IN THE SUPREME COURT OF FLORIDA

CASE NO.: SC20-1419

STATE OF FLORIDA,

Petitioner,

v.

JOHNATHAN DAVID GARCIA,

Respondent.

ON PETITION FOR DISCRETIONARY REVIEW OF A DECISION OF THE FIFTH DISTRICT COURT OF APPEAL
LOWER CASE NO.: 5D19-0590

APPENDIX TO THE ANSWER BRIEF

ROBERT WESLEY, B.C.S.
Public Defender

ROBERT THOMPSON ADAMS IV
Florida Bar No. 107152
Assistant Public Defender

CATHERINE CONLON, B.C.S.
Florida Bar No. 663271
Assistant Public Defender

DAVID L. REDFEARN, B.C.S.
Florida Bar No. 21228
Assistant Public Defender

MARIE TAYLOR
Florida Bar No. 1003697
Assistant Public Defender

Office of the Public Defender
435 N. Orange Ave., Suite 400
Orlando, FL 32801
407-270-0402
radams@circuit9.org
cconlon@circuit9.org
dredfearn@circuit9.org
mtaylor@circuit9.org

Counsel for Respondent

INDEX

Garcia's Amended Petition for Writ of Certiorari (Mar. 7, 2019).....3

State's Response to Garcia's Cert. Petition (Apr. 1, 2019).....22

Garcia's Reply to the State's Response (Apr. 11, 2019).....31

FDLE Contracts, Agreements and Purchases for the 2017–18 Fiscal Year.....48

IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
IN AND FOR THE FIFTH JUDICIAL DISTRICT

Case No.: 5D19-0590
Lower Case No.: 2018-CF-005112-A-OR

JOHNATHAN DAVID GARCIA,

Petitioner,

v.

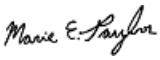
STATE OF FLORIDA,

Respondent.

AMENDED PETITION FOR WRIT OF CERTIORARI

ROBERT WESLEY
PUBLIC DEFENDER

Robert Adams
Florida Bar No. 107152
Assistant Public Defender



Marie Taylor
Florida Bar No. 1003697
Assistant Public Defender

Office of the Public Defender
435 N. Orange Ave., Suite 400
Orlando, FL 32801
407-836-4887
radams@circuit9.org

TABLE OF CONTENTS

TABLE OF CONTENTS…… ii

TABLE OF AUTHORITIES iii

JURISDICTION.....1

FACTS 1

ARGUMENT 6

CONCLUSION.....14

CERTIFICATE OF SERVICE 16

CERTIFICATE OF COMPLIANCE.....16

TABLE OF AUTHORITIES

Cases

Doe v. United States, 487 U.S. 201 (1988) 8, 9, 15

Fisher v. United States, 425 U.S. 391 (1976) 8, 12

G.A.Q.L. v. State, 257 So. 3d 1058 (Fla. 4th DCA 2018) 8, 10, 11, 12, 13, 15

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) 9, 10, 11, 12, 13

Seo v. State, 109 N.E.3d 418 (Ind. Ct. App. 2018) 9

State v. Stahl, 206 So. 3d 124 (Fla. 2d DCA 2016) 8, 9, 10

United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010) 9

Rules

Fla. R. App. P. 9.030 2

Constitutional Provisions

Amend. V, U.S. Const. 8

Art. I, § 9, Fla. Const. 8

JURISDICTION

This Court has jurisdiction to issue a Writ of Certiorari pursuant to Florida Rule of Appellate Procedure 9.030(b)(3). The subject matter of the case is within the jurisdiction of the District Court of Appeal, and the lower tribunal is within the Court's jurisdiction.

FACTS

1. On March 22, 2018, law enforcement provided an affidavit for and subsequently acquired an arrest warrant authorizing the arrest of the Defendant on suspicion of aggravated stalking. *See* Amend. App. Ex. A.

2. On April 25, 2018, the Defendant was arrested on the active warrant. *See* Amend. App. Ex. B.

3. On May 21, 2018, the State filed an Information charging the Defendant with three counts: aggravated stalking with a credible threat, a third-degree felony; criminal mischief causing damage of $1000 or more, a third-degree felony; and criminal mischief, a second-degree misdemeanor.

4. On January 3, 2019, almost a year after applying for a warrant to arrest the Defendant, the State applied for and acquired a search warrant to download and search through the contents of a Samsung Galaxy Note 8 purportedly belonging to the Defendant. *See* Amend. App. Ex. D.

5. The search warrant identifies the phone as one found near a broken window at the alleged victim's home. Amend. App. Ex. D at 2. The State suspects that the Defendant threw the phone at the alleged victim's window. The warrant describes how law enforcement identified the phone as belonging to the Defendant. Amend. App. Ex. D at 2. The warrant also describes how a GPS tracker was found in the alleged victim's car that can be tracked using a smart phone. Amend. App. Ex. D. at 2. The warrant concludes that there is "probable cause to believe the black Samsung Galaxy Note8 [. . .] contains storage of evidentuary [sic] data pertaining to Aggravated Stalking with Crediable [sic] Threat[.]" Amend. App. Ex. D at 2.

6. The warrant seeks to acquire all data from the phone's "central processing units, internal and peripheral storage, memory storage devices or media such as optical disks, or any other storage where data can be stored, together with indicia of use, ownership, possession, or control of such data." Amend. App. Ex. D at 2. Furthermore, the warrant also seeks "[o]ther data of relevance to this incident" including "video files (digital, analog or any other format), still photo camera files (digital, analog, or any other format), e-mails, chat logs, passwords/login names, and internet access documents, history and cache." Amend. App. Ex. D. at 2.

7. On January 11, 2019, the State filed an Amended Information charging the Petitioner with five counts: throwing deadly missile at, within, or into a building, a second-degree felony; two counts of aggravated stalking with a credible threat, a

third-degree felony; criminal mischief with damage of more than $200, a first-degree misdemeanor; and criminal mischief, a second-degree misdemeanor. *See* Amend. App. Ex. C.

8. On February 26, 2019, the State filed its Motion to Compel Defendant's Phone Passcode. *See* Amend. App. Ex. E. The motion states that a download of the data contained in the phone was attempted pursuant to the warrant by law enforcement, but since law enforcement was unable to unlock the phone, the download was unsuccessful. Amend. App. Ex. E at 1. The motion seeks an order from the trial court to compel the Defendant to unlock the phone by providing the passcode or using his fingerprint to unlock the phone. Amend. App. Ex. E at 1. The motion contends that the "contents of the Defendant's phone are relevant to how the events occurred and whether Defendant is guilty," and that the compelled disclosure of the passcode "will involve no unreasonable intrusions upon the body of the Defendant." Amend. App. Ex. E at 1.

9. The Defense objected to the State's motion and a hearing was held on the morning of March 4, 2019, before the Honorable Gail Adams.

10. At the hearing, the State noted that law enforcement previously acquired a search warrant to search the contents of the phone. Amend. App. Ex. F at 4. The State explained that law enforcement is unable to execute the search via

downloading the contents of the phone because the phone is passcode protected. Amend. App. Ex. F at 4.

11. Judge Adams noted that there was new case law concerning this issue, and the State acknowledged that there is inter-district conflict between the Second District Court and the Fourth District Court. Amend. App. Ex. F at 4.

12. The trial court then inquired what effect the existence of the search warrant has on the merits of the State's motion to compel the passcode. Amend. App. Ex. F at 4–5. The State conceded that the existence of the search warrant does not change the merits or the interpretation of the applicable case law. Amend. App. Ex. F at 5.

13. The State analogized the passcode to a lock on the front door to a house that the law enforcement already has a search warrant to search. Amend. App. Ex. F at 5.

14. The trial court solicited the Defense's position, and Petitioner's counsel argued that Petitioner's objection is based on the interpretation applied by the Fourth District in the case of *G.A.Q.L. v. State*, 257 So. 3d 1058 (Fla. 4th DCA 2018). Amend. App. Ex. F at 5–6.

15. Copies of that case and the Second District case, *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016) were provided to the trial court by Petitioner's counsel and the State. Amend. App. Ex. F at 6.

16. Petitioner's counsel began arguing that an order compelling Petitioner to disclose a passcode to a phone "would be testimonial and would be in violation of the Fifth Amendment based on [*G.A.Q.L.*]." Amend. App. Ex. F at 6.

17. The State then interjected, noting that the Second District found "the exact opposite" in the *Stahl* case. Amend. App. Ex. F at 6. The State summarized *Stahl* by arguing that the Second District found that providing the passcode is not testimonial and that, even if it is, the State could establish in *Stahl* "with particularity what they're looking for is in the possession and control of the Defendant, then the foregone conclusion doctrine would provide an exception ot the Fifth Amendment right." Amend. App. Ex. F at 7.

18. The trial court then asked the State to confirm that one of the charges in this case is stalking, which the State confirmed. Amend. App. Ex. F at 7. The trial court then asked the State for a conclusory answer as to whether the contents of the phone have "to do with the stalking," which the State answered "[It] does, your honor." Amend. App. Ex. F at 7.

19. The State then began to expound on that point, but the trial court interjected by granting the State's motion over Petitioner's objection. Amend. App. Ex. F at 7. The trial court then ordered that Petitioner provide the passcode by 9:00 a.m. the following morning when he appeared in court for pre-trial conference. Amend. App. Ex. F at 8.

20. Petitioner's counsel asked the trial court for clarification as to the basis for its finding and whether it was finding the *Stahl* case controlling; the trial court answered that it was finding that compelling the passcode is "non-testimonial and it's pursuant to a warrant that's already been issued based on probable cause." Amend. App. Ex. F at 8.

21. The trial court's order was done orally on the record and is memorialized in the court minutes. *See* Amend. App. Ex. G. The trial court has not issued a written order with specific findings of fact and law disposing of the State's motion.

22. Later that day, Petitioner's counsel filed a Motion for Stay of Proceedings seeking a stay of the trial court's order and the trial proceedings until this Petition is resolved.

23. On the morning of March 5, 2019, just before Petitioner was to provide his passcode, the trial court heard and granted Petitioner's motion to stay the proceedings and the order compelling Petitioner to provide the passcode pending the outcome of the Petition.

ARGUMENT

The trial court has granted the State's motion to compel the Petitioner to disclose the passcode to a Samsung Galaxy Note 8 smart phone, and, in doing so, issued an order that violates the Petitioner's Fifth Amendment right against compelled self-incrimination as applied to the State of Florida through the

Fourteenth Amendment. The trial court's determination that the Petitioner's Fifth Amendment right does not protect him from the compelled disclosure constitutes a departure from the essential requirements of the law. This departure from the requirements of the law will result in material injury to the Petitioner, namely the violation of his Fifth Amendment right, which will then be compounded by whatever evidence the State acquires as a result of that unconstitutionally compelled disclosure. This injury has no adequate remedy on direct appeal. Therefore, as both the Second District and Fourth District Courts of Appeal have previously recognized, a petition for writ of certiorari is the proper means for the Petitioner to seek this Court's review of the trial court's order. *See G.A.Q.L. v. State*, 257 So. 3d 1058 (Fla. 4th DCA 2018); *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016).

The Fifth Amendment to the United States Constitution provides the Petitioner's right against self-incrimination: "No person [. . .] shall be compelled in any criminal case to be a witness against himself [. . .]" Amend. V, U.S. Const.[1]. Included in this protection against bearing witness against oneself includes a protection against the compelled disclosure or production of incriminating information where such disclosure or production would be deemed testimonial. *Fisher v. United States*, 425 U.S. 391, 408 (1976). The disclosure constitutes

[1] Also recognized in Article I, § 9 of the Florida Constitution.

testimonial communication when the disclosure itself "explicitly or implicitly, relate[s] a factual assertion or disclose[s] information." *Doe v. United States,* 487 U.S. 201, 210 (1988). A testimonial communication is one that requires the Petitioner to "disclose any knowledge he might have" or otherwise "speak his guilt." *Id*. at 211. As the Fourth District noted in *G.A.Q.L.*, Justice Breyer's dissent in the *Doe* case has become a point of reference in determining when a defendant's right against self-incrimination is triggered: "[A defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed." *Doe*, 487 U.S. at 219.[2]

A number of cases and courts have dealt with the question of whether compelling a defendant to provide a passcode constitutes a violation of the Fifth Amendment. *See State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012) (hereinafter "*In re Supboena*"); *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010); *Seo v. State*, 109 N.E.3d 418 (Ind. Ct. App. 2018). Out of

[2] The Second District cast doubt on this analogy despite its common usage, stating, "Despite the many cases referencing the quote, we have found none that provide details of 'surrender[ing] a key.' We question whether identifying the key which will open the strongbox—such that the key is surrendered—is, in fact, distinct from telling an offer the combination." *Stahl*, 206 So. 3d at 134–35. Petitioner believes this is an indication of the aberrant nature of the Second District's analysis and holding on the question of whether compelled disclosure of a passcode is testimonial.

these cases, the only court to conclude that the compelled production of a phone passcode is not prohibited by the Fifth Amendment was Florida's Second District Court of Appeal in *Stahl*. As the Fourth District summarized in *G.A.Q.L.*, the other courts held that:

> [R]evealing one's password requires more than just a physical act; instead it probes into the contents of an individual's mind and therefore implicates the Fifth Amendment. *See Kirschner*, 823 F. Supp. 2d at 669. The very act of revealing a password asserts a fact: that the defendant knows the password. *See Hubbell*, 530 U.S. at 43 (stating that the Fifth Amendment applies "to the testimonial aspect of a response to a subpoena seeking discovery" of sources of potentially incriminating information). Thus, being forced to produce a password is testimonial and can violate the Fifth Amendment privilege against compelled self-incrimination. *See id*. at 38 ("Compelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory.") (quoting *Doe*, 487 U.S. at 208 n. 6).

G.A.Q.L., 257 So. 3d at 1061–62.

The Fourth District considered and rejected the Second District's interpretation of what was being compelled in *Stahl*. The Fourth District noted that the Second District believed compelling a defendant to provide a phone passcode did not constitute compelling testimonial communication because the passcode was supposedly "sought only for its content and the content has no other value or significance[.]" *Stahl*, 206 So. 3d at 134. The Fourth District disagreed with this

analysis, and Petitioner urges this Court to do the same. Instead, the Fourth District relied upon the Eleventh Circuit Court of Appeals' interpretation of the issue in the *In re Supboena* case. *G.A.Q..L.*, 257 So. 3d at 1062. The Fourth District found the question of whether the defendant in *In re Subpoena* could be compelled to provide the password to a decryption key for the defendant's hard drives analogous to the question presented in this case and in *G.A.Q.L.* The Fourth District found that as a matter of technical fact, a decryption key and the passcode to unlock a phone are practically and conceptually identical. *Id*. at 1062 n. 1. The Fourth District concluded that, just as in *In re Subpoena*, the "state seeks the phone passcode not because it wants the passcode itself, but because it wants to know what communications lie beyond the passcode wall." *Id*. at 1062. The Fourth District held that in providing the passcode, the defendant in *G.A.Q.L.* "would be engaging in a testimonial act utilizing the 'contents of his mind' and demonstrating as a factual matter that he knows how to access the phone." *Ibid*. Therefore, the compelled production of the phone passcode is testimonial and proscribed by the Fifth Amendment as a violation of a defendant's right against compelled self-incrimination.

While the State made brief reference to the Second District Court's reliance on the foregone conclusion exception to the Fifth Amendment's protection against compelled self-incrimination at the hearing on its motion, it is worth noting that the

trial court did not rely on this exception in reaching its ruling in this case. Ex. F at 7–8. Petitioner argues that this Court, therefore, need not apply the foregone conclusion analysis in this case to determine whether the trial court's order constitute a departure from the requirements of the law. However, should this Court apply the foregone conclusion, Petitioner argues that it should reach the same conclusions that the Fourth District reached in *G.A.Q.L.* as opposed to those reached in *Stahl* by the Second District.

In *G.A.Q.L.*, the Fourth District recognized that "if the state can meet the requirements of the foregone conclusion exception, it may compel otherwise ostensibly self-incriminating testimonial production of information." *G.A.Q.L.*, 257 So. 3d at 1063 (citing *Fisher*, 425 U.S. at 411; *In re Subpoena*, 670 F.3d at 1345–46). However, in order to meet the exception, the State must demonstrate "with reasonable particularity 'that (1) the files exist in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic.'" *Ibid.* (quoting *In re Subpoena*, 670 F.3d at 1349 n. 28). Importantly, the Fourth District distinguished its application of the foregone conclusion exception to the compelled disclosure of a phone passcode from the Second District's application, stating:

> It is critical to note here that when it comes to data locked behind a passcode wall, **the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall** [. . .] To find otherwise would expand the contours of the foregone conclusion exception so as to swallow the

> protections of the Fifth Amendment. For example, 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.

Ibid. (emphasis added). This interpretation, as noted by the Fourth District, is consistent with the federal Eleventh Circuit Court of Appeals application of the foregone conclusion exception to the government's attempt to compel a defendant to provide a decryption key to an encrypted hard drive in *In re Subpoena*, where the Eleventh Circuit concluded that the foregone conclusion exception did not apply because the government had failed to demonstrate with reasonable particularity that the specific files sought by the government existed on the drive protected by the encryption. *In re Subpoena*, 670 F.3d at 1349. The Eleventh Circuit did not find that the foregone conclusion exception could be met simply by the government demonstrating with reasonable particularity that the decryption key or passcode existed and was in the defendant's possession or control.

In this case, the State did not present any testimony or physical evidence to prove the existence of the particular data or files sought behind the passcode wall. In fact, it remains unclear from the affidavit for the arrest warrant, the search warrant, the State's motion to compel the passcode, and the State's argument at the hearing what particular data or files the State is after; the State certainly has not demonstrated with reasonable particularity that the data or files exist on the phone

in law enforcement's possession. In comparison, the State in *G.A.Q.L.* provided the trial court with a sworn statement from the surviving passenger of a fatal car crash that there were text and Snapchat communications between herself and the defendant on the defendant's phone regarding his drinking leading up to his decision to drive, which resulted in the car crash. *G.A.Q.L.*, 257 So. 3d at 1060. This level of particularity, which was still determined to be insufficient by the Fourth District, stands in stark contrast to this case where it remains unclear what data or files the State is seeking and the search warrant is patently aimed at conducting a fishing expedition to sift through and collect all the data the phone can access regardless of the data's relevance to the charges in this case. Therefore, Petitioner argues that this Court should find the foregone conclusion exception has not been met and the State was not entitled to an order compelling Petitioner to provide a passcode to the phone.

The trial court should have arrived at the same conclusion as the Fourth District and denied the State's motion. The State is compelling the Petitioner to provide self-incriminating, testimonial information. Specifically, the State is compelling Petitioner to either tell law enforcement what the passcode to the phone is, enter the passcode himself, reduce the passcode to writing and provide it to law enforcement, or apply the correct fingerprint to the phone to unlock it. The State seeks this passcode not for the information of the passcode itself, but for the access

it provides to all of the data in the phone behind the passcode wall. By providing the sought-after information, Petitioner will be providing evidence, both explicit and implicit, that he knows the passcode, which fingerprint is necessary to open the phone, and/or that he is the person who setup the passcode and/or fingerprint needed to get past the passcode wall. Additionally, this compelled disclosure will "communicat[e] information that 'may lead to incriminating evidence'" and is therefore privileged even if "the information itself is not inculpatory." *G.A.Q.L.*, 257 So. 3d at 1062 (quoting *Doe*, 487 U.S. at 208 n. 6).

CONCLUSION

The trial court's determination in this case that the compelled disclosure of the passcode does not violate the Petitioner's Fifth Amendment right against compelled self-incrimination is contrary to law. The trial court departed from the essential requirements of the law by ordering that Petitioner be compelled to provide the passcode. This Court should find that the compelling Petitioner to provide the passcode constitutes compelling a testimonial disclosure in violation of the Fifth Amendment and vacate the trial court's order.

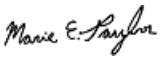
WHEREFORE Petitioner respectfully petitions this Honorable Court to grant the Petition and vacate the trial court's order compelling Petitioner to provide the passcode to the smart phone in this case.

Respectfully submitted,

ROBERT WESLEY
PUBLIC DEFENDER

By: 

Robert Adams
Florida Bar No. 107152
Assistant Public Defender

By: 

Marie Taylor
Florida Bar No. 1003697
Assistant Public Defender

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing has been furnished by e-service/e-mail/e-portal delivery to the Office of the State Attorney, PCF@sao9.org; the Office of the Attorney General, CrimAppDAB@myfloridalegal.com; and by mail delivery to the Honorable Judge Gail Adams, at the Orange County Courthouse, 425 N. Orange Ave., Orlando, FL 32801 on this the 7th day of March, 2019.

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that the foregoing brief, submitted in 14-point Times New Roman, complies with the font standards of Florida Rule of Appellate Procedure 9.100(*l*).

ROBERT WESLEY
PUBLIC DEFENDER

By: 

Robert Adams
Florida Bar No. 107152
Assistant Public Defender

Marie Taylor
Florida Bar No. 1003697
Assistant Public Defender

435 North Orange Avenue Suite 400
Orlando, Florida 32801
radams@circuit9.org
(407) 836-4887

IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FIFTH DISTRICT

JONATHAN DAVID GARCIA,

Petitioner,

v. CASE NO. 5D19-0590

STATE OF FLORIDA,

Respondent.

_____ /

RESPONSE TO AMENDED PETITION FOR WRIT OF CERTIORARI

COMES NOW, Respondent, State of Florida, through the undersigned Assistant Attorney General, pursuant to this Court's March 8, 2019, order to respond to Petitioner's Amended Petition for Writ of Certiorari, and states as follows:

STATEMENT OF THE CASE AND FACTS

Petitioner is seeking a writ of certiorari to reverse the trial court's order granting the State's Motion to Compel Phone Passcode. (Appx. G.)[1]

Petitioner was charged with throwing a deadly missile at, within, or into a building; two counts of aggravated stalking with a credible threat; criminal mischief with damage of more than $200; and criminal mischief. (Appx. C.) The State obtained a search warrant to search Petitioner's phone, a Samsung Galaxy Note 8,

[1] Respondent hereby incorporates Petitioner's amended appendix into this response.

which had been found outside the victim's broken window, and which the police believed held evidence relating to the aggravated stalking charges. (Appx. D.) Thereafter, the State filed a Motion to Compel Defendant's Phone Passcode, explaining that when a forensic download was attempted pursuant to the warrant, the officers were unable to unlock the phone. (Appx. E.) Therefore, the State requested that the court compel Petitioner to provide either his passcode or his fingerprint. (Appx. E.)

A hearing was held on the motion to compel, at which the State explained that as it related to passcodes, there was a circuit split between the Second and Fourth District Courts of Appeal. (Appx. F, pg. 4.) The State acknowledged that the existence of a warrant did not affect the case law. (Appx. F, pg. 5.) Defense counsel objected to the motion based on the Fourth DCA's decision in G.A.Q.L. v. State, 257 So. 3d 1058 (Fla. 4th DCA 2018), which held that compelling the defendant to disclose a password was testimonial and a violation of the Fifth Amendment. (Appx. F, pg. 5-6.) The State gave the court the opinion of the Second DCA – State v. Stahl, 206 So. 3d 124 (Fla. 2d DCA 2016), which held the opposite. (Appx. F, pg. 6.)

The court asked whether evidence in the phone dealt with the stalking charge. (Appx. F, pg. 7.) When the State responded that it did, the trial court granted the motion, and ordered Appellant to turn over his passcode. (Appx. F, pg. 7-8.) When

asked, the trial court found that Stahl was controlling, and found that the passcode was non-testimonial and pursuant to a warrant that had already been issued based on probable cause. (Appx. F, pg. 8.)

ARGUMENT

A writ of certiorari is a special mechanism wherein an appellate court can review the record of a pending case and evaluate the proceedings for regularity, such that the appellate court may "halt a miscarriage of justice" where no other remedy exists. Broward County v. G.B.V. Intern., Ltd., 787 So. 2d 838, 842 (Fla. 2001). It is not "intended to redress mere legal error, for common law certiorari—above all—is an extraordinary remedy . . . ." Id. Certiorari review may be utilized only where the petitioner "demonstrates a departure from the essential requirements of the law resulting in material injury for the remainder of the case that cannot be remedied on post-judgment appeal." Alascia v. State, Dept. of Legal Affairs, 135 So. 3d 402, 406 (Fla. 5th DCA 2014).

The Fifth Amendment provides that no person shall be compelled to be a witness against himself. Amend V, U.S. Const. This privilege protects a person from being incriminated by his own compelled testimonial communications. Doe v. United States, 487 U.S. 201, 207 (1988). In order to be testimonial, a communication must relate a factual assertion or disclose information. Id. at 210.

The Second District Court of Appeal examined the issue in State v. Stahl, 206 So. 3d 124 (Fla. 2d DCA 2016). The appellate court held that the communication (the passcode) was sought only for its content and that the content had no other value or significance because by providing the passcode, the defendant was not acknowledging that the phone contained incriminating evidence. Id. at 134. Although the passcode would allow the State to access the phone, and therefore access a source of potential evidence, the State already had a warrant to search the phone and the source of evidence had already been uncovered. Id. Further, the court was not inclined to believe that the Fifth Amendment provided greater protection to individuals who passcode protected their phones with a combination than to individuals who used a fingerprint as the passcode, as compelling an individual to place his finger on the phone would not be a protected act. Id. at 135.

The Second DCA also considered whether the foregone conclusion exception to the Fifth Amendment applied, which is where the State has established, through independent means, the existence, possession, and authenticity of the documents; therefore, by admitting the existence of the evidence requested, the accused adds little or nothing to the State's information because the information provided is a foregone conclusion. Id. In order for this doctrine to apply, the State must show with reasonable particularity, that at the time it sought the act of production, it

already knew that the evidence existed, that the evidence was in the possession of the accused, and that the evidence was authentic. Id. The court found that the question was not the State's knowledge of the contents of the phone, because the State was not requesting that the defendant provide the contents of the phone. Id. at 136. The State had established that the phone could not be searched without a passcode, thereby proving the existence of a passcode, and as the phone belonged to the defendant, the passcode was in the defendant's possession. Id. The court also found that the passcode was self-authenticating. Id. The Second DCA concluded that this was "a case of surrender and not testimony." Id. at 137.

The Fourth DCA disagreed in G.A.Q.L. v. State, 257 So. 3d 1058 (Fla. 4th DCA 2018). The appellate court noted that the compelled production of a passcode was more akin to revealing a combination than producing a key, because it probed into the content of one's mind and therefore implicated the Fifth Amendment. Id. at 1061. The very act of revealing a password asserts the fact that the defendant knows the password, and therefore the production is testimonial. Id.

The Fourth DCA also determined that the foregone conclusion exception did not apply because "when it comes to data locked behind a passcode wall, the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall." Id. at 1063. In making this determination, the

Fourth DCA relied on the reasoning of In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012). As the State failed to identify any specific file names or locations on the phone, the State failed to meet the "reasonable particularity" requirement of the exception. Id. at 1064. The Fourth DCA concluded that the production of the passcode was testimonial and that the requirements of the foregone conclusion exception were not met. Id. at 1065.

Recently, a federal district court declined to follow G.A.Q.L. in State v. Johnson, WD 80945, 2019 WL 1028462 (Mo. Ct. App. Mar. 5, 2019). The federal court agreed with cases that rejected reliance on In re Grand Jury, and held that the focus of the foregone conclusion exception is "the extent of the State's knowledge of the existence of the facts conveyed through the compelled act of production." Id. at *14. In this type of case, the focus of the foregone conclusion exception was the passcode. Id. Therefore, as the State demonstrated that they had knowledge of the existence, possession, and authenticity of the passcode, the compelled act of production was not testimonial and not protected by the Fifth Amendment privilege. Id.

Here, it cannot be said that the trial court departed from the essential requirements of law. As there is a circuit split on this issue, and this Court has not yet weighed in, the trial court did not depart from an essential requirement of law by

choosing one decision over the other. See First Liberty Ins. Corp. v. O'Neill, 190 So. 3d 136, 137 (Fla. 4th DCA 2016) ("Given the lack of binding authority from this court on the underlying issue, and given the split of authority between our sister courts on the underlying issue, we cannot say that the circuit court's apparent decision to follow the First District's authority was a departure from the essential requirements of the law at the time of its decision."). Therefore, the petition should be denied.

Petitioner urges this Court to adopt the reasoning in G.A.Q.L. and find that the production of the passcode is a violation of Petitioner's Fifth Amendment rights. Respondent disagrees, as Stahl is better reasoned. A "rule that the government can never compel decryption of a password-protected device would lead to absurd results." United States v. Spencer, 17-CR-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018). For example, it could lead to an absurd result in the instant case, where the State obtained a valid search warrant to search the device, but unless the phone is unlocked, the State will be unable to execute the warrant.

Moreover, Petitioner is not entitled to relief based on the reasoning of either G.A.Q.L. or Stahl because the State's Motion to Compel requested that Petitioner be required to produce either a passcode *or a fingerprint*. Although the trial court ordered that Petitioner provide the passcode, as that is all that was discussed at the

motion hearing, it is clear that the State would also accept Petitioner's fingerprint to unlock the phone. "Compelling an individual to place his finger on the iPhone would not be a protected act; it would be an exhibition of a physical characteristic, the forced production of physical evidence, not unlike being compelled to provide a blood sample or provide a handwriting exemplar." Stahl, 206 So. 3d at 135. See also Commonwealth v. Baust, 89 Va. Cir. 267 (2014) ("In this case, the Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same.").

Since the trial court properly relied on Stahl, and regardless, the trial court properly granted the State's motion to compel the production of Petitioner's fingerprint, the instant petition should be denied.

CONCLUSION

Based on the arguments and authorities presented herein, Respondent respectfully requests this Honorable Court deny Petitioner's Petition for Writ of Certiorari.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the above and foregoing Response has been furnished by the Florida Courts E-Filing Portal to counsel for Petitioner – Robert Adams (435 North Orange Avenue, Suite 400, Orlando, Florida

32801) at radams@circuit9.org, and Marie Taylor (435 North Orange Avenue, Suite 400, Orlando, Florida 32801) at mtaylor@circuit9.org, on April 1, 2019.

DESIGNATION OF E-MAIL ADDRESS

I HEREBY DESIGNATE crimappdab@myfloridalegal.com as my primary e-mail address and kaylee.tatman@myfloridalegal.com as my secondary address, pursuant to Rule 2.516, in this proceeding.

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that the size and style of type used in this response is 14-point Times New Roman, in compliance with Fla. R. App. P. 9.210(a)(2).

Respectfully submitted,
ASHLEY MOODY
ATTORNEY GENERAL

/s/ *Kaylee D. Tatman*
By: KAYLEE D. TATMAN
ASSISTANT ATTORNEY GENERAL
Florida Bar No. 0100052
Office of the Attorney General
444 Seabreeze Boulevard 5th Floor
Daytona Beach, FL 32118
crimappdab@myfloridalegal.com
kaylee.tatman@myfloridalegal.com
(386) 238-4990
(386) 238-4997 (Fax)

COUNSEL FOR RESPONDENT

IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
IN AND FOR THE FIFTH JUDICIAL DISTRICT

Case No.: 5D19-0590
Lower Case No.: 2018-CF-005112-A-OR

JOHNATHAN DAVID GARCIA,

Petitioner,

v.

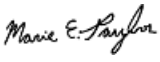
STATE OF FLORIDA,

Respondent.

REPLY TO THE RESPONDENT'S RESPONSE TO THE PETITION FOR WRIT OF CERTIORARI

ROBERT WESLEY
PUBLIC DEFENDER

Robert Adams
Florida Bar No. 107152
Assistant Public Defender



Marie Taylor
Florida Bar No. 1003697
Assistant Public Defender

Office of the Public Defender
435 N. Orange Ave., Suite 400
Orlando, FL 32801
407-836-4887
radams@circuit9.org

Counsel for Petitioner

INTRODUCTION

COMES NOW the Petitioner, Johnathan David Garcia, by and through the undersigned counsel, and hereby submits this Reply to the State's Response to Mr. Garcia's Petition for Writ of Certiorari. Petitioner does not address every argument made by the Respondent in this Reply; however, the absence of a rebuttal is not a waiver or abandonment of any claim or argument made in the Petition for Writ of Certiorari. For arguments not addresssed herein, Petitioner stands on the arguments presented in his Amended Petition for Writ of Certiorari.

ARGUMENT IN REPLY

The State's response to Mr. Garcia's petition presents four arguments Petitioner seeks to address in this reply: (1) that the trial court could not have departed from the essential requirements of the law due to the inter-district conflict regarding this issue and a lack of controlling precedent; (2) that providing the passcode is not testimonial; (3) that the foregone conclusion exception applies; and (4) that the Court should treat a fingerprint passcode differently if it is inclined to rule that a defednant cannot be compelled to provide a numerical passcode. Petitioner will address each of these arguments in this reply and demonstrate why Petitioner respectfully disagrees with the Respondent's analysis in all four.

In its response, the State raised an argument challenging the propriety of a petition for writ of certiorari as the vehicle for seeking this Court's review of the

trial court's order compelling Petitioner to provide a phone passcode. It appears both the Petitioner and Respondent agree that there is both inter-district conflict regarding this issue between the Second District's opinion in *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016) and the Fourth District's opinion in *G.A.Q.L. v. State*, 257 So. 3d 1058 (Fla. 4th DCA 2018), and a lack of controlling precedent from this Court. The trial court, mere moments after being handed both cases and without hearing either a presentation of evidence or full argument from the parties regarding the case law, ordered that the Petitioner provide the phone passcode to law enforcement and cited the *Stahl* case for its ruling. Amend. App. Ex. F at 6–7. The Respondent argues that the trial court did not depart from the essential requirements of the law in doing so.

The Respondent relies on the Fourth District's opinion in *First Liberty Ins. Corp. v. O'Neill*, 190 So. 3d 136 (Fla. 4th DCA 2016). In *First Liberty*, the petitioner filed an appeal seeking review of the trial court's order granting partial final judgment and granting the respondent's motion to amend the complaint to add a new claim. *Id.* at 136. The Fourth District treated the appeal as a petition for writ of certiorari and denied it, holding:

> Given the lack of binding authority from this court on the underlying issue, and given the split of authority between our sister courts on the underlying issue, we cannot say that the circuit court's apparent decision to follow the First District's authority was a departure from the essential requirements of the law at the time of its

> decision. Thus, because of that procedural posture, we are compelled to deny the petition for writ of certiorari **and not decide the underlying issue until a final appealable judgment is entered**.

Id. at 137 (emphasis added). This case is distinguishable for a few reasons. First, a writ of certiorari is used, as the Respondent noted, to "halt a miscarriage of justice **where no other remedy exists**." *Broward County v. G.B.V. Intern., Ltd.*, 787 So. 2d 838 (Fla. 2001) (emphasis added). The jurisdictional requirements for a writ of certiorari require the Petitioner to demonstrate that the trial court's erroroneous ruling: (1) constituted "'a departure from the essential requirements of the law;'" (2) "'result[s] in material injury for the remainder of the case;'" and (3) that injury "'cannot be corrected on postjudgment appeal.'" *G.A.Q.L.*, 257 So. 3d at 1060–61 (quoting *Reeves v. Fleetwood Homes of Fla., Inc.*, 889 So. 2d 812, 822 (Fla. 2004)).

It is apparent from the procedural posture summarized in the Fourth District's opinion that the petitioner in *First Liberty* did not have a claim that could not be remedied on postjudgment appeal. The petitioner in *First Liberty* had filed the pleading challenging the trial court's rulings as a postjudgment appeal; it was the Fourth District that chose to treat it as a petition for writ of certiorari since there had only been a partial final judgment rendered. *First Liberty*, 190 So. 3d at 136. Furthermore, the Fourth District's holding indicates that the Fourth District believed that the issue would be ripe and properly before the appellate court as a

postjudgment appeal after the trial court rendered a complete final judgment, indicating that the Fourth District believed that whatever injury might have been caused by a potentially erroneous ruling could be corrected on postjudgment appeal.

That is not the case here. The act of compelling the Petitioner to provide the passcode rings a bell that cannot be unrung. Once the State has acquired the passcode and gains access to the contents of the phone, that information will help the State prepare the presentation of its case at trial regardless of whether the contents of the phone are directly introduced. It can also aid the State in determining what avenues of pre-trial investigations the State should conduct. Finally, if the Petitioner provides a working passcode to the phone, the State would use the act of providing the passcode as evidence that Petitioner is the owner of the phone, that Petitioner had exclusive dominion or control over the phone leading up to the moment when it was left at the crime scene, and that Petitioner has knowledge of all the contents of the phone. Both the Second District and the Fourth District agreed that this constituted a harm that could not be remedied on postjudgment appeal when each court agreed to accept jurisdiction and review the rulings of the trial courts in *Stahl* and *G.A.Q.L.*

The State's response focuses on the fact that the trial court in this case faced inter-district conflict without direction from this Court and essentially had to

choose which precedent to adopt. The State argues that such a choice cannot constitute a departure from the essential requirements of the law. Petitioner respectfully disagrees. The "clearly established principle of law" (*Stahl*, 206 So. 2d at 129) from which the trial court departed is not one established by the Second or Fourth District Courts of Appeal. Rather it is the clearly established prohibition contained in the Fifth Amendment of the United States Constitution, applied to the State of Florida through the Fourteenth Amendment, which provides that "[n]o person shall be compelled in any criminal case to be a witness against himself." Amend. V, U.S. Const.

It is worth noting that, while the trial court in this case was put in the unenviable position of having to choose between two conflicting district court opinions, the trial court in *Stahl* had no precedent at all to rely on, and the trial court in *G.A.Q.L.* had relied on the Second District's holding in *Stahl*, which at the time was binding precedent. *See Pardo v. State*, 596 So. 2d 665 (Fla. 1992) ("This Court has stated that '[t]he decisions of the district courts of appeal represent the law of Florida unless and until they are overruled by this Court.' [. . .] Thus, in the absence of interdistrict conflict, district court decisions bind all Florida trial courts." (internal citations omitted)) Yet, the Second District accepted jurisdiction and granted certiorari review of the trial court's ruling in *Stahl*, and the Fourth District accepted jurisdiction and granted certiorari review of the trial court's

ruling in *G.A.Q.L.* The Petitioner argues that there is no blanket rule that a trial court is incapable of departing from the essential requirements of the law whenever two or more district courts have disagreed about what the essential requirements are.

Applying such a rule would lead to an absurd result whereby criminal defendants would be subjected to the consequences of erroneous rulings without adequate remedy on postjudgment appeal and without the ability to seek pre-judgment review through a petition for extraordinary writ. The defendant would never be able to have an interdistrict conflict resolved within this judicial district with precedent from this Court. While there may be certain circumstances in which a new legal concept leads to interdistrict conflict, when the district courts disagree over the application of longstanding principles such as those inscribed in our country's constitution, interdistrict conflict neither negates the fact that the issue in dispute is an essential legal principle, nor absolves the prejudice to the petitioner resulting from an erroneous ruling that cannot be remedied on postjudgment appeal.

Turning to the State's next argument in its response, the State asserts that between the Fourth District's holding in *G.A.Q.L.* and the Second District's holding in *Stahl* that the *Stahl* opinion is "better reasoned." Resp. at 7. The State does not specify why or in what way the Second District's opinion is "better

reasoned." Petitioner assumes that the Respondent is arguing for the application of the Second District's holding that the act of providing a passcode to a phone is not testimonial. *Stahl*, 206 So. 3d at 134–35. The Petitioner respectfully disagrees. As the State summarized in its response, the Second District determined that a compelled numerical passcode to a phone is "sought only for its content and that the content had no other value or significance because by providing the passcode, the defendant was not acknowledging that the phone contained incriminating evidence." Resp. at 4 (citing *Stahl*, 206 So. 3d at 134). Petitioner agrees that this is the proper test for determining whether the compelled speech or act is testimonial and therein protected by the Fifth Amendment, but argues that the Second District and the State have not properly applied this test.

By compelling a defendant to provide a phone passcode, the Court is not merely compelling the defendant to provide the passcode. The very act of providing the passcode provides the State in this case with circumstantial, if not direct, evidence that the Petitioner: either set up the passcode himself or, less likely, was given the passcode by someone else so that the defendant could use the phone, and in so doing exercised exclusive possession and control of the phone; was in possession of the phone at the time of the crime; downloaded and/or used the applications installed on the phone; and owned and/or used any email accounts, social media accounts, and/or messaging application accounts installed and logged

into on the phone. While the State in its response asserts that by compelling the Petitioner to provide the passcode, the act of providing the passcode in compliance with the trial court's order will have no evidentiary value in and of itself, the Petitioner has little doubt that the State at trial will introduce the fact that the Petitioner provided the passcode to law enforcement and argue that the jury should make the above-mentioned inferences about Petitioner's ability to do so. Petitioner believes this is especially true in his case where there has been no admission from him that the phone belongs to him, the State did not present any evidence at the hearing on its motion to compel to prove that Petitioner either owned the phone or knew its passcode, and there is no direct evidence that Petitioner was at the scene of the crime when the charged offense is alleged to have occurred.[1]

The Fourth District anticipated this kind of evidentiary value, noting that, in addition to "prob[ing] the contents of an individual's mind," the act of providing the passcode itself "asserts a fact: that the defendant knows the password." *G.A.Q.L.*, 257 So. 3d at 1062. The Fourth District similarly concluded that the state "seeks the phone passcode not because it wants the passcode itself, but because it wants to know what communications lie beyond the passcode wall. If the

[1] Additionally, Petitioner makes no factual representations in this Reply or in the Petition that he either owned the phone, knows its passcode, or would be able to unlock the phone with his fingerprints. Any references contained in this Petition or Reply that assume Petitioner would be able to provide either a numerical or fingerprint passcode are made by Petitioner's counsel for argument purposes only.

[defendant] were to reveal this passcode, he would be engaging in a testimonial act utilizing the 'contents of his mind' and demonstrating as a factual matter that he knows how to access the phone." *Id*. at 1062–63. This Court has previously recognized that this kind of derivative evidence is protected by the Fifth Amendment. *See State v. Mitrani*, 19 So. 3d 1065, 1068 (Fla. 5th DCA 2009) ("The privilege applies not only to answers that would themselves support a conviction, but also to those answers that might furnish a link in the chain of incriminating evidence.").

The State's next argument is that the foregone conclusion should apply if the compelled production of the passcode is deemed testimonial. The State recognized in its response that "[i]n order for this doctrine to apply, the State must show with reasonable particularity, that at the time it sought the act of production, it already knew that the evidence existed, that the evidence was in the possession of the accused, and that the evidence was authentic." Resp. at 4–5 (citing *Stahl*, 206 So. 3d at 135). The difference between the Second District's holding and the Fourth District's holding regarding this doctrine is that the Second District "found that the question was not the State's knowledge of the contents of the phone" but rather the State's knowledge of the existence of a passcode "because the State was not requesting that the defendant provide the contents of the phone" (Resp. at 5 (citing *Stahl*, 206 So. 3d at 136), whereas the Fourth District held that such an application

of the foregone conclusion "would expand the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment." *G.A.Q.L.*, 257 So. 3d at 1063. Additionally, in a concurring opinion, Judge Kuntz noted that the foregone conclusion doctrine cannot be applied to compel a defendant to tell the State or law enforcement the passcode to a phone:

> The foregone conclusion exception is a judicially created exception [. . .] It is not found with in the Fifth Amendment. It is also a doctrine of limited application [. . .] The Supreme Court has applied the foregone conclusion exception only when the compelled testimony has consisted of existing evidence such as documents.
>
> But, here, the State sought to compel the oral production of the requested information. The foregone conclusion exception has not been applied to oral testimony, and for good reason. [. . .] Requiring the accused to orally communicate to the government information maintained only in his mind would certainly compel oral testimony. [. . .] [T]he petition should be granted because the foregone conclusion exception is inapplicable to the compelled oral testimony sought in this case.

Id. at 1066 (internal citations omitted). The Petitioner believes this Court should adopt the Fourth District's analysis and argues that the Second District's analysis leads to an absurd result whereby the State needs to show only that law enforcement is in possession of a password-protected phone in order to compel a defendant to "be a witness against himself." Amend. V, U.S. Const.

Lastly, the Petitioner would draw the Court's attention to the dirth of evidence presented at the hearing on the State's motion to compel the passcode.

Even if the foregone conclusion doctrine can be applied in general, the State patently failed to show with "reasonable particularity" that it "already knew that the evidence existed," that "the evidence was in the possession of the accused," or "that the evidence was authentic." Resp. at 4–5. Instead, after hearing no evidence and only partial argument, the trial court made its ruling based only on the name of a charge in the information, the existence of a search warrant, and the bald, conclusory assertion by the State that the phone contains evidence relevant to the case. The State failed to establish the foregone conclusion exception in this case, and it should not be a basis for denying the Petition.

The State's final argument is that this Court does not need to address the question of whether compelling a defendant to provide a numerical passcode violates the Fifth Amendment because the State's motion to compel in this case calls for the Petitioner to provide either a numerical passcode or one of his fingerprints as a passcode. While it's true that the written motion called for either the numerical or fingerprint passcode, the trial court's order makes no such distinction. Instead the trial court's order calls for the Petitioner to provide the numerical passcode; therefore, Petitioner believes that certiorari review of the trial court's order requires the Court to address the issue of whether compelling a defendant to provide a numerical passcode violates the Fifth Amendment.

Additionally, Petitioner urges the Court to address this issue because an order requiring Petitioner to provide a fingerprint passcode is likely unworkable at this point. The smart phone in question is an iPhone. When a fingerprint scan is set up as an alternative to a numerical passcode on an iPhone, the fingerprint can be used to gain entry into the phone only under certain circumstances. There are limitations built into the iPhone software that require a user to enter a numerical passcode before the phone will accept a fingerprint scan. According to the manufacturer, Apple, a user must use a numerical password:

> - after you restart your iPhone, iPad, or Mac;
> - when more than 48 hours have passed from the last time you unlocked your device;
>
> [. . .]
>
> - when there have been more than five unrecognized Touch ID authorization attempts in a row; and
> - after you log out of your Mac.

About Touch ID advanced security technology – Apple Support, APPLE, INC. [US], https://support.apple.com/en-us/HT204587 (last visited April 11, 2019). As the phone was taken into law enforcement custody at the time of the offense several months ago, even if it has not been turned off or run out of battery power, more than 48 hours have certainly passed since the device was last unlocked. Therefore, a ruling from this Court limited to the question of whether the Petitioner can be compelled to provide his fingerprints without addressing whether he can be

compelled to provide a numerical passcode would almost certainly not provide a true resolution to the issue presented by this case. Such a ruling would ultimately lead to the State confirming that the phone will not accept a fingerprint anymore and a numerical passcode is required, which in turn will lead to Petitioner petitioning this Court to address the question of whether the court can compel a numerical passcode again.

Finally, the Petitioner disagrees with the State's argument that the trial court would not violate the Petitioner's Fifth Amendment rights by compelling Petitioner to provide his fingerprint(s) in lieu of a numerical passcode. The Petitioner recognizes that the Second District in *Stahl* held that compelling a defendant to provide a fingerprint in lieu of a numerical passcode "would not be a protected act; it would be an exhibition of a physical characteristic, the forced production of physical evidence, not unlike being compelled to provide a blood sample or provide a handwriting exemplar." *Stahl*, 206 So. 3d at 135. The act of providing his fingerprint(s) for a fingerprint passcode is testimonial for the same reasons that compelling a numerical passcode is testimonial. In order to comply with an order compelling Petitioner to provide the fingerprint passcode, the Petitioner has to choose one of his ten fingers as opposed to a series of ten digits, but the act of selecting a particular finger demonstrates that the Petitioner knows which fingerprint will unlock the device, which means that the act of compelling the

fingerprint passcode probes the Petitioner's mind. It also implies that the Petitioner knows the passcode to the device and provides evidence for all the same inferences Petitioner noted above in this reply that could be made with a compelled numerical passcode. In this way, the act of providing a fingerprint passcode is unique from the other instances in criminal law where a defendant is compelled to provide his fingerprint(s). As such, it should be treated differently, and considered a testimonial communication protected by the Fifth Amendment.

As the State noted in its response, the Second District "was not inclined to believe that the Fifth Amendment provided greater protection to individuals who passcode protect their phones with a combination than to individuals who used a fingerprint as the passcode[.]" Resp. at 4 (citing *Stahl*, 206 So. 3d at 135). While the Second District used this reasoning to conclude that numerical passcodes can be compelled because the Second District believed fingerprint passcodes could be compelled, Petitioner believes that the similarities between a numerical passcode's testimonial status and a fingerprint passcode's testimonial status should lead the Court to conclude that neither can be compelled.

CONCLUSION AND RELIEF SOUGHT

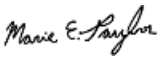
For the reasons discussed herein and in Mr. Garcia's Petition for Writ of Certiorari, Petitioner respectfully petitions this Honorable Court to grant certiorari review, find that the trial court departed from the essential requirements of the law, and reverse the trial court's order compelling Petitioner to provide the passcode to the phone.

Respectfully submitted,

ROBERT WESLEY
PUBLIC DEFENDER

By: 

Robert Adams
Florida Bar No. 107152
Assistant Public Defender

By: 

Marie Taylor
Florida Bar No. 1003697
Assistant Public Defender

Counsel for Petitioner

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing has been furnished by e-service/e-mail/e-portal delivery to the Office of the State Attorney, PCF@sao9.org, and to Kaylee D. Tatman, State Attorney General's Office, CrimAppDAB@myfloridalegal.com, kaylee.tatman@myfloridalegal.com; and by mail delivery to the Honorable Gail Adams, at the Orange County Courthouse, 425 N. Orange Ave., Orlando, FL 32801 on this the 11th day of April, 2019.

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that the foregoing brief, submitted in 14-point Times New Roman, complies with the font standards of Florida Rule of Appellate Procedure 9.100(*l*).

ROBERT WESLEY
PUBLIC DEFENDER

By: 

Robert Adams
Florida Bar No. 107152
Assistant Public Defender

Marie Taylor
Florida Bar No. 1003697
Assistant Public Defender

435 North Orange Avenue Suite 400
Orlando, Florida 32801
radams@circuit9.org
(407) 836-4887

P.O.#	VENDOR/SERVICE	AMOUNT
B31269	**Dell Marketing LP** Purchase of 8 Dell PowerEdge R740 servers. ▪ Alternate Contract ▪ Term: 5/02/2018 - 6/30/2018	**$162,637**
B16C65	**DNA Labs International, Inc.** Sexual Assault Kit testing fees. Adjustment to Purchase Order. ▪ Alternate Contract ▪ Term: 7/1/2017 - 6/30/2018	**$738,900**
PO1764622	**DSM Technology Consultants, LLC** Disaster Recovery Direct Connect Layer 2 1GB point to point circuit. ▪ State Term Contract ▪ Term: 5/18/2018 - 6/30/2021	**$129,600**
FDLE-003-18	**Georgia Tech Applied Research** Professional Information Technology and business consulting services for creating a National Incident-Based Reporting System Uniform Reporting System. Adjustment to Contract. ▪ Exempt ▪ Term: 8/1/2017 - 6/30/2019	**$816,000**
B308A8 **B2EB4B** **B303B3**	**Life Technologies Corp.** Reagents and supplies for Tampa Bay, Pensacola and Tallahassee Regional Operations Center Laboratories. ▪ Single Source ▪ One Time Purchase	**$171,278** **$124,630** **$308,908**
FDLE-023-18	**Porter Lee Corp.** Modifications to the existing Forensic Laboratory Information Management System to Microsoft .NET (Web) architecture. ▪ Single Source ▪ Term: 5/1/2018 - 4/30/2019	**$ 116,420**
FDLE-025-18	**Stacs DNA, Inc.** Support and maintenance to the DNA Database Sample Tracking and Control Software Database Enterprise. ▪ Single Source ▪ Term: 7/1/2018 - 6/30/2023	**$450,423**
FDLE-026-18	**Tri-Tech Forensics, Inc.** Software upgrade, subscription and maintenance of 9 Cellebrite Universal Forensic Extraction Devices (UFED) from UFED Touch to UFED Touch 2. ▪ Invitation to Bid ▪ Term: 6/7/2018 - 6/30/2021	**$ 343,699**

P.O.#	VENDOR/SERVICE	AMOUNT
B3534D	**A Child Is Missing** A Child is Missing notification and alert services. ▪ Exempt ▪ Term: 07/1/2018 - 6/30/2019	**$232,461**
B2E9FC	**AB Sciex, LLC** Maintenance and repair service for laboratory spectrometers located at Orlando and Tallahassee Regional Operations Centers. ▪ Single Source ▪ Term: 07/1/2018 - 6/30/2019	**$170,920**
CA-FDLE-17051000	**Affiliated Engineers, Inc.** Commissioning services for HVAC / mechanical work competitively procured by DMS for Tampa Bay Regional Operations Center repairs and maintenance project. ▪ Consultant's Competitive Negotiation Act ▪ Term: 5/4/2018 - 6/30/2020	**$101,670**
B35A06	**Bode Cellmark Forensics, Inc.** Sexual Assault Kit testing fees. ▪ Invitation to Bid ▪ Term: 7/1/2018 - 2/5/2019	**$354,116**
FDLE-005-19	**Cutcom Software, Inc.** FortifyFL Reporting System. ▪ Invitation to Negotiate ▪ Term: 7/31/2018 - 7/30/2021	**$254,400**
FDLE-011-19	**Diverse Computing, Inc.** eAgent Client Messaging System license, maintenance and technical support for FCIC, NCIC, NLETS and other messages. ▪ Single Source ▪ Term: 10/15/2018 - 10/14/2021	**$ 795,000**
FDLE-010-19	**Diverse Computing, Inc.** FCIC IPC XML Communications Library and Gateway Production Enterprise License with 24 x 7 server support. ▪ Single Source ▪ Term: 9/26/2018 - 9/25/2021	**$ 294,000**
PO1901087	**Diverse Computing, Inc.** Maintenance and after hours services for FCIC II Message Switch / Hot Files System. ▪ Single Source ▪ Term: 10/1/2018 - 6/30/2022	**$ 331,650**

B3711D	**DLT Solutions, LLC** Maintenance and technical support for Oracle database software. ▪ Alternate Contract ▪ Term: 7/1/2018 - 6/30/2019	**$640,766**
B35A0E	**DNA Labs International, Inc.** Non-Sexual Assault Kit testing fees. ▪ Alternate Contract ▪ Term: 7/1/2018 - 4/1/2019	**$242,950**
B35A12	**DNA Labs International, Inc.** Sexual Assault Kit testing fees. ▪ Alternate Contract ▪ Term: 7/1/2018 - 4/1/2019	**$652,325**
B3F071	**Emergent, LLC** Software license for Red Hat Enterprise Linux operating system and Jboss middleware platforms. ▪ Alternate Contract ▪ Term: 9/26/2018 - 6/30/2019	**$475,059**
B3E07A	**Garber Chrysler Dodge Truck, Inc.** Purchase of 7 Jeep Grand Cherokees. ▪ State Term Contract ▪ Term: One Time Purchase	**$168,861**
710:0226 **710:0170**	**Lee County Port Authority** Facilities 5-year lease renewal for 17,256 square feet of office space for Fort Myers Regional Operations Center. ▪ Lease Agreement ▪ Term: 11/1/2018 - 10/31/2023	**$2,418,859** **$9,082,845** Amounts reflect total lease beginning 11/1/1998
B3412B	**LexisNexis Risk Solutions FL, Inc.** 121 Software licenses for LexisNexis Accurint LE Plus. ▪ State Term Contract ▪ Term: One Time Purchase	**$113,329**
B3BDAF **B3DAA3** **B37DED** **B3653B** **B3C18F**	**Life Technologies Corp.** Reagents used for the Orlando, Pensacola, Tampa Bay and Tallahassee Regional Operations Centers. ▪ Single Source ▪ Term: One Time Purchase	**$166,383** **$101,749** **$220,194** **$294,594** **$317,344**

FDLE-009-19	**National Law Enforcement** NLETS access to International Justice Public Safety Network. ▪ Single Source ▪ Term: 10/1/2018 - 9/30/2021	**$180,000**
FDLE-024-18	**NCS Pearson, Inc.** Computer-based testing and facilitation for State Officer Certification Exam. ▪ Invitation to Negotiate ▪ Term: 2/14/2019 - 02/13/2024	**$2,214,000**
CP1031	**Pen Link, LTD** Software and maintenance support. ▪ Single Source ▪ Term: 2/14/2019 - 02/13/2024	**$130,837**
CP1031	**Presidio Networked Solutions, LLC** Maintenance and technical support for Cisco Enterprise routers, network switches, and VoIP phone systems. ▪ Alternate Contract ▪ Term: 6/1/2018 - 6/30/2019	**$173,587**
B35A14	**Sorenson Forensics, LLC** Sexual Assault Kit testing fees. ▪ Invitation to Bid ▪ Term: 07/1/2018 - 2/5/2019	**$295,350**
B37FC7	**Summit East Investors** Lodging for Special Agent Training Class 40. ▪ Direct Pay to Hotel / Motel ▪ Term: 09/9/2018 - 11/2/2018	**$170,640**
B37535	**Tampa Electric Company** Utility services for Tampa Bay Regional Operations Center. ▪ Exempt ▪ Term: 7/1/2018 - 6/30/2019	**$282,000**
CA-FDLE-17051000	**Wilder Architecture, Inc.** Architect-Engineer services competitively procured by Department of Management Services for the Tampa Bay Regional Operations Center repairs and maintenance project. ▪ Consultant's Competitive Negotiation Act ▪ Term: 5/4/2018 - 6/30/2020	**$139,020**

IT Staff Augmentation (Multiple Vendors)
Staff augmentation from multiple vendors to support various criminal justice applications and agency systems including: Sexual Offender / Predator Registry Improvement Project, Computerized Criminal History System Modernization project, FCIC, Automated Training Management System, Career Offender Application for Statewide Tracking, Missing Endangered Persons Information Clearinghouse, Firearm Eligibility System, Concealed Weapons Permitting, Revenue Accounting Management System and FDLE Modernization to Counter 21st Century Threats.

- State Term Contracts
- Term: Various

*Minority Vendor

B371FC	**3k Technologies, LLC**	**$ 170,000**
B37281	**3k Technologies, LLC**	**$ 156,000**
B3713D	**ADO Staffing, Inc.**	**$ 180,000**
B371EB*	**Advanced Systems Design, Inc.**	**$ 156,000**
B371E6*	**Advanced Systems Design, Inc.**	**$ 156,000**
B371DB*	**Advanced Systems Design, Inc.**	**$ 160,000**
B3716A	**Brandt Information Services, Inc.**	**$ 176,000**
B37294	**Brandt Information Services, Inc.**	**$ 152,000**
B3728E	**Brandt Information Services, Inc.**	**$ 152,000**
B371CC*	**Global Information Services, Inc.**	**$ 152,000**
B374B3*	**Global Information Services, Inc.**	**$ 196,000**
B37216*	**Global Information Services, Inc.**	**$ 160,000**
B37229*	**Global Information Services, Inc.**	**$ 162,000**
B37183*	**Global Information Services, Inc.**	**$ 180,000**
B37206*	**Global Information Services, Inc.**	**$ 165,000**
B371E1*	**Global Information Services, Inc.**	**$ 164,000**
B3729C*	**Global Information Services, Inc.**	**$ 160,000**
B3715C*	**Global Information Services, Inc.**	**$ 160,000**
B37155	**KLC Consulting, Inc.**	**$ 156,000**
B37201*	**Kyra Solutions, Inc.**	**$ 169,000**
B37187*	**Kyra Solutions, Inc.**	**$ 154,000**
B37284*	**Kyra Solutions, Inc.**	**$ 175,000**
B37282*	**Kyra Solutions, Inc.**	**$ 242,000**
B371F0*	**Kyra Solutions, Inc.**	**$ 164,000**
B37207*	**Kyra Solutions, Inc.**	**$ 168,000**
B3714B*	**Kyra Solutions, Inc.**	**$ 160,000**
B37159*	**Kyra Solutions, Inc.**	**$ 160,000**
B37170	**Optimum Software Solutions, Inc.**	**$ 152,000**
B37153	**Optimum Software Solutions, Inc.**	**$ 200,000**

B36EBB	**Optimum Software Solutions, Inc.**	**$ 158,000**
B37297	**Optimum Software Solutions, Inc.**	**$ 164,000**
B3727E	**Randstad Technologies, LLC**	**$ 170,000**
B372AA*	**Sanrose Information Services, Inc.**	**$ 140,000**
B3A4C8*	**Sanrose Information Services, Inc.**	**$ 156,000**
B3720B	**Seva Technologies, LLC**	**$ 158,000**
B37234	**Strategic IT Alignment Group, LLC**	**$ 158,000**
B371ED	**Strategic IT Alignment Group, LLC**	**$ 156,000**
B3727B*	**System Soft Technologies, LLC**	**$ 160,000**
B3720D*	**System Soft Technologies, LLC**	**$ 160,000**
B37286*	**System Soft Technologies, LLC**	**$ 150,000**
B37279	**Tal Search Group, Inc.**	**$ 180,000**
B371C9	**Tal Search Group, Inc.**	**$ 156,000**
B3728F	**Tal Search Group, Inc.**	**$ 150,000**
B37126*	**Vitaver and Associates, Inc.**	**$ 193,000**

P.O.#	VENDOR/SERVICE	AMOUNT
B3FE2A	**Unisys Corp.** Maintenance and support for Libra 460 system. ▪ State Term Contract ▪ Term: 11/1/2018-1/31/19	**$326,925**
B4084E	**Seva Technologies, LLC** Information Technology staff augmentation – Systems Analyst for Sexual Offender/Predator Improvement Project. ▪ State Term Contract ▪ Term: 10/22/2018-06/30/2019	**$117,936**
B4109B	**SHI International Corp.** Microsoft SQL Server 2017 Enterprise – 12 Linux licenses. ▪ State Term Contract ▪ Term: One Time Purchase	**$101,392**
B3E075	**Coggin Chevrolet, LLC** Purchase of 8 Chevrolet Traverses. ▪ State Term Purchase ▪ Term: One Time Purchase	**$213,024**
B43B36	**Coggin Chevrolet, LLC** Purchase of 4 Chevrolet Traverses. ▪ State Term Purchase ▪ Term: One Time Purchase	**$106,512**
B44282	**ESCAL Institute of Advanced Technologies, Inc.** Training for Windows Forensic Analysis. ▪ Single Source ▪ Term: 12/5/2018-6/30/2019	**$219,520**
B45026	**Life Technologies Corp.** Upgrade Genemapper ID-X software for Life Technologies 3500 model Genetic Analyzers. ▪ Single Source ▪ Term: 12/20/2018-06/30/2019	**$836,936**
FDLE-018-19	**Parabon Nanolabs** DNA Genetic Geneology, DNA Phenotyping and Kinship Inference Analysis. ▪ Single Source ▪ Term: 11/16/2018-11/15/2019	**$130,000**
B455DF	**Life Technologies Corp.** Reagents for Orlando Regional Operations Center Laboratory. ▪ Single Source ▪ Term: One Time Purchase	**$166,760**

B414BC	**Life Technologies Corp.** Reagents for Tallahassee Regional Operations Center Laboratory. ▪ Single Source ▪ Term: One Time Purchase	**$332,953**
B4011A	**Life Technologies Corp.** Reagents for Tampa Bay Regional Operations Center Laboratory. ▪ Single Source ▪ Term: One Time Purchase	**$202,278**

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been furnished via the e-Filing Portal to the Office of the Attorney General, The Capitol, PL-01, Tallahassee, FL 32399, amit.agarwal@myfloridalegal.com, jeffrey.desousa@myfloridalegal.com, christopher.baum@myfloridalegal.com, and jason.hilborn@myfloridalegal.com on this the 14th day of June, 2021.

ROBERT WESLEY
Public Defender

By: 

ROBERT THOMPSON ADAMS IV
Florida Bar No. 107152
Assistant Public Defender
435 North Orange Avenue Suite 400
Orlando, Florida 32801
radams@circuit9.org
(407) 270-0402