (Fla. 1989). And the U.S. Supreme Court has similarly held that "the controlling burden of proof at suppression hearings should impose no greater burden than proof by a preponderance of the evidence." *United States v. Matlock*, 415 U.S. 164, 177 n.14 (1974) (citing *Lego v. Twomey*, 404 U.S. 477, 488-89 (1972)).

Florida courts elevate the standard—from a preponderance evidence to clear and convincing evidence—only when the defendant has already established some "illegal conduct on the part of the police," *Reynolds v. State*, 592 So. 2d 1082, 1082 (Fla. 1992) (holding consent to search was not voluntary because suspect was illegally handcuffed when he consented), or other unusual circumstances like a child's consenting to search a parent's bedroom, *Saavedra v. State*, 622 So. 2d 952, 956 n.6 (Fla. 1993). Police misconduct or other unusual circumstances like that do not exist here.

Consistent with this generally applicable Fifth Amendment evidentiary burden, at least one federal court has asked whether the Government showed by a preponderance that the defendant already

controls or possesses the passcode. *Fricosu*, 841 F. Supp. 2d at 1235–36. As discussed next, the State satisfied that burden here.

4. The foregone-conclusion doctrine is met here.

If, instead of his phone, the State held a warrant to search Respondent's locked home or storage locker, litigation would be unnecessary—the State could break in as needed. But Respondent put a passcode on his phone that stands as an impenetrable barrier to the search, and the only practicable way to execute the warrant is to ask Respondent to grant access.

Under the framework discussed above, the trial court correctly ruled that Respondent must disclose his passcode. That is because the State has shown by a preponderance of the evidence that it already knows that (1) the passcode exists, (2) Respondent controls or possesses it, and (3) it is authentic.

That the passcode exists is obvious: it has frustrated law enforcement's efforts to access the phone to execute their search warrant. The passcode also is self-authenticating, as the authenticity of the passcode will be readily apparent when it successfully unlocks the phone. *Andrews*, 234 A.3d at 1275. The only debate is whether the State has shown by a preponderance of the evidence that

Respondent has possession or control over the passcode. As amply demonstrated by the record, it has.

A witness—the victim—has already "identified the black Samsung as belonging to [Respondent]." App'x 4. To corroborate that assertion, police asked the witness to call the phone number that she had saved as Respondent's number. *Id*. When she did, the "Samsung began to ring and the contact on the home screen read [the victim's name,] with [the victim's] phone number displayed." *Id*. And Respondent's sworn arrest affidavit lists his phone number as the same that the victim relayed. *Id*. at 4, 8. The victim's statements to police are further corroborated by Respondent's "documented" history of dating violence. *Id*. at 4.

Throughout this litigation, Respondent has never argued that the phone is not his and even appeared to concede in the trial court that he owned the phone. *See id*. at 24 ("[C]ompelling the Defendant in this case to disclose or provide *his password* would be testimonial." (emphasis added)). At the motion-to-compel hearing, Respondent never disputed that the phone was his or argued that he could not produce the passcode. And Respondent offered no evidence to rebut

the State's assertion that the phone was his; nor did he ask for an evidentiary hearing to establish that he was not the owner. In a word, the State's evidence went uncontradicted.

Respondent's silence on whether the phone was his continued into the Fifth District. There, Respondent did not expressly dispute in his certiorari petition that the phone was his. Am'd Pet. for Writ of Cert., No. 5D19-590, at *1 (Mar. 7, 2019) (referring to the phone as "purportedly belonging to the Defendant"). It was not until his reply brief that, for the first time, Respondent argued that "there has been no admission from him that the phone belongs to him," Reply, No. 5D19-590, at *9 (Apr. 11, 2019), but even then he did not argue that he was *not* the phone's owner.

These unrebutted facts are enough to show by a preponderance of the evidence—and even by a *higher* standard—that the phone belongs to Respondent and thus that Respondent has control or possession over the phone's passcode. So even though Respondent's producing the passcode would convey that he has control or possession over his passcode, the State already sufficiently knows this. Under the foregone-conclusion doctrine, the Fifth Amendment

Self-Incrimination Clause therefore does not prevent the State's compelling Respondent to produce his passcode.

CONCLUSION

This Court should quash the Fifth District's decision.

Dated: March 12, 2021

Respectfully submitted,

ASHLEY MOODY
Attorney General

/s/ Jason H. Hilborn
AMIT AGARWAL (FBN125637)
Solicitor General
JEFFREY PAUL DESOUSA (FBN110951)
Chief Deputy Solicitor General
CHRISTOPHER J. BAUM (FBN1007882)
Senior Deputy Solicitor General
JASON H. HILBORN (FBN1008829)
Assistant Solicitor General
Office of the Attorney General
The Capitol, PL-01
Tallahassee, Florida 32399
(850) 414-3300
amit.agarwal@myfloridalegal.com
jeffrey.desousa@myfloridalegal.com
christopher.baum@myfloridalegal.com
jason.hilborn@myfloridalegal.com

Counsel for State of Florida

CERTIFICATE OF COMPLIANCE

I certify that this brief was prepared in 14-point Bookman font, in compliance with Florida Rule of Appellate Procedure 9.210(a)(2) and contains fewer than 13,000 words.

/s/ Jason H. Hilborn
Assistant Solicitor General

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing was furnished via the e-Filing Portal on this **twelfth** day of March 2021, to the following:

Robert Adams
Marie Taylor
Assistant Public Defender
435 North Orange Avenue Suite 400
Orlando, FL 32801
radams@circuit9.org
(407) 270-0402

Counsel for Respondent

/s/ Jason H. Hilborn
Assistant Solicitor General