

**IN THE DISTRICT COURT OF APPEAL
FOR THE FIRST DISTRICT, STATE OF FLORIDA**

MATTHEW TYLER POLLARD,

Petitioner,

v.

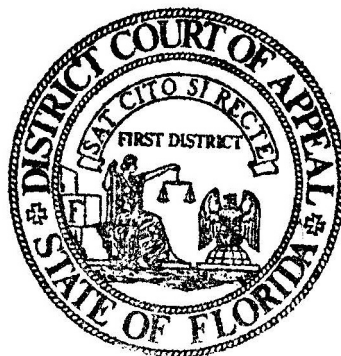
STATE OF FLORIDA,

Respondent.

Case No. 1D18-4572

NOTICE TO INVOKE DISCRETIONARY JURISDICTION

Notice is given that the State of Florida, Respondent, invokes the discretionary jurisdiction of the Florida Supreme Court to review the decision of this Court rendered on December 23, 2019. The decision is within the Florida Supreme Court's jurisdiction because this Court passed on two questions that it certified to be of great public importance. Ex. A, at 1; Art. V, s. 3(b)(4). The decision also "expressly and directly conflicts with a decision of another district court of appeal . . . on the same question of law." Art. V, s. 3(b)(3), Fla. Const.; *see* Ex. A, at 6-9 (Winokur, J., dissenting); *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016).



I CERTIFY THE ABOVE TO BE A TRUE COPY
KRISTINA SAMUELS, CLERK
FIRST DISTRICT COURT OF APPEAL

By: _____

Deputy Clerk

RECEIVED, 01/22/2020 04:50:29 PM, Clerk, Supreme Court
RECEIVED, 01/22/2020 01:58:35 PM, Clerk, First District Court of Appeal

Respectfully submitted.

ASHLEY MOODY
ATTORNEY GENERAL

/s/ Christopher J. Baum
Christopher J. Baum (FBN 1007882)
DEPUTY SOLICITOR GENERAL

Amit Agarwal (FBN 125637)
SOLICITOR GENERAL
Office of the Attorney General
State of Florida
1 SE 3rd Ave Suite 900
Miami, FL 33131
(786) 792-6269
(850) 410-2672 (fax)
christopher.baum@myfloridalegal.com

Attorney for Respondent

EXHIBIT A

FIRST DISTRICT COURT OF APPEAL
STATE OF FLORIDA

No. 1D18-4572

MATTHEW TYLER POLLARD,

Petitioner,

v.

STATE OF FLORIDA,

Respondent.

Petition for Writ of Prohibition—Original Jurisdiction.

December 23, 2019

ON MOTION FOR REHEARING AND CERTIFICATION

MAKAR, J.,

The State has filed a motion for rehearing and certification, which we grant in part by certifying the following questions of great public importance:

WHAT IS THE PROPER LEGAL INQUIRY WHEN THE STATE SEEKS TO COMPEL A SUSPECT TO PROVIDE A PASSWORD TO THE SUSPECT'S CELLPHONE IF THE SUSPECT HAS NOT PREVIOUSLY GIVEN UP HIS FIFTH AMENDMENT PRIVILEGE IN THE PASSWORD? WHAT LEGAL STANDARD APPLIES IN DETERMINING WHETHER THE FOREGONE CONCLUSION APPLIES TO COMPELLED PRODUCTION OF PASSWORDS IN THESE SITUATIONS?

The State's motion for rehearing is narrow and limited solely to our jurisdiction in this case and seeks no substantive changes on the merits of the constitutional issue. Concluding that jurisdiction exists, we deny the motion.

The State's motion for certification of conflict does not ask for any substantive changes to our opinion either. It urges, instead, that our opinion conflicts with the decision in *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016), because it adopted the approach in *G.A.Q.L. v. State*, 257 So. 3d 1058, 1062 (Fla. 4th DCA 2018), a case that disagreed with *Stahl* but neither certified conflict nor a question of great public importance. Certification presents a close question, but the factual differences in those cases and this case, such as whether a defendant has given up his testimonial privilege, make them distinguishable such that no *direct* conflict exists within the meaning of article V, section 3(b)(4), Florida Constitution. We therefore deny the motion for certification of conflict. That said, the proper approach to analyzing compelled password production needs clarification, which is why a question of great public importance has been certified.

Despite the narrow focus of the State's motion, our dissenting colleague presents many pages of arguments—old and new—that amount to a second opinion on the merits. Tellingly, our colleague's almost exclusive focus is on the Fourth Amendment and probable cause despite *no party mentioning either of them* in their merits briefs and the State advancing no argument on such matters in its motion for rehearing and certification. And whether the probable cause affidavit (which sought to seize broad categories of information from the cellphone—without identifying any specific item—on the basis that criminals use cellphones) was proper or a fishing expedition matters not; we fail to see how the issuance of a subpoena or warrant—whether carefully drawn or a fishing expedition—negates the Fifth Amendment's protections, which are the focus of this case.

If anything, the relationship that exists between the Fifth Amendment right against compelled personal disclosures and its neighboring and complementary Fourth Amendment right against unreasonable searches and seizures counsels in favor of protection

against governmental overreach into individual autonomy in criminal cases. LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT 431 (1968) (“With good reason the Bill of Rights showed a preoccupation with the subject of criminal justice. The framers understood that without fair and regularized procedures to protect the criminally accused, there could be no liberty.”). As expressed in our original opinion, the expansion of governmental powers to compel disclosures of personally-held information to search person’s homes and personal effects, as reflected in *Stahl* and our dissenting colleague’s view, is the antipode of the original understanding of the Fifth Amendment, which protected individual freedom by prohibiting compelled disclosures used to incriminate an accused. See Donald Dripps, *Self-Incrimination*, in THE HERITAGE GUIDE TO THE CONSTITUTION 437-439 (David F. Forte & Matthew Spalding eds., 2d ed. 2014); see also LEVY, at 432 (“Above all, the Fifth Amendment reflected [the framers’] judgment that in a free society, based on respect for the individual, the determination of guilt or innocence by just procedures, *in which the accused made no unwilling contribution to his conviction*, was more important than punishing the guilty.”) (emphasis added). At its core, the debate in *Stahl*, *G.A.Q.L.*, and this case is about which vision of the right against compelled testimony prevails: those of the Founders who erred on the side of personal liberty or those who defend state powers to extract testimony and see no problem in “merely compel[ling a defendant] to unlock [a] phone by entering the passcode himself.”

JAY, J., concurs; WINOKUR, J., concurs in part and dissents in part with opinion.

Not final until disposition of any timely and authorized motion under Fla. R. App. P. 9.330 or 9.331.

WINOKUR, J., concurring in part and dissenting in part.

I concur in the Court’s decision to certify questions of great public importance to the Florida Supreme Court. I believe that it is appropriate to add some additional insight into why this question is important enough to merit certification. I also concur in the decision to deny rehearing. However, I dissent from the decision to deny certification of conflict with *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016).

Great Public Importance

I find that the State’s motion reveals that one of the central issues in this case is the contention that the State’s attempt to access data on Pollard’s phone “amount[s] to a mere fishing expedition.” *Pollard v. State*, 44 Fla. L. Weekly D1573, D1576 (Fla. 1st DCA June 20, 2019) (citing *G.A.Q.L. v. State*, 257 So. 3d 1058, 1064 (Fla. 4th DCA 2018)). The use of this phrase suggests that the State had nothing but sheer hope that the phone contained evidence of a crime. But if this were true, the State could not have obtained a warrant to seize and search the phone. In order to obtain the search warrant, police had to demonstrate to a magistrate that it had probable cause to believe that the phone contained evidence of a crime; that is, that there was a “reasonable probability that contraband will be found” on the phone. *Pagan v. State*, 830 So. 2d 792, 806 (Fla. 2002). The State met this standard by introducing evidence—including a co-defendant’s admission that the robbery Pollard allegedly participated in was planned via text message—indicating that incriminating evidence existed on Pollard’s phone. No “mere fishing expedition” was involved.

The majority draws this language from *G.A.Q.L. v. State*, which in turn cited *United States v. Hubbell*, 530 U.S. 27, 44 (2000). But in *Hubbell*, the Government sought information by subpoena, not by search warrant. The Government never had to make a showing that it had probable cause to seize the disputed documents; it merely issued a grand jury subpoena to Hubbell. *Id.* at 31. The Supreme Court approved the District Court’s characterization of the subpoena as a “fishing expedition” because the Government could not state with “reasonable particularity a prior awareness that the [documents] sought existed and were in Hubbell’s possession.” *Id.* at 32-33. In that context, this finding meant the demand for documents violated Hubbell’s rights,

because the Government was merely compelling Hubbell to provide incriminating information without knowing what those documents might reveal, rather than seeking documents it could already identify without forcing Hubbell to produce them. This is why the Court characterized the Government's demand as a "fishing expedition."

Nothing of the sort occurred here. The State did not merely issue a subpoena for Pollard's phone with a hunch that it might provide incriminating information. Rather, the State introduced evidence showing, to a magistrate's satisfaction, that probable cause existed that Pollard's phone contained evidence of a crime. This evidence was what they sought, not the passcode that is the subject of this petition.

It is true that the *Hubbell* Court wrote that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Id.* at 43 (emphasis supplied). The majority opinion suggests that this passage states a general rule that a requirement to tell police a "combination" violates the right against self-incrimination. I submit this claim misreads *Hubbell*. The State here was not asking Pollard to "assemble" anything. It already had probable cause that incriminating information was located on the phone. Compelling Pollard to provide the passcode in order to access this incriminating information is more like forcing him to surrender a key than embarking on a "fishing expedition" for unknown information.¹ In short, I believe that the characterization of the State's request as a "fishing expedition," and its relation to the foregone conclusion exception, amplify why this case is of great

¹ It is worth repeating that the opinion does not address whether it would be improper for the State to merely compel Pollard to unlock the phone by entering the passcode himself. And if this is not improper, then the demand for the passcode, which accomplishes the same result, cannot be deemed a "fishing expedition."

public importance, especially since the same point was made in *G.A.Q.L.*²

Certification of Conflict

In *Stahl*, the Second District concluded that the foregone conclusion exception applied to permit compulsion because the State proved that the passcode existed, the defendant knew it, and the passcode was self-authenticating:

To know whether providing the passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has established that it knows with reasonable particularity that the *passcode* exists, is within the accused's possession or control, and is authentic. The question is not the State's knowledge of the contents of the phone; the State has not requested the contents of the phone or the photos or videos on Stahl's phone. The State established that the phone could not be searched without entry of a passcode. A passcode therefore must exist. It also established . . . that the phone was Stahl's and therefore the passcode would be in Stahl's possession. That leaves only authenticity. And as

² Admittedly, it is unclear whether the majority still adheres to this view. In its opinion, the majority ruled that the State's failure to "describe with reasonable particularity" the information it sought on Pollard's phone made its request a "mere fishing expedition," which invalidated the applicability of the foregone conclusion exception to Fifth Amendment rights. *Pollard*, 44 Fla. L. Weekly at D1576. But in its opinion on rehearing, the majority contends "whether the probable cause affidavit . . . was proper or a fishing expedition matters not," and that the specificity of the warrant is irrelevant to Pollard's Fifth Amendment protections. Maj. op. on rehearing at 2. If the majority now contends that a supposed lack of specificity of the warrant does not matter to the outcome of this case, then I agree. However, without this fact, the foregone conclusion exception requires disclosure.

has been seen, the act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating—no other means of authentication may exist. If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.

206 So. 3d at 136 (citations omitted).

Similarly here, it is undisputed that the passcode existed and that Pollard knew it; the answers to the determinative questions in *Stahl* are the same. However, the majority applied a different analysis by questioning how precisely the State could identify the evidence it sought on the phone, rather than by focusing on the passcode as *Stahl* did. The majority consequently came to a different conclusion, finding that “unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communications, data and images ‘amount[s] to a mere fishing expedition.’” *Pollard*, 44 Fla. L. Weekly at D1576 (quoting *G.A.Q.L.*, 257 So. 3d at 1064). Had this Court applied the holding of *Stahl*, we would have denied the petition for certiorari, but the majority employed a different analysis and granted certiorari. As such, the majority’s opinion directly conflicts with *Stahl*.

The majority attempted to distinguish *Stahl* by stating that Stahl “initially agreed to allow police to search the phone, thereby inferring his knowledge of the passcode and its authenticity,” finding that the Second District held “that the suspect’s actions disclosed or authenticated the password sought (here by Stahl initially agreeing to allow police to access the phone),” thus making authentication a foregone conclusion, and concluding that Pollard, conversely, had never “previously given up his privilege in the password sought.” *Id.* at D1575. This argument fails for two reasons.

First, Stahl initially consented to a search of his cellphone before withdrawing his consent after police recovered the

cellphone from his house, thus requiring the State to obtain a search warrant. *Stahl*, 206 So. 3d at 128. The State then found that it could not view the contents of the phone and moved to compel Stahl to produce his passcode. *Id.* It is clear that Stahl's initial consent was a waiver of his Fourth Amendment rights against unreasonable searches, requiring the State to obtain a search warrant. If Stahl had maintained his consent and handed his phone to the State, the State still could not have viewed the information inside it without obtaining the passcode. Thus, the majority's assertion that Stahl "had previously given up his privilege in the password sought," *Pollard*, 44 Fla. L. Weekly at D1575, is without support and further conflates the Fourth Amendment and Fifth Amendment protections. Regardless, *even if* Stahl had stated that he would provide his passcode before changing his mind, the majority provides no logical reason why we would use a passcode-centric approach to the foregone conclusion exception then, while utilizing a completely different content-centric approach when a defendant like Pollard simply admits that he knows the passcode to his phone (but does not briefly say he will provide it before changing his mind). This factual distinction is unsupported and would be meritless if it was.

Second, contrary to the majority opinion's assertion, *Stahl* did not hold that the authenticity requirement was satisfied because he "disclosed or authenticated the password sought" when he initially provided consent to search his phone; as discussed above, he never mentioned a passcode when he waived his Fourth Amendment rights. *Id.* The Second District found that the foregone conclusion exception "cannot be seamlessly applied to passcodes and decryption keys" without "recogniz[ing] that the technology is self-authenticating—no other means of authentication may exist." *Stahl*, 206 So. 3d at 136. *Stahl* concluded that "[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." *Id.* Despite the majority's contention, *Stahl* is clear that its ruling is based on the passcode's self-authentication rather than any purported disclosure of the password. This ruling is in clear conflict with the majority's conclusion that "simply because a compelled password unlocks a cellphone after the fact doesn't make it authentic ex ante." *Pollard*, 44 Fla. L. Weekly at D1575.

The majority decision is in direct conflict with *Stahl*, so I would grant the State’s motion to certify conflict.³

Stacy A. Scott, Public Defender, and Logan P. Doll, Assistant Public Defender, Gainesville, for Petitioner.

Ashley Moody, Attorney General, Benjamin L. Hoffman, Assistant Attorney General, Edward Wenger, Chief Deputy Solicitor General, and Christopher Baum, Deputy Solicitor General, Tallahassee, for Respondent.

³ The majority suggests I have turned my back on “the Founders” and their commitment to personal liberty and sees my position as “defend[ing] state powers to extract testimony.” Maj. op. on rehearing at 2-3. I disagree with the majority that this case turns on one’s “vision” of the Fifth Amendment. Rather, it turns on the application of the foregone conclusion exception established by the United States Supreme Court, which we cannot contradict even if it conflicts with our personal conception of the United States Constitution.

EXHIBIT B

FIRST DISTRICT COURT OF APPEAL
STATE OF FLORIDA

No. 1D18-4572

MATTHEW TYLER POLLARD,

Petitioner,

v.

STATE OF FLORIDA,

Respondent.

CORRECTED PAGES: pg 11
CORRECTION IS
UNDERLINED IN RED
MAILED: June 27, 2019
BY: KMS

Petition for Writ of Prohibition—Original Jurisdiction.

June 20, 2019

MAKAR, J.

To what extent does the Fifth Amendment right against self-incrimination protect a suspect in a criminal case from the compelled disclosure of a password to an electronic communications device in the state's possession? Courts differ in their legal analysis of this question, resulting in no consensus in state and federal courts; indeed, different approaches currently exist between two Florida appellate courts on the topic. In this case, we conclude that the proper legal inquiry on the facts presented is whether the state is seeking to compel a suspect to provide a password that would allow access to information the state knows is on the suspect's cellphone and has described with reasonable particularity.

Matthew Tyler Pollard was arrested and charged with armed robbery of two victims who were misled into believing they were buying drugs. Pursuant to a warrant, the state seized an iPhone® from Pollard’s car and filed a motion to compel Pollard to disclose the phone’s passcode so that it could access broad categories of encrypted information on the cellphone. The information sought was described in general terms and broad categories in the investigating detective’s affidavit in support of the search warrant:

- Call/text/communication history on and between June 19, 2018 and June 25, 2018.
- Content of communications on and between June 19, 2018 and June 25, 2018.
- Picture(s) of narcotics, money, firearms.
- Written information about the illegal purchase, possession, and sale of illegal narcotics, and or plans of a robbery on and between June 19, 2018 and June 25, 2018.
- Activity listed in phone applications: Facebook, Facebook Messenger, etc., concerning buying, selling, or possessing illegal narcotics and or planning a robbery on and between June 19, 2018 and June 25, 2018.

The affidavit did not state the existence or content of any specific text, picture, call or other particular information. It noted, however, that “it was reasonable to believe” that a co-defendant, Draven Rouse, had “communicated with Pollard via cell phone” both prior to and on the day of the robbery, presumably to coordinate the robbery. Based on his training and experience, the detective stated that persons in “criminal enterprises” sometimes use cellphones to communicate and coordinate activities with accomplices, to document criminal activities, and to compile contacts useful in a criminal investigation; he did not, however, identify any specific item that was on Pollard’s cellphone, only that the state wished to seize from the cellphone all items in the categories of information listed above.

Accessing the cellphone’s content required a passcode, which the state in a one-page motion sought to compel from Pollard. The state’s motion—and the trial court’s favorable ruling—relied

exclusively on *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016), which upheld the compelled production of a cellphone’s passcode over a defendant’s Fifth Amendment objection that doing so violated his right not to testify as to the “contents of his mind,” i.e., knowledge of the passcode itself. The trial court relied on *Stahl*, even though it arose in another district and (as discussed later) involved different facts, because no other Florida court had weighed in on the general topic at that time. *Pardo v. State*, 596 So. 2d 665, 666 (Fla. 1992) (“in the absence of interdistrict conflict, district court decisions bind all Florida trial courts.”).

Based on *Stahl*, the trial court held the state established that the cellphone was Pollard’s, that it was password protected, and that if the password compelled from Pollard made the cellphone’s content accessible, the password was deemed authentic, thereby requiring Pollard to provide the password. Quoting *Stahl*, the trial court also noted that the state had established by independent means the “existence, possession, and authenticity of the documents’ it seeks to recover from [Pollard’s] phone.” 206 So. 3d at 135. It concluded that the “State already knows the information it is seeking [Pollard] to produce and why.” The trial court did not identify any specific documents or information in this regard, but noted that “at [a] minimum, text messages” were part of the coordinated effort to conduct the robbery. No limits were placed on the scope of the search of the contents of the cellphone, but the state was prohibited from using the compelled production of Pollard’s password as evidence at trial; no limitation was put on use of the documents and information that might be discovered. The password was placed in a sealed and confidential file pending resolution of Pollard’s petition for writ of prohibition, which seeks to prevent the compelled use of the embargoed password. We treat the petition as a petition for writ of certiorari, which requires a departure from the essential requirements of the law that results in material injury that cannot be corrected post-judgment. Art. V, § 4(b)(3), Fla. Const. (2019); *Stahl*, 206 So. 3d at 129; *Grant v. State*, 832 So. 2d 770, 771 (Fla. 5th DCA 2002).

Courts nationwide are struggling to find common legal ground on the constitutionality of compelled password production under the Fifth Amendment and its application in specific cases. U.S. Const. amend. V. (“No person . . . shall be compelled in any

criminal case to be a witness against himself”); *see also* Art. I, § 9, Fla. Const. (2019) (same); *see generally* Marjorie A. Shields, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*, 84 A.L.R. 6th 251 (2019) (compiling Fifth Amendment cases involving “compelled disclosure of an individual's password, means of decryption, or unencrypted copy of electronically stored data.”).

The Fifth Amendment forbids a governmentally-compelled *testimonial* communication (or act) that tends to incriminate the communicator (or actor). *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1341 (11th Cir. 2012). “The touchstone of whether an act of production is testimonial is whether the government compels the individual to use ‘the contents of his own mind’ to explicitly or implicitly communicate some statement of fact. *Id.* at 1345 (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)). Forcing a defendant to disclose a password, whether by speaking it, writing it down, or physically entering it into a cellphone, compels information from that person’s mind and thereby falls within the core of what constitutes a testimonial disclosure. In this case, Pollard was compelled to act in a testimonial manner by disclosing a password known only in his mind. In this type of password compulsion case, the law is unsettled as to whether a “foregone conclusion” exception might apply, i.e., where the government knows that identifiable documents exist under a defendant’s control such that obtaining them via a compelled disclosure of a password is a mere formality and thereby non-testimonial. The Supreme Court has approved the exception’s use but not in the context of a compelled passcode disclosure. *See G.A.Q.L.*, 257 So. 3d at 1066 (Fla. 4th DCA 2018) (“The Supreme Court has applied the foregone conclusion exception only when the compelled testimony has consisted of existing evidence such as documents.”) (Kuntz, J., concurring in result).

Florida is no exception in the national judicial debate over compelled password production. Since the trial court’s ruling, the Fourth District issued its opinion in *G.A.Q.L. v. State*, 257 So. 3d 1058, 1062 (Fla. 4th DCA 2018), which seemingly conflicts with the approach taken in *Stahl* as to the foregone conclusion

exception and allows compelled production of information where the testimonial value of doing so is negligible. As a result, two different analytical methods currently exist in Florida, though both apply the same two-step framework, which asks (a) is the compelled production of the password a testimonial and potentially incriminating act, and, if so, (b) is the compelled password production nonetheless permissible under the foregone conclusion exception because its testimonial value is inconsequential due to the state already knowing of the existence of the requested information. *Id.* at 1063 (“Under this exception, an act of production is not a violation of the Fifth Amendment—even if it conveys a fact—if the state can show with reasonable particularity that, at the time it sought to compel the act of production, it already knew of the materials sought, thereby making any testimonial aspect a foregone conclusion.”); *Stahl*, 206 So. 3d at 135 (“That is, by implicitly admitting the existence of the evidence requested and that it is in the accused's possession the accused ‘adds little or nothing to the sum total of the Government's information’; the information provided is a foregone conclusion.”) (quoting *Fisher v. United States*, 425 U.S. 391, 411 (1976) (“The existence and location of the [tax-preparation] papers are a foregone conclusion” such that taxpayer’s compelled production of them “adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons ‘no constitutional rights are touched. The question is not of testimony but of surrender.’”)) (citation omitted); see generally Fern L. Kletter, *Construction and Application of "Foregone Conclusion" Exception to Fifth Amendment Privilege against Self-Incrimination*, 25 A.L.R. Fed. 3d Art. 10 (2017) (compiling cases that discuss the foregone conclusion exception).

For example, if the central feature in a criminal case is *what* files are on a cellphone, and the state can establish that a defendant’s cellphone contains files that are described with “reasonable particularity,” the compelled production of the password to access those files (but only those files) does no damage to the defendant’s constitutional right against self-incrimination where sufficient evidence establishes that it is his phone on which the files reside. In contrast, if a central feature of a criminal case is *who* owns a seized cellphone or has the code to access it,

compelling a defendant to provide a password may be testimonial and incriminating because it proves an unknown fact, i.e., who is the cellphone's owner or who can access it. For instance, if an employee was alleged to have broken into a password protected computer system, and caused cyber-harm therein, evidence as to his ability to access the system (i.e., possession of the password) would be incriminating because it supports the ability to access the system.

In *Stahl*, a video voyeurism case, the defendant used a cellphone to take video under a customer's skirt, was identified via store surveillance video, and arrested. After his locked cellphone was produced pursuant to a search warrant, he admitted it was his cellphone and initially agreed to permit police to search it for images, but he changed his mind, resulting in the state's request to compel its password. Under those circumstances, the Second District concluded that compulsion of the passcode was not a Fifth Amendment violation under the foregone conclusion exception. The three-part test for the foregone conclusion exception requires that the state "must show with reasonable particularity that, at the time it sought the act of production, it already knew the evidence sought existed, the evidence was in the possession of the accused, and the evidence was authentic." *Stahl*, 206 So. 3d at 135 (citing *In re Grand Jury Subpoena*, 670 F.3d at 1344 ("Where the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available.") (footnote omitted)).

Stahl's application of foregone conclusion exception focused on disclosure of the *password* itself, rather than the *information* that access to the cellphone would produce. *Stahl* viewed the forced disclosure of the *password* as non-testimonial because the existence, custody, and authenticity of the *password* were a "foregone conclusion" under the facts of that case. No one disputed that the cellphone was the defendant's and that he put it under a customer's skirt with its flash enabled and appeared to take pictures that would be accessible in the cellphone's memory (or via cloud storage). The testimonial value of compelling the cellphone's password was negligible under the circumstances: it was *Stahl's* phone, evidence established his use of the phone during the

incident for flash-photography, and he initially agreed to allow police to search the phone, thereby inferring his knowledge of the passcode and its authenticity. By its holding, *Stahl* stands for the proposition that where the state establishes factually that it knows that a password existed, that the suspect possesses or controls the password, and that the suspect's actions disclosed or authenticated the password sought (here by Stahl initially agreeing to allow police to access the phone), it is a foregone conclusion to force its disclosure. A similar result arose in *State v. Johnson*, WD 80945, 2019 WL 1028462 (Mo. Ct. App. Mar. 5, 2019), which involved compelled production of a passcode by a defendant who had previously entered it into his phone in the presence of government actors.

The facts conveyed through his act of producing the passcode were the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity. The State showed that it had prior knowledge of those facts because Johnson knowingly and voluntarily entered the passcode the first time in the presence of law enforcement and defense counsel for the purpose of having his expert examine the phone; hence, their disclosure a second time pursuant to the order to compel was a foregone conclusion.

Id. at *14 (footnote omitted). Because the defendant had already openly used the passcode in the manner described, the "compelled act of production was not testimonial" and not a Fifth Amendment violations. *Id.*

Unlike *Stahl* and *Johnson*, the decision in *G.A.Q.L* was not based on application of the foregone conclusion exception to unearth a passcode about which the state had prior knowledge via its open use by the suspect (*Johnson*) or the suspect's initial agreement to disclose it (*Stahl*). Instead, *G.A.Q.L* focused on the state's goal of accessing the *information* on the suspect's cellphone because the state lacked prior knowledge of the suspect's password. In *Stahl*, the court noted that the state sought "the phone passcode not because it wants the passcode itself, but because it wants to know what communications lie beyond the

passcode wall.” *G.A.Q.L.*, 257 So. 3d at 1062. The court in *G.A.Q.L.* concluded that compelling the passcode was akin to a testimonial act (i.e., revealing the “contents of the mind” of the minor) protected by the Fifth Amendment. It rejected *Stahl*’s analysis under the foregone conclusion exception, applying the three-part test to the *information* sought rather than the passcode. *Id.* at 1063 (“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.”). In rejecting *Stahl*’s password-centric approach, the court said that to do “otherwise would expand the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment.” *Id.* It pointed out that under the approach in *Stahl* “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.” *Id.**

The application of *Stahl* is inconsistent with protection of a defendant’s right against self-incrimination in situations *where a defendant has not given up his testimonial privilege in the*

* Judge Kuntz concurred in the result, noting that the “foregone conclusion exception is a judicially created exception” to the Fifth Amendment with limited application to compelled production of documents. *G.A.Q.L.*, 257 So. 3d at 1066 (Kuntz, J., concurring in result). His conclusion, that “the foregone conclusion doctrine cannot apply to compelled oral testimony,” is based on the principle that forcing an “accused to orally communicate to the government information maintained only in his mind would certainly compel oral testimony.” *Id.* His bright-line approach is appealing and has the virtue of consistency with the intent of the Founders to protect against surrendering incriminating evidence before or at trial. See Donald Dripps, *Self-Incrimination*, in *THE HERITAGE GUIDE TO THE CONSTITUTION* 437-439 (David F. Forte & Matthew Spalding eds., 2d ed. 2014) (noting that the Supreme Court in the 1880s “took the view that the privilege protected private books and papers” but has since “changed significantly” Fifth Amendment doctrine.).

password itself. Unlike the situations in *Stahl* and *Johnson*, no evidence establishes that Pollard had previously given up his privilege in the password sought. In these situations, as the court in *G.A.Q.L.* noted, the three-part test is tautological when applied to passwords because all password-protected cellphones have an “authentic” password, making the *Stahl* test somewhat circular. In this regard, the court in *Stahl* said that “[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic,” 206 So. 3d at 136, which begs the question of whether sufficient evidence established that the passcode is authentic *before* it had been compelled and used successfully. The state must have sufficient proof of authenticity *before* it can compel the password’s production; simply because a compelled password unlocks a cellphone after the fact doesn’t make it authentic *ex ante*. To do otherwise is “like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.” *United States v. Hubbell*, 530 U.S. 27, 43 (2000).

The approach in *Stahl* makes sense, however, in those limited situations where the state establishes that the testimonial value of the compelled password has been abandoned, such as where a defendant has voluntarily entered his passcode to access his cellphone in the presence of law enforcement such that the testimonial value of compelling the passcode’s production a second time is negligible. *Johnson*, 2019 WL 1028462, at *14 (state showed that defendant “knowingly and voluntarily entered the passcode the first time in the presence of law enforcement and defense counsel for the purpose of having his expert examine the phone; hence, their disclosure a second time pursuant to the order to compel was a foregone conclusion.”). We note that it becomes predominantly a Fourth Amendment issue, not a Fifth Amendment one, in such cases as to the scope of what the state is allowed access in using the compelled password.

Turning back to *G.A.Q.L.*, that court held that “if the state can meet the requirements of the foregone conclusion exception, it may compel otherwise ostensibly self-incriminating testimonial production of information.” 257 So. 3d at 1063.

Under this exception, an act of production is not a violation of the Fifth Amendment—even if it conveys a fact—if the state can show with reasonable particularity that, at the time it sought to compel the act of production, it already knew of the materials sought, thereby making any testimonial aspect a foregone conclusion. . . . As it pertains to electronic files, this doctrine requires that the state demonstrate with reasonable particularity “that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic.”

Id. (citing *In re Grand Jury Subpoena*, 670 F.3d at 1349 n.28). In applying the three-part test, the court concluded that the state failed to identify with reasonable particularity any specific files sought on the minor’s cellphone. It noted that “the state’s subpoena fails to identify any specific file locations or even name particular files that it seeks from the encrypted, passcode-protected phone. *Instead, it generally seeks essentially all communications, data, and images on the locked iPhone.*” *G.A.Q.L.*, 257 So. 3d at 1064 (emphasis added). At best, the prosecutor at a hearing said a surviving passenger had been communicating with the minor via Snapchat and text message on the day of the accident and after the accident, but it held that “this stand-alone statement is not enough to meet the ‘reasonable particularity’ requirement of the foregone conclusion exception.” *Id.* “It is not enough for the state to infer that evidence exists—it must identify what evidence lies beyond the passcode wall with reasonable particularity.” *Id.* The court in *G.A.Q.L.* therefore concluded that the foregone conclusion exception was not met.

We agree with the Fourth District that unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communications, data and images “amount[s] to a mere fishing expedition.” *Id.* On the assumption that the foregone conclusion exception applies to core testimonial communications, such as a compelled oral disclosure of a password, it is not applicable here because the state failed to identify with particularity and certainty what information existed beyond the password-protected cellphone wall; mere inference that evidence may exist is not

enough. *In re Grand Jury Subpoena*, 670 F.3d at 1347 (“Case law from the Supreme Court does not demand that the Government identify exactly the documents it seeks, but it does require some specificity in its requests—categorical requests for documents the Government anticipates are likely to exist simply will not suffice.”).

Applied here, the state’s generalized requests for multiple categories of communications, pictures, and social media activity fit the description of a net cast far too broadly. The only category of information that potentially meets the reasonable particularity standard is the investigating officer’s affidavit, which avers only that “it is reasonable to believe” that a co-defendant had “communicated with Pollard via cell phone” leading up to and on the day the robbery occurred. The basis for this belief is that because the co-defendant had sent text messages to another person involved in the robbery, it would be reasonable to believe that the co-defendant must have communicated with Pollard in a similar manner as well, even though no specific communication is identified or alleged. As in *G.A.Q.L.*, the evidentiary record is too thin to conclude that the foregone conclusion exception applies. At best, the officer believed that text messages likely existed on Pollard’s phone because most criminal enterprises of this type operate via coordinated electronic communications that would leave a discoverable digital trail, but this generalized belief falls short of the reasonable particularity standard. *See Hubbell*, 530 U.S. at 45 (government’s deficient identification of particular documents sought cannot be cured by “the overbroad argument that a businessman such as [Hubbell] will always possess general business and tax records that fall within the broad categories described in this subpoena.”).

In conclusion, we grant the writ of certiorari and quash the trial court’s order.

PETITION GRANTED; ORDER QUASHED

JAY, J., concurs; WINOKUR, J., dissents with opinion.

Not final until disposition of any timely and authorized motion under Fla. R. App. P. 9.330 or 9.331.

WINOKUR, J., dissenting.

The Fifth Amendment’s Self-Incrimination Clause, the relevant provision here, “provides: ‘No person ... shall be compelled in any criminal case to be a witness against himself’” and, at its core, “is a prohibition on compelling a criminal defendant to testify against himself at trial.” *United States v. Patane*, 542 U.S. 630, 637 (2004) (quoting amend. V, U.S. Const.). Upon compulsion, an “act of producing evidence” that is incriminating could have “communicative aspects” sufficient to implicate the Fifth Amendment, but this is not the case when the evidence the state seeks to compel production of is a “foregone conclusion” known by the state, eliminating its testimonial worth. *Fisher v. United States*, 425 U.S. 391, 410-11 (1976). In holding that the Fifth Amendment bars the state from compelling an accused to produce the password to his cell phone—where he does not dispute the existence of the password or his knowledge of it—the majority conflates Fifth Amendment jurisprudence with the protections provided in the Fourth Amendment,¹ which is not at issue. I would deny relief.

I.

Matthew Pollard was arrested and charged, along with co-defendants, with armed robbery. The state proved to the trial court

¹ “The Fourth Amendment protects ‘[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,’” *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018), and was purposed “to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials,” *id.* (quoting *Camara v. Mun. Court of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967)).

that Pollard participated in the robbery and provided the firearm, and that he and the co-defendants planned the robbery through text messages. The state sought a search warrant for Pollard's phone, asserting probable cause that the phone contained incriminating evidence, which the trial court issued and Pollard unsuccessfully challenged. After seizing Pollard's phone, law enforcement was unable to access its contents without his passcode and the state filed a motion to compel him to produce it. Pollard objected, arguing that production of the password could not be severed from production of the data inside the phone (which is what the state truly sought) and the state has not adequately identified the data in the phone for the "foregone conclusion" exception to apply. The trial court found that the phone belonged to Pollard, he knew its passcode, and it could not be accessed without the passcode—none of which was disputed—and granted the motion to compel pursuant to *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016). The trial court ordered Pollard to provide his passcode, ruled that the state could not use his production of the passcode as evidence at trial, and allowed the passcode he provided to be sealed pending our review.

II.

The Fifth Amendment "applies only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher*, 425 U.S. at 408; *see also Doe v. United States*, 487 U.S. 201, 207 (1988) (finding that compliance would be compelled and incriminating, thus the only question is whether it would be a "testimonial communication"). Here, the parties do not dispute that disclosure of the passcode is being compelled or that it would be incriminating. The question at issue is whether Pollard's act of producing his password is a testimonial communication.

Testimonial Communication

"[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Doe*, 487 U.S. at 210. For this reason, compelled acts that do not require an accused to disclose his knowledge—such as furnishing a blood sample, providing a voice or handwriting exemplar, or standing in a lineup—are not

testimonial and are not protected by the Fifth Amendment. *Id.* at 210-11 (collecting cases). Whether a particular compelled communication is testimonial “depend[s] on the facts and circumstances” of the particular case. *Fisher*, 425 U.S. at 410.

The Fourth District in *G.A.Q.L. v. State*, 257 So. 3d 1058, 1061-62 (Fla. 4th DCA 2018), found that disclosing a password “is testimonial and can violate the Fifth Amendment privilege against compelled self-incrimination” because the “very act of revealing a password asserts a fact: that the defendant knows the password.” *But see Stahl*, 206 So. 3d at 133-34 (finding that disclosure of the password was not testimonial because the password was not itself significant or an acknowledgment of the incriminating evidence found on the phone). Generally, I agree that when an accused provides a passcode to a cell phone, he engages “in a testimonial act utilizing the ‘contents of his mind’ and demonstrating as a factual matter that he knows how to access the phone.” *G.A.Q.L.*, 257 So. 3d at 1062. Pollard’s production of his password is testimonial in that it shows that he has control over the phone and can access its contents, an incriminating fact if the phone contains plans for committing an armed robbery.

Foregone Conclusion

While production of the password may generally be testimonial, the Fifth Amendment may not bar compulsion if the state already knows of the testimonial aspect of the communication. In *Fisher*, the Supreme Court considered whether compelled production implicated the Fifth Amendment. Even if the act of production would include testimonial self-incrimination, the Court held that compelled production was permissible because the existence and location of the evidence was known to the Government, or was a “foregone conclusion.” 425 U.S. at 411. “Under these circumstances by enforcement of the summons ‘no constitutional rights are touched. The question is not of testimony but of surrender.’” *Id.* (quoting *In re Harris*, 221 U.S. 274, 279 (1911)).

Under this exception, an act of production is not a violation of the Fifth Amendment—even if it conveys a fact—if the state can show with reasonable particularity that, at the time it sought to compel the act of production,

it already knew of the materials sought, thereby making any testimonial aspect a foregone conclusion.

G.A.Q.L., 257 So. 3d at 1063.; *see also United States v. Apple MacPro Computer*, 851 F.3d 238, 247 (3d Cir. 2017), cert. denied sub nom. *Doe v. United States*, 138 S. Ct. 1988 (2018) (“[T]he Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a ‘foregone conclusion’ that ‘adds little or nothing to the sum total of the Government’s information.’” (quoting *Fisher*, 425 U.S. at 411)). In contrast, compelling the production of incriminating evidence (which implicitly admits existence and possession) violated the Fifth Amendment where the state’s demand was akin to a “detailed written interrogatory or a series of oral questions at a discovery deposition,” characterized “as a ‘fishing expedition.’” *United States v. Hubbell*, 530 U.S. 27, 36, 41-42 (2000).

Here, the state’s only demand of Pollard is to produce his passcode. The state is not asking him to recover or retrieve any files that might exist on his phone. Because production of the passcode is the only communication the state seeks, this is where the analysis must be focused. *See Stahl*, 206 So. 3d at 136 (holding that the relevant question is whether the state “has established that it knows with reasonable particularity that the *passcode* exists, is within the accused’s possession or control, and is authentic”); *Apple MacPro Computer*, 851 F.3d at 248 n.7 (“[A] very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is ‘I, John Doe, know the password for these devices.’”); *State v. Johnson*, No. WD80945, 2019 WL 1028462, at *14 (Mo. Ct. App. Mar. 5, 2019) (“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. Here, Johnson was ordered to produce the passcode to his phone. The facts conveyed through his act of producing the passcode were the existence of the passcode, his possession and control of the phone’s passcode, and the passcode’s authenticity.”).

Before the trial court, the state proved—and Pollard conceded—that the phone belonged to Pollard, that he had control over it, and that he knew the passcode to unlock it. Thus, the facts making this communication implicitly “testimonial” are not in dispute, but are a foregone conclusion.² See *Com. v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014) (“The facts that would be conveyed by the defendant through his act of decryption—his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key—already are known to the government and, thus, are a ‘foregone conclusion.’”).³

² Unlike compelling one to produce documents, requiring someone to produce a passcode to unlock a cell phone does not implicate a question of authenticity. See *State v. Stahl*, 206 So. 3d 124, 136 (Fla. 2d DCA 2016) (“[W]e must recognize that the technology is self-authenticating—no other means of authentication may exist. If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.” (citation omitted)); *Com. v. Gelfgatt*, 11 N.E.3d 605, 616 n.14 (Mass. 2014) (“Here, the defendant’s decryption of his computers does not present an authentication issue analogous to that arising from a subpoena for specific documents because he is not selecting documents and producing them, but merely entering a password into encryption software.”).

³ See also *State v. Andrews*, 197 A.3d 200, 207 (N.J. Super. Ct. App. Div. 2018), leave to appeal granted, No. 082209, 2019 WL 2011594 (N.J. May 3, 2019) (“[D]efendant’s Fifth Amendment right against self-incrimination is not violated by requiring him to disclose the passcodes for his iPhones, which the State lawfully possessed. The act of producing the passcodes has testimonial aspects because defendant is acknowledging ownership, possession, and control of the devices. He is also acknowledging he has the ability to access the contents of the phone. However, by producing the passcodes, defendant is not implicitly conveying any information the State does not already possess. Defendant is not telling the government something it does not already know. Therefore, the implicit facts conveyed by the act of producing the passcodes is a ‘foregone conclusion’ and compelled disclosure of the passcodes does not violate defendant’s Fifth Amendment right against self-incrimination.”); *Commonwealth v. Davis*, 176 A.3d

The question is not whether Pollard knows the password, but whether he must surrender it, *see Fisher*, 425 U.S. at 411, so the Fifth Amendment’s protection against self-incrimination does not apply.

III.

G.A.Q.L. focused on the contents of the phone when determining whether the testimony is a foregone conclusion. 257 So. 3d at 1063 (“[T]he object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall.”). The majority now follows suit.⁴ In this view, “it is not enough to know that a passcode wall exists, but rather, the state must demonstrate with reasonable particularity that what it is looking for is in fact located behind that wall” because “the ‘evidence sought’ in a password production case such as this is not the password itself; rather, it is the actual files or evidence on the

869, 876 (Pa. Super. Ct. 2017), appeal granted, 195 A.3d 557 (Pa. 2018) (citing, *inter alia*, *Apple MacPro Computer* and *Gelfgatt* and agreeing that the “appellant’s act of providing the password in question is not testimonial in nature and his Fifth Amendment right against self-incrimination would not be violated” where the appellant admitted that he knew the password to the computer).

⁴ The majority asserts that the “password-centric approach” “makes sense . . . where the state establishes that the testimonial value of the compelled password has been abandoned, such as where a defendant has voluntarily entered his passcode to access his cellphone in the presence of law enforcement such that the testimonial value of compelling the passcode’s production a second time is negligible,” and such a situation “becomes predominantly a Fourth Amendment issue, not a Fifth Amendment one[.]” Maj. op. at 8-9. This distinction is without a difference as applied to this case. If the analysis is properly focused on the accused’s knowledge of the passcode when he has entered it in the presence of law enforcement previously, there is no reason it should be centered elsewhere when the accused simply admits that he knows it and can enter it.

locked phone.” *Id.* at 1063-64.⁵ Thus, *G.A.Q.L.* holds, the state must identify with reasonable particularity the evidence on the phone to compel an accused to produce his password. *Id.* at 1064.

It is true that the state does not seek the passcode for itself, but as a means to access the files in the phone. This, however, does not change what the accused is being compelled to produce. *See, e.g., State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. Ct. App. Div. 2018), leave to appeal granted, No. 082209, 2019 WL 2011594 (N.J. May 3, 2019) (“Defendant argues the State is unaware of all of the possible contents of defendant’s devices. This is immaterial because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes.”). In no other context does the foregone-conclusion analysis focus on evidence other than the evidence being compelled, and there is no reason to shift the focus now.

G.A.Q.L. is correct that the state must identify with particularity the files on the phone it seeks. But when these files are not what the state is compelling production of, the Fifth Amendment is not implicated. The Fifth Amendment does not “protect[] private information obtained without compelling self-incriminating testimony[.]” *Fisher*, 425 U.S. at 400. “Insofar as private information not obtained through compelled self-incriminating testimony is legally protected, its protection stems from other sources” such as “the Fourth Amendment’s protection

⁵ *G.A.Q.L.* drew on the analysis in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1349 (11th Cir. 2012), which found that the government failed to prove that it “knew to any degree of particularity what, if anything, was hidden behind the encrypted wall.” However, the Eleventh Circuit also found that the government did not show “any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives, that [the accused] has access to those files, or that he is capable of decrypting the files.” *Id.* In contrast, the state here had probable cause that the phone contained incriminating text messages, from which it obtained a warrant to seize the phone, and showed that the phone belonged to Pollard and that he knew the passcode to unlock it.

against seizures without warrant or probable cause,” the First Amendment’s protection against being compelled to disclose who you associate with, “or evidentiary privileges such as the attorney-client privilege.” *Id.* at 401.

The state’s obligation to describe with particularity the files it seeks is required because the “Fourth Amendment by its terms requires particularity in the [search] warrant[.]” *Groh v. Ramirez*, 540 U.S. 551, 557 (2004); *see also Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984) (“The uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional.”). Here, as in *G.A.Q.L.*, the validity of the search warrant and the Fourth Amendment are not at issue.

The Fourth Amendment protected Pollard’s phone from search and seizure until a search warrant issued. Whether Pollard must produce the passcode to his phone—enabling the state to search and seize what is already entitled to—depends on whether that compelled act is testimonial and self-incriminating. Here, the only testimonial aspect of the production—Pollard’s ownership and control of the phone—is undisputed and a foregone conclusion. The Fifth Amendment, contrary to the analysis of the majority and the Fourth District in *G.A.Q.L.*, does not provide any further quasi-Fourth-Amendment protections where the state is not compelling production of the phone or data on it and the state possesses a valid search warrant for the phone.⁶ *See United States v. Spencer*, No. 17-Cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26,

⁶ The Supreme Court explained the issue of privacy in relation to the Fourth and Fifth Amendments in *Fisher*, 425 U.S. at 400:

The Framers addressed the subject of personal privacy directly in the Fourth Amendment. They struck a balance so that when the State’s reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue. They did not seek in still another Amendment the Fifth to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination.

2018) (“To the extent Spencer contends that the government has not adequately identified the files it seeks” in the devices it compelled him to decrypt, “that is an issue properly raised under the Fourth Amendment, not the Fifth.”).⁷

IV.

In this case, we do not need to determine whether the state can sufficiently describe the evidence it seeks on the phone because the state has not compelled Pollard to produce that evidence and the Fourth Amendment is not at issue. Pollard argues that he may not be compelled to produce the passcode to his cell phone due to the Fifth Amendment’s Self-Incrimination Clause, but this argument fails where the testimonial component of the communication is undisputed. I would deny Pollard’s petition for writ of certiorari.

Stacy A. Scott, Public Defender, and Logan P. Doll, Assistant Public Defender, Gainesville, for Petitioner.

Ashley Moody, Attorney General, and Benjamin L. Hoffman, Assistant Attorney General, Tallahassee, for Respondent.

⁷ We need not decide whether the state may compel an accused to disclose his passcode orally or in writing. Several authorities have distinguished whether the state may “compel the defendant to disclose -- whether orally or in writing -- the actual password, as opposed to cases requiring merely physically entering it into the device.” *Commonwealth v. Jones*, 117 N.E.3d 702, 710 n.9 (Mass. 2019); *see also G.A.Q.L.*, 257 So. at 1061-62 (Kuntz, J., concurring in result) (concluding “that the foregone conclusion doctrine cannot apply to compelled oral testimony”). Here, Pollard does not distinguish between the act of entering the passcode and disclosure of the passcode orally or in writing. Instead, he argues that the passcode and phone data are so intertwined that the proper inquiry concerns the state’s knowledge of the data on the phone. As stated above, I disagree with this position.

CERTIFICATE OF SERVICE

I certify that on this 22nd day of January, 2020, a true and correct copy of the foregoing notice has been furnished by electronic service through the Florida Courts E-Filing Portal to the following:

Counsel for Petitioner

Logan Doll
Public Defender's Office
151 SW 2nd Street
Gainesville, Florida 32601
Phone: 352-338-7381
Dolll@pdo8.org

/s/ Christopher J. Baum
Christopher J. Baum (FBN 1007882)

FIRST DISTRICT COURT OF APPEAL
STATE OF FLORIDA

No. 1D18-4572

MATTHEW TYLER POLLARD,

Petitioner,

v.

STATE OF FLORIDA,

Respondent.

CORRECTED PAGES: pg 11
CORRECTION IS
UNDERLINED IN RED
MAILED: June 27, 2019
BY: KMS

Petition for Writ of Prohibition—Original Jurisdiction.

June 20, 2019

MAKAR, J.

To what extent does the Fifth Amendment right against self-incrimination protect a suspect in a criminal case from the compelled disclosure of a password to an electronic communications device in the state's possession? Courts differ in their legal analysis of this question, resulting in no consensus in state and federal courts; indeed, different approaches currently exist between two Florida appellate courts on the topic. In this case, we conclude that the proper legal inquiry on the facts presented is whether the state is seeking to compel a suspect to provide a password that would allow access to information the state knows is on the suspect's cellphone and has described with reasonable particularity.

Matthew Tyler Pollard was arrested and charged with armed robbery of two victims who were misled into believing they were buying drugs. Pursuant to a warrant, the state seized an iPhone® from Pollard’s car and filed a motion to compel Pollard to disclose the phone’s passcode so that it could access broad categories of encrypted information on the cellphone. The information sought was described in general terms and broad categories in the investigating detective’s affidavit in support of the search warrant:

- Call/text/communication history on and between June 19, 2018 and June 25, 2018.
- Content of communications on and between June 19, 2018 and June 25, 2018.
- Picture(s) of narcotics, money, firearms.
- Written information about the illegal purchase, possession, and sale of illegal narcotics, and or plans of a robbery on and between June 19, 2018 and June 25, 2018.
- Activity listed in phone applications: Facebook, Facebook Messenger, etc., concerning buying, selling, or possessing illegal narcotics and or planning a robbery on and between June 19, 2018 and June 25, 2018.

The affidavit did not state the existence or content of any specific text, picture, call or other particular information. It noted, however, that “it was reasonable to believe” that a co-defendant, Draven Rouse, had “communicated with Pollard via cell phone” both prior to and on the day of the robbery, presumably to coordinate the robbery. Based on his training and experience, the detective stated that persons in “criminal enterprises” sometimes use cellphones to communicate and coordinate activities with accomplices, to document criminal activities, and to compile contacts useful in a criminal investigation; he did not, however, identify any specific item that was on Pollard’s cellphone, only that the state wished to seize from the cellphone all items in the categories of information listed above.

Accessing the cellphone’s content required a passcode, which the state in a one-page motion sought to compel from Pollard. The state’s motion—and the trial court’s favorable ruling—relied

exclusively on *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016), which upheld the compelled production of a cellphone's passcode over a defendant's Fifth Amendment objection that doing so violated his right not to testify as to the "contents of his mind," i.e., knowledge of the passcode itself. The trial court relied on *Stahl*, even though it arose in another district and (as discussed later) involved different facts, because no other Florida court had weighed in on the general topic at that time. *Pardo v. State*, 596 So. 2d 665, 666 (Fla. 1992) ("in the absence of interdistrict conflict, district court decisions bind all Florida trial courts.").

Based on *Stahl*, the trial court held the state established that the cellphone was Pollard's, that it was password protected, and that if the password compelled from Pollard made the cellphone's content accessible, the password was deemed authentic, thereby requiring Pollard to provide the password. Quoting *Stahl*, the trial court also noted that the state had established by independent means the "existence, possession, and authenticity of the documents' it seeks to recover from [Pollard's] phone." 206 So. 3d at 135. It concluded that the "State already knows the information it is seeking [Pollard] to produce and why." The trial court did not identify any specific documents or information in this regard, but noted that "at [a] minimum, text messages" were part of the coordinated effort to conduct the robbery. No limits were placed on the scope of the search of the contents of the cellphone, but the state was prohibited from using the compelled production of Pollard's password as evidence at trial; no limitation was put on use of the documents and information that might be discovered. The password was placed in a sealed and confidential file pending resolution of Pollard's petition for writ of prohibition, which seeks to prevent the compelled use of the embargoed password. We treat the petition as a petition for writ of certiorari, which requires a departure from the essential requirements of the law that results in material injury that cannot be corrected post-judgment. Art. V, § 4(b)(3), Fla. Const. (2019); *Stahl*, 206 So. 3d at 129; *Grant v. State*, 832 So. 2d 770, 771 (Fla. 5th DCA 2002).

Courts nationwide are struggling to find common legal ground on the constitutionality of compelled password production under the Fifth Amendment and its application in specific cases. U.S. Const. amend. V. ("No person . . . shall be compelled in any

criminal case to be a witness against himself”); *see also* Art. I, § 9, Fla. Const. (2019) (same); *see generally* Marjorie A. Shields, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*, 84 A.L.R. 6th 251 (2019) (compiling Fifth Amendment cases involving “compelled disclosure of an individual's password, means of decryption, or unencrypted copy of electronically stored data.”).

The Fifth Amendment forbids a governmentally-compelled *testimonial* communication (or act) that tends to incriminate the communicator (or actor). *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1341 (11th Cir. 2012). “The touchstone of whether an act of production is testimonial is whether the government compels the individual to use ‘the contents of his own mind’ to explicitly or implicitly communicate some statement of fact. *Id.* at 1345 (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)). Forcing a defendant to disclose a password, whether by speaking it, writing it down, or physically entering it into a cellphone, compels information from that person’s mind and thereby falls within the core of what constitutes a testimonial disclosure. In this case, Pollard was compelled to act in a testimonial manner by disclosing a password known only in his mind. In this type of password compulsion case, the law is unsettled as to whether a “foregone conclusion” exception might apply, i.e., where the government knows that identifiable documents exist under a defendant’s control such that obtaining them via a compelled disclosure of a password is a mere formality and thereby non-testimonial. The Supreme Court has approved the exception’s use but not in the context of a compelled passcode disclosure. *See G.A.Q.L.*, 257 So. 3d at 1066 (Fla. 4th DCA 2018) (“The Supreme Court has applied the foregone conclusion exception only when the compelled testimony has consisted of existing evidence such as documents.”) (Kuntz, J., concurring in result).

Florida is no exception in the national judicial debate over compelled password production. Since the trial court’s ruling, the Fourth District issued its opinion in *G.A.Q.L. v. State*, 257 So. 3d 1058, 1062 (Fla. 4th DCA 2018), which seemingly conflicts with the approach taken in *Stahl* as to the foregone conclusion

exception and allows compelled production of information where the testimonial value of doing so is negligible. As a result, two different analytical methods currently exist in Florida, though both apply the same two-step framework, which asks (a) is the compelled production of the password a testimonial and potentially incriminating act, and, if so, (b) is the compelled password production nonetheless permissible under the foregone conclusion exception because its testimonial value is inconsequential due to the state already knowing of the existence of the requested information. *Id.* at 1063 (“Under this exception, an act of production is not a violation of the Fifth Amendment—even if it conveys a fact—if the state can show with reasonable particularity that, at the time it sought to compel the act of production, it already knew of the materials sought, thereby making any testimonial aspect a foregone conclusion.”); *Stahl*, 206 So. 3d at 135 (“That is, by implicitly admitting the existence of the evidence requested and that it is in the accused's possession the accused ‘adds little or nothing to the sum total of the Government's information’; the information provided is a foregone conclusion.”) (quoting *Fisher v. United States*, 425 U.S. 391, 411 (1976) (“The existence and location of the [tax-preparation] papers are a foregone conclusion” such that taxpayer’s compelled production of them “adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons ‘no constitutional rights are touched. The question is not of testimony but of surrender.’”)) (citation omitted); see generally Fern L. Kletter, *Construction and Application of "Foregone Conclusion" Exception to Fifth Amendment Privilege against Self-Incrimination*, 25 A.L.R. Fed. 3d Art. 10 (2017) (compiling cases that discuss the foregone conclusion exception).

For example, if the central feature in a criminal case is *what* files are on a cellphone, and the state can establish that a defendant’s cellphone contains files that are described with “reasonable particularity,” the compelled production of the password to access those files (but only those files) does no damage to the defendant’s constitutional right against self-incrimination where sufficient evidence establishes that it is his phone on which the files reside. In contrast, if a central feature of a criminal case is *who* owns a seized cellphone or has the code to access it,

compelling a defendant to provide a password may be testimonial and incriminating because it proves an unknown fact, i.e., who is the cellphone's owner or who can access it. For instance, if an employee was alleged to have broken into a password protected computer system, and caused cyber-harm therein, evidence as to his ability to access the system (i.e., possession of the password) would be incriminating because it supports the ability to access the system.

In *Stahl*, a video voyeurism case, the defendant used a cellphone to take video under a customer's skirt, was identified via store surveillance video, and arrested. After his locked cellphone was produced pursuant to a search warrant, he admitted it was his cellphone and initially agreed to permit police to search it for images, but he changed his mind, resulting in the state's request to compel its password. Under those circumstances, the Second District concluded that compulsion of the passcode was not a Fifth Amendment violation under the foregone conclusion exception. The three-part test for the foregone conclusion exception requires that the state "must show with reasonable particularity that, at the time it sought the act of production, it already knew the evidence sought existed, the evidence was in the possession of the accused, and the evidence was authentic." *Stahl*, 206 So. 3d at 135 (citing *In re Grand Jury Subpoena*, 670 F.3d at 1344 ("Where the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available.")) (footnote omitted).

Stahl's application of foregone conclusion exception focused on disclosure of the *password* itself, rather than the *information* that access to the cellphone would produce. *Stahl* viewed the forced disclosure of the *password* as non-testimonial because the existence, custody, and authenticity of the *password* were a "foregone conclusion" under the facts of that case. No one disputed that the cellphone was the defendant's and that he put it under a customer's skirt with its flash enabled and appeared to take pictures that would be accessible in the cellphone's memory (or via cloud storage). The testimonial value of compelling the cellphone's password was negligible under the circumstances: it was *Stahl's* phone, evidence established his use of the phone during the

incident for flash-photography, and he initially agreed to allow police to search the phone, thereby inferring his knowledge of the passcode and its authenticity. By its holding, *Stahl* stands for the proposition that where the state establishes factually that it knows that a password existed, that the suspect possesses or controls the password, and that the suspect's actions disclosed or authenticated the password sought (here by Stahl initially agreeing to allow police to access the phone), it is a foregone conclusion to force its disclosure. A similar result arose in *State v. Johnson*, WD 80945, 2019 WL 1028462 (Mo. Ct. App. Mar. 5, 2019), which involved compelled production of a passcode by a defendant who had previously entered it into his phone in the presence of government actors.

The facts conveyed through his act of producing the passcode were the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity. The State showed that it had prior knowledge of those facts because Johnson knowingly and voluntarily entered the passcode the first time in the presence of law enforcement and defense counsel for the purpose of having his expert examine the phone; hence, their disclosure a second time pursuant to the order to compel was a foregone conclusion.

Id. at *14 (footnote omitted). Because the defendant had already openly used the passcode in the manner described, the "compelled act of production was not testimonial" and not a Fifth Amendment violations. *Id.*

Unlike *Stahl* and *Johnson*, the decision in *G.A.Q.L* was not based on application of the foregone conclusion exception to unearth a passcode about which the state had prior knowledge via its open use by the suspect (*Johnson*) or the suspect's initial agreement to disclose it (*Stahl*). Instead, *G.A.Q.L* focused on the state's goal of accessing the *information* on the suspect's cellphone because the state lacked prior knowledge of the suspect's password. In *Stahl*, the court noted that the state sought "the phone passcode not because it wants the passcode itself, but because it wants to know what communications lie beyond the

passcode wall.” *G.A.Q.L.*, 257 So. 3d at 1062. The court in *G.A.Q.L.* concluded that compelling the passcode was akin to a testimonial act (i.e., revealing the “contents of the mind” of the minor) protected by the Fifth Amendment. It rejected *Stahl*’s analysis under the foregone conclusion exception, applying the three-part test to the *information* sought rather than the passcode. *Id.* at 1063 (“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.”). In rejecting *Stahl*’s password-centric approach, the court said that to do “otherwise would expand the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment.” *Id.* It pointed out that under the approach in *Stahl* “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.” *Id.**

The application of *Stahl* is inconsistent with protection of a defendant’s right against self-incrimination in situations *where a defendant has not given up his testimonial privilege in the*

* Judge Kuntz concurred in the result, noting that the “foregone conclusion exception is a judicially created exception” to the Fifth Amendment with limited application to compelled production of documents. *G.A.Q.L.*, 257 So. 3d at 1066 (Kuntz, J., concurring in result). His conclusion, that “the foregone conclusion doctrine cannot apply to compelled oral testimony,” is based on the principle that forcing an “accused to orally communicate to the government information maintained only in his mind would certainly compel oral testimony.” *Id.* His bright-line approach is appealing and has the virtue of consistency with the intent of the Founders to protect against surrendering incriminating evidence before or at trial. See Donald Dripps, *Self-Incrimination*, in THE HERITAGE GUIDE TO THE CONSTITUTION 437-439 (David F. Forte & Matthew Spalding eds., 2d ed. 2014) (noting that the Supreme Court in the 1880s “took the view that the privilege protected private books and papers” but has since “changed significantly” Fifth Amendment doctrine.).

password itself. Unlike the situations in *Stahl* and *Johnson*, no evidence establishes that Pollard had previously given up his privilege in the password sought. In these situations, as the court in *G.A.Q.L.* noted, the three-part test is tautological when applied to passwords because all password-protected cellphones have an “authentic” password, making the *Stahl* test somewhat circular. In this regard, the court in *Stahl* said that “[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic,” 206 So. 3d at 136, which begs the question of whether sufficient evidence established that the passcode is authentic *before* it had been compelled and used successfully. The state must have sufficient proof of authenticity *before* it can compel the password’s production; simply because a compelled password unlocks a cellphone after the fact doesn’t make it authentic *ex ante*. To do otherwise is “like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.” *United States v. Hubbell*, 530 U.S. 27, 43 (2000).

The approach in *Stahl* makes sense, however, in those limited situations where the state establishes that the testimonial value of the compelled password has been abandoned, such as where a defendant has voluntarily entered his passcode to access his cellphone in the presence of law enforcement such that the testimonial value of compelling the passcode’s production a second time is negligible. *Johnson*, 2019 WL 1028462, at *14 (state showed that defendant “knowingly and voluntarily entered the passcode the first time in the presence of law enforcement and defense counsel for the purpose of having his expert examine the phone; hence, their disclosure a second time pursuant to the order to compel was a foregone conclusion.”). We note that it becomes predominantly a Fourth Amendment issue, not a Fifth Amendment one, in such cases as to the scope of what the state is allowed access in using the compelled password.

Turning back to *G.A.Q.L.*, that court held that “if the state can meet the requirements of the foregone conclusion exception, it may compel otherwise ostensibly self-incriminating testimonial production of information.” 257 So. 3d at 1063.

Under this exception, an act of production is not a violation of the Fifth Amendment—even if it conveys a fact—if the state can show with reasonable particularity that, at the time it sought to compel the act of production, it already knew of the materials sought, thereby making any testimonial aspect a foregone conclusion. . . . As it pertains to electronic files, this doctrine requires that the state demonstrate with reasonable particularity “that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic.”

Id. (citing *In re Grand Jury Subpoena*, 670 F.3d at 1349 n.28). In applying the three-part test, the court concluded that the state failed to identify with reasonable particularity any specific files sought on the minor’s cellphone. It noted that “the state’s subpoena fails to identify any specific file locations or even name particular files that it seeks from the encrypted, passcode-protected phone. *Instead, it generally seeks essentially all communications, data, and images on the locked iPhone.*” *G.A.Q.L.*, 257 So. 3d at 1064 (emphasis added). At best, the prosecutor at a hearing said a surviving passenger had been communicating with the minor via Snapchat and text message on the day of the accident and after the accident, but it held that “this stand-alone statement is not enough to meet the ‘reasonable particularity’ requirement of the foregone conclusion exception.” *Id.* “It is not enough for the state to infer that evidence exists—it must identify what evidence lies beyond the passcode wall with reasonable particularity.” *Id.* The court in *G.A.Q.L.* therefore concluded that the foregone conclusion exception was not met.

We agree with the Fourth District that unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communications, data and images “amount[s] to a mere fishing expedition.” *Id.* On the assumption that the foregone conclusion exception applies to core testimonial communications, such as a compelled oral disclosure of a password, it is not applicable here because the state failed to identify with particularity and certainty what information existed beyond the password-protected cellphone wall; mere inference that evidence may exist is not

enough. *In re Grand Jury Subpoena*, 670 F.3d at 1347 (“Case law from the Supreme Court does not demand that the Government identify exactly the documents it seeks, but it does require some specificity in its requests—categorical requests for documents the Government anticipates are likely to exist simply will not suffice.”).

Applied here, the state’s generalized requests for multiple categories of communications, pictures, and social media activity fit the description of a net cast far too broadly. The only category of information that potentially meets the reasonable particularity standard is the investigating officer’s affidavit, which avers only that “it is reasonable to believe” that a co-defendant had “communicated with Pollard via cell phone” leading up to and on the day the robbery occurred. The basis for this belief is that because the co-defendant had sent text messages to another person involved in the robbery, it would be reasonable to believe that the co-defendant must have communicated with Pollard in a similar manner as well, even though no specific communication is identified or alleged. As in *G.A.Q.L.*, the evidentiary record is too thin to conclude that the foregone conclusion exception applies. At best, the officer believed that text messages likely existed on Pollard’s phone because most criminal enterprises of this type operate via coordinated electronic communications that would leave a discoverable digital trail, but this generalized belief falls short of the reasonable particularity standard. *See Hubbell*, 530 U.S. at 45 (government’s deficient identification of particular documents sought cannot be cured by “the overbroad argument that a businessman such as [Hubbell] will always possess general business and tax records that fall within the broad categories described in this subpoena.”).

In conclusion, we grant the writ of certiorari and quash the trial court’s order.

PETITION GRANTED; ORDER QUASHED

JAY, J., concurs; WINOKUR, J., dissents with opinion.

Not final until disposition of any timely and authorized motion under Fla. R. App. P. 9.330 or 9.331.

WINOKUR, J., dissenting.

The Fifth Amendment’s Self-Incrimination Clause, the relevant provision here, “provides: ‘No person ... shall be compelled in any criminal case to be a witness against himself’” and, at its core, “is a prohibition on compelling a criminal defendant to testify against himself at trial.” *United States v. Patane*, 542 U.S. 630, 637 (2004) (quoting amend. V, U.S. Const.). Upon compulsion, an “act of producing evidence” that is incriminating could have “communicative aspects” sufficient to implicate the Fifth Amendment, but this is not the case when the evidence the state seeks to compel production of is a “foregone conclusion” known by the state, eliminating its testimonial worth. *Fisher v. United States*, 425 U.S. 391, 410-11 (1976). In holding that the Fifth Amendment bars the state from compelling an accused to produce the password to his cell phone—where he does not dispute the existence of the password or his knowledge of it—the majority conflates Fifth Amendment jurisprudence with the protections provided in the Fourth Amendment,¹ which is not at issue. I would deny relief.

I.

Matthew Pollard was arrested and charged, along with co-defendants, with armed robbery. The state proved to the trial court

¹ “The Fourth Amendment protects ‘[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,’” *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018), and was purposed “to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials,” *id.* (quoting *Camara v. Mun. Court of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967)).

that Pollard participated in the robbery and provided the firearm, and that he and the co-defendants planned the robbery through text messages. The state sought a search warrant for Pollard's phone, asserting probable cause that the phone contained incriminating evidence, which the trial court issued and Pollard unsuccessfully challenged. After seizing Pollard's phone, law enforcement was unable to access its contents without his passcode and the state filed a motion to compel him to produce it. Pollard objected, arguing that production of the password could not be severed from production of the data inside the phone (which is what the state truly sought) and the state has not adequately identified the data in the phone for the "foregone conclusion" exception to apply. The trial court found that the phone belonged to Pollard, he knew its passcode, and it could not be accessed without the passcode—none of which was disputed—and granted the motion to compel pursuant to *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016). The trial court ordered Pollard to provide his passcode, ruled that the state could not use his production of the passcode as evidence at trial, and allowed the passcode he provided to be sealed pending our review.

II.

The Fifth Amendment "applies only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher*, 425 U.S. at 408; *see also Doe v. United States*, 487 U.S. 201, 207 (1988) (finding that compliance would be compelled and incriminating, thus the only question is whether it would be a "testimonial communication"). Here, the parties do not dispute that disclosure of the passcode is being compelled or that it would be incriminating. The question at issue is whether Pollard's act of producing his password is a testimonial communication.

Testimonial Communication

"[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Doe*, 487 U.S. at 210. For this reason, compelled acts that do not require an accused to disclose his knowledge—such as furnishing a blood sample, providing a voice or handwriting exemplar, or standing in a lineup—are not

testimonial and are not protected by the Fifth Amendment. *Id.* at 210-11 (collecting cases). Whether a particular compelled communication is testimonial “depend[s] on the facts and circumstances” of the particular case. *Fisher*, 425 U.S. at 410.

The Fourth District in *G.A.Q.L. v. State*, 257 So. 3d 1058, 1061-62 (Fla. 4th DCA 2018), found that disclosing a password “is testimonial and can violate the Fifth Amendment privilege against compelled self-incrimination” because the “very act of revealing a password asserts a fact: that the defendant knows the password.” *But see Stahl*, 206 So. 3d at 133-34 (finding that disclosure of the password was not testimonial because the password was not itself significant or an acknowledgment of the incriminating evidence found on the phone). Generally, I agree that when an accused provides a passcode to a cell phone, he engages “in a testimonial act utilizing the ‘contents of his mind’ and demonstrating as a factual matter that he knows how to access the phone.” *G.A.Q.L.*, 257 So. 3d at 1062. Pollard’s production of his password is testimonial in that it shows that he has control over the phone and can access its contents, an incriminating fact if the phone contains plans for committing an armed robbery.

Foregone Conclusion

While production of the password may generally be testimonial, the Fifth Amendment may not bar compulsion if the state already knows of the testimonial aspect of the communication. In *Fisher*, the Supreme Court considered whether compelled production implicated the Fifth Amendment. Even if the act of production would include testimonial self-incrimination, the Court held that compelled production was permissible because the existence and location of the evidence was known to the Government, or was a “foregone conclusion.” 425 U.S. at 411. “Under these circumstances by enforcement of the summons ‘no constitutional rights are touched. The question is not of testimony but of surrender.’” *Id.* (quoting *In re Harris*, 221 U.S. 274, 279 (1911)).

Under this exception, an act of production is not a violation of the Fifth Amendment—even if it conveys a fact—if the state can show with reasonable particularity that, at the time it sought to compel the act of production,

it already knew of the materials sought, thereby making any testimonial aspect a foregone conclusion.

G.A.Q.L., 257 So. 3d at 1063.; *see also United States v. Apple MacPro Computer*, 851 F.3d 238, 247 (3d Cir. 2017), cert. denied sub nom. *Doe v. United States*, 138 S. Ct. 1988 (2018) (“[T]he Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a ‘foregone conclusion’ that ‘adds little or nothing to the sum total of the Government’s information.’” (quoting *Fisher*, 425 U.S. at 411)). In contrast, compelling the production of incriminating evidence (which implicitly admits existence and possession) violated the Fifth Amendment where the state’s demand was akin to a “detailed written interrogatory or a series of oral questions at a discovery deposition,” characterized “as a ‘fishing expedition.’” *United States v. Hubbell*, 530 U.S. 27, 36, 41-42 (2000).

Here, the state’s only demand of Pollard is to produce his passcode. The state is not asking him to recover or retrieve any files that might exist on his phone. Because production of the passcode is the only communication the state seeks, this is where the analysis must be focused. *See Stahl*, 206 So. 3d at 136 (holding that the relevant question is whether the state “has established that it knows with reasonable particularity that the *passcode* exists, is within the accused’s possession or control, and is authentic”); *Apple MacPro Computer*, 851 F.3d at 248 n.7 (“[A] very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is ‘I, John Doe, know the password for these devices.’”); *State v. Johnson*, No. WD80945, 2019 WL 1028462, at *14 (Mo. Ct. App. Mar. 5, 2019) (“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. Here, Johnson was ordered to produce the passcode to his phone. The facts conveyed through his act of producing the passcode were the existence of the passcode, his possession and control of the phone’s passcode, and the passcode’s authenticity.”).

Before the trial court, the state proved—and Pollard conceded—that the phone belonged to Pollard, that he had control over it, and that he knew the passcode to unlock it. Thus, the facts making this communication implicitly “testimonial” are not in dispute, but are a foregone conclusion.² See *Com. v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014) (“The facts that would be conveyed by the defendant through his act of decryption—his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key—already are known to the government and, thus, are a ‘foregone conclusion.’”).³

² Unlike compelling one to produce documents, requiring someone to produce a passcode to unlock a cell phone does not implicate a question of authenticity. See *State v. Stahl*, 206 So. 3d 124, 136 (Fla. 2d DCA 2016) (“[W]e must recognize that the technology is self-authenticating—no other means of authentication may exist. If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.” (citation omitted)); *Com. v. Gelfgatt*, 11 N.E.3d 605, 616 n.14 (Mass. 2014) (“Here, the defendant’s decryption of his computers does not present an authentication issue analogous to that arising from a subpoena for specific documents because he is not selecting documents and producing them, but merely entering a password into encryption software.”).

³ See also *State v. Andrews*, 197 A.3d 200, 207 (N.J. Super. Ct. App. Div. 2018), leave to appeal granted, No. 082209, 2019 WL 2011594 (N.J. May 3, 2019) (“[D]efendant’s Fifth Amendment right against self-incrimination is not violated by requiring him to disclose the passcodes for his iPhones, which the State lawfully possessed. The act of producing the passcodes has testimonial aspects because defendant is acknowledging ownership, possession, and control of the devices. He is also acknowledging he has the ability to access the contents of the phone. However, by producing the passcodes, defendant is not implicitly conveying any information the State does not already possess. Defendant is not telling the government something it does not already know. Therefore, the implicit facts conveyed by the act of producing the passcodes is a ‘foregone conclusion’ and compelled disclosure of the passcodes does not violate defendant’s Fifth Amendment right against self-incrimination.”); *Commonwealth v. Davis*, 176 A.3d

The question is not whether Pollard knows the password, but whether he must surrender it, *see Fisher*, 425 U.S. at 411, so the Fifth Amendment’s protection against self-incrimination does not apply.

III.

G.A.Q.L. focused on the contents of the phone when determining whether the testimony is a foregone conclusion. 257 So. 3d at 1063 (“[T]he object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall.”). The majority now follows suit.⁴ In this view, “it is not enough to know that a passcode wall exists, but rather, the state must demonstrate with reasonable particularity that what it is looking for is in fact located behind that wall” because “the ‘evidence sought’ in a password production case such as this is not the password itself; rather, it is the actual files or evidence on the

869, 876 (Pa. Super. Ct. 2017), appeal granted, 195 A.3d 557 (Pa. 2018) (citing, *inter alia*, *Apple MacPro Computer* and *Gelfgatt* and agreeing that the “appellant’s act of providing the password in question is not testimonial in nature and his Fifth Amendment right against self-incrimination would not be violated” where the appellant admitted that he knew the password to the computer).

⁴ The majority asserts that the “password-centric approach” “makes sense . . . where the state establishes that the testimonial value of the compelled password has been abandoned, such as where a defendant has voluntarily entered his passcode to access his cellphone in the presence of law enforcement such that the testimonial value of compelling the passcode’s production a second time is negligible,” and such a situation “becomes predominantly a Fourth Amendment issue, not a Fifth Amendment one[.]” Maj. op. at 8-9. This distinction is without a difference as applied to this case. If the analysis is properly focused on the accused’s knowledge of the passcode when he has entered it in the presence of law enforcement previously, there is no reason it should be centered elsewhere when the accused simply admits that he knows it and can enter it.

locked phone.” *Id.* at 1063-64.⁵ Thus, *G.A.Q.L.* holds, the state must identify with reasonable particularity the evidence on the phone to compel an accused to produce his password. *Id.* at 1064.

It is true that the state does not seek the passcode for itself, but as a means to access the files in the phone. This, however, does not change what the accused is being compelled to produce. *See, e.g., State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. Ct. App. Div. 2018), leave to appeal granted, No. 082209, 2019 WL 2011594 (N.J. May 3, 2019) (“Defendant argues the State is unaware of all of the possible contents of defendant’s devices. This is immaterial because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes.”). In no other context does the foregone-conclusion analysis focus on evidence other than the evidence being compelled, and there is no reason to shift the focus now.

G.A.Q.L. is correct that the state must identify with particularity the files on the phone it seeks. But when these files are not what the state is compelling production of, the Fifth Amendment is not implicated. The Fifth Amendment does not “protect[] private information obtained without compelling self-incriminating testimony[.]” *Fisher*, 425 U.S. at 400. “Insofar as private information not obtained through compelled self-incriminating testimony is legally protected, its protection stems from other sources” such as “the Fourth Amendment’s protection

⁵ *G.A.Q.L.* drew on the analysis in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1349 (11th Cir. 2012), which found that the government failed to prove that it “knew to any degree of particularity what, if anything, was hidden behind the encrypted wall.” However, the Eleventh Circuit also found that the government did not show “any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives, that [the accused] has access to those files, or that he is capable of decrypting the files.” *Id.* In contrast, the state here had probable cause that the phone contained incriminating text messages, from which it obtained a warrant to seize the phone, and showed that the phone belonged to Pollard and that he knew the passcode to unlock it.

against seizures without warrant or probable cause,” the First Amendment’s protection against being compelled to disclose who you associate with, “or evidentiary privileges such as the attorney-client privilege.” *Id.* at 401.

The state’s obligation to describe with particularity the files it seeks is required because the “Fourth Amendment by its terms requires particularity in the [search] warrant[.]” *Groh v. Ramirez*, 540 U.S. 551, 557 (2004); *see also Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984) (“The uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional.”). Here, as in *G.A.Q.L.*, the validity of the search warrant and the Fourth Amendment are not at issue.

The Fourth Amendment protected Pollard’s phone from search and seizure until a search warrant issued. Whether Pollard must produce the passcode to his phone—enabling the state to search and seize what is already entitled to—depends on whether that compelled act is testimonial and self-incriminating. Here, the only testimonial aspect of the production—Pollard’s ownership and control of the phone—is undisputed and a foregone conclusion. The Fifth Amendment, contrary to the analysis of the majority and the Fourth District in *G.A.Q.L.*, does not provide any further quasi-Fourth-Amendment protections where the state is not compelling production of the phone or data on it and the state possesses a valid search warrant for the phone.⁶ *See United States v. Spencer*, No. 17-Cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26,

⁶ The Supreme Court explained the issue of privacy in relation to the Fourth and Fifth Amendments in *Fisher*, 425 U.S. at 400:

The Framers addressed the subject of personal privacy directly in the Fourth Amendment. They struck a balance so that when the State’s reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue. They did not seek in still another Amendment the Fifth to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination.

2018) (“To the extent Spencer contends that the government has not adequately identified the files it seeks” in the devices it compelled him to decrypt, “that is an issue properly raised under the Fourth Amendment, not the Fifth.”).⁷

IV.

In this case, we do not need to determine whether the state can sufficiently describe the evidence it seeks on the phone because the state has not compelled Pollard to produce that evidence and the Fourth Amendment is not at issue. Pollard argues that he may not be compelled to produce the passcode to his cell phone due to the Fifth Amendment’s Self-Incrimination Clause, but this argument fails where the testimonial component of the communication is undisputed. I would deny Pollard’s petition for writ of certiorari.

Stacy A. Scott, Public Defender, and Logan P. Doll, Assistant Public Defender, Gainesville, for Petitioner.

Ashley Moody, Attorney General, and Benjamin L. Hoffman, Assistant Attorney General, Tallahassee, for Respondent.

⁷ We need not decide whether the state may compel an accused to disclose his passcode orally or in writing. Several authorities have distinguished whether the state may “compel the defendant to disclose -- whether orally or in writing -- the actual password, as opposed to cases requiring merely physically entering it into the device.” *Commonwealth v. Jones*, 117 N.E.3d 702, 710 n.9 (Mass. 2019); *see also G.A.Q.L.*, 257 So. at 1061-62 (Kuntz, J., concurring in result) (concluding “that the foregone conclusion doctrine cannot apply to compelled oral testimony”). Here, Pollard does not distinguish between the act of entering the passcode and disclosure of the passcode orally or in writing. Instead, he argues that the passcode and phone data are so intertwined that the proper inquiry concerns the state’s knowledge of the data on the phone. As stated above, I disagree with this position.

FIRST DISTRICT COURT OF APPEAL
STATE OF FLORIDA

No. 1D18-4572

MATTHEW TYLER POLLARD,

Petitioner,

v.

STATE OF FLORIDA,

Respondent.

Petition for Writ of Prohibition—Original Jurisdiction.

December 23, 2019

ON MOTION FOR REHEARING AND CERTIFICATION

MAKAR, J.,

The State has filed a motion for rehearing and certification, which we grant in part by certifying the following questions of great public importance:

WHAT IS THE PROPER LEGAL INQUIRY WHEN THE STATE SEEKS TO COMPEL A SUSPECT TO PROVIDE A PASSWORD TO THE SUSPECT'S CELLPHONE IF THE SUSPECT HAS NOT PREVIOUSLY GIVEN UP HIS FIFTH AMENDMENT PRIVILEGE IN THE PASSWORD? WHAT LEGAL STANDARD APPLIES IN DETERMINING WHETHER THE FOREGONE CONCLUSION APPLIES TO COMPELLED PRODUCTION OF PASSWORDS IN THESE SITUATIONS?

The State's motion for rehearing is narrow and limited solely to our jurisdiction in this case and seeks no substantive changes on the merits of the constitutional issue. Concluding that jurisdiction exists, we deny the motion.

The State's motion for certification of conflict does not ask for any substantive changes to our opinion either. It urges, instead, that our opinion conflicts with the decision in *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016), because it adopted the approach in *G.A.Q.L. v. State*, 257 So. 3d 1058, 1062 (Fla. 4th DCA 2018), a case that disagreed with *Stahl* but neither certified conflict nor a question of great public importance. Certification presents a close question, but the factual differences in those cases and this case, such as whether a defendant has given up his testimonial privilege, make them distinguishable such that no *direct* conflict exists within the meaning of article V, section 3(b)(4), Florida Constitution. We therefore deny the motion for certification of conflict. That said, the proper approach to analyzing compelled password production needs clarification, which is why a question of great public importance has been certified.

Despite the narrow focus of the State's motion, our dissenting colleague presents many pages of arguments—old and new—that amount to a second opinion on the merits. Tellingly, our colleague's almost exclusive focus is on the Fourth Amendment and probable cause despite *no party mentioning either of them* in their merits briefs and the State advancing no argument on such matters in its motion for rehearing and certification. And whether the probable cause affidavit (which sought to seize broad categories of information from the cellphone—without identifying any specific item—on the basis that criminals use cellphones) was proper or a fishing expedition matters not; we fail to see how the issuance of a subpoena or warrant—whether carefully drawn or a fishing expedition—negates the Fifth Amendment's protections, which are the focus of this case.

If anything, the relationship that exists between the Fifth Amendment right against compelled personal disclosures and its neighboring and complementary Fourth Amendment right against unreasonable searches and seizures counsels in favor of protection

against governmental overreach into individual autonomy in criminal cases. LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT 431 (1968) (“With good reason the Bill of Rights showed a preoccupation with the subject of criminal justice. The framers understood that without fair and regularized procedures to protect the criminally accused, there could be no liberty.”). As expressed in our original opinion, the expansion of governmental powers to compel disclosures of personally-held information to search person’s homes and personal effects, as reflected in *Stahl* and our dissenting colleague’s view, is the antipode of the original understanding of the Fifth Amendment, which protected individual freedom by prohibiting compelled disclosures used to incriminate an accused. See Donald Dripps, *Self-Incrimination*, in THE HERITAGE GUIDE TO THE CONSTITUTION 437-439 (David F. Forte & Matthew Spalding eds., 2d ed. 2014); see also LEVY, at 432 (“Above all, the Fifth Amendment reflected [the framers’] judgment that in a free society, based on respect for the individual, the determination of guilt or innocence by just procedures, *in which the accused made no unwilling contribution to his conviction*, was more important than punishing the guilty.”) (emphasis added). At its core, the debate in *Stahl*, *G.A.Q.L.*, and this case is about which vision of the right against compelled testimony prevails: those of the Founders who erred on the side of personal liberty or those who defend state powers to extract testimony and see no problem in “merely compel[ling a defendant] to unlock [a] phone by entering the passcode himself.”

JAY, J., concurs; WINOKUR, J., concurs in part and dissents in part with opinion.

Not final until disposition of any timely and authorized motion under Fla. R. App. P. 9.330 or 9.331.

WINOKUR, J., concurring in part and dissenting in part.

I concur in the Court’s decision to certify questions of great public importance to the Florida Supreme Court. I believe that it is appropriate to add some additional insight into why this question is important enough to merit certification. I also concur in the decision to deny rehearing. However, I dissent from the decision to deny certification of conflict with *State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016).

Great Public Importance

I find that the State’s motion reveals that one of the central issues in this case is the contention that the State’s attempt to access data on Pollard’s phone “amount[s] to a mere fishing expedition.” *Pollard v. State*, 44 Fla. L. Weekly D1573, D1576 (Fla. 1st DCA June 20, 2019) (citing *G.A.Q.L. v. State*, 257 So. 3d 1058, 1064 (Fla. 4th DCA 2018)). The use of this phrase suggests that the State had nothing but sheer hope that the phone contained evidence of a crime. But if this were true, the State could not have obtained a warrant to seize and search the phone. In order to obtain the search warrant, police had to demonstrate to a magistrate that it had probable cause to believe that the phone contained evidence of a crime; that is, that there was a “reasonable probability that contraband will be found” on the phone. *Pagan v. State*, 830 So. 2d 792, 806 (Fla. 2002). The State met this standard by introducing evidence—including a co-defendant’s admission that the robbery Pollard allegedly participated in was planned via text message—indicating that incriminating evidence existed on Pollard’s phone. No “mere fishing expedition” was involved.

The majority draws this language from *G.A.Q.L. v. State*, which in turn cited *United States v. Hubbell*, 530 U.S. 27, 44 (2000). But in *Hubbell*, the Government sought information by subpoena, not by search warrant. The Government never had to make a showing that it had probable cause to seize the disputed documents; it merely issued a grand jury subpoena to Hubbell. *Id.* at 31. The Supreme Court approved the District Court’s characterization of the subpoena as a “fishing expedition” because the Government could not state with “reasonable particularity a prior awareness that the [documents] sought existed and were in Hubbell’s possession.” *Id.* at 32-33. In that context, this finding meant the demand for documents violated Hubbell’s rights,

because the Government was merely compelling Hubbell to provide incriminating information without knowing what those documents might reveal, rather than seeking documents it could already identify without forcing Hubbell to produce them. This is why the Court characterized the Government's demand as a "fishing expedition."

Nothing of the sort occurred here. The State did not merely issue a subpoena for Pollard's phone with a hunch that it might provide incriminating information. Rather, the State introduced evidence showing, to a magistrate's satisfaction, that probable cause existed that Pollard's phone contained evidence of a crime. This evidence was what they sought, not the passcode that is the subject of this petition.

It is true that the *Hubbell* Court wrote that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Id.* at 43 (emphasis supplied). The majority opinion suggests that this passage states a general rule that a requirement to tell police a "combination" violates the right against self-incrimination. I submit this claim misreads *Hubbell*. The State here was not asking Pollard to "assemble" anything. It already had probable cause that incriminating information was located on the phone. Compelling Pollard to provide the passcode in order to access this incriminating information is more like forcing him to surrender a key than embarking on a "fishing expedition" for unknown information.¹ In short, I believe that the characterization of the State's request as a "fishing expedition," and its relation to the foregone conclusion exception, amplify why this case is of great

¹ It is worth repeating that the opinion does not address whether it would be improper for the State to merely compel Pollard to unlock the phone by entering the passcode himself. And if this is not improper, then the demand for the passcode, which accomplishes the same result, cannot be deemed a "fishing expedition."

public importance, especially since the same point was made in *G.A.Q.L.*²

Certification of Conflict

In *Stahl*, the Second District concluded that the foregone conclusion exception applied to permit compulsion because the State proved that the passcode existed, the defendant knew it, and the passcode was self-authenticating:

To know whether providing the passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has established that it knows with reasonable particularity that the *passcode* exists, is within the accused's possession or control, and is authentic. The question is not the State's knowledge of the contents of the phone; the State has not requested the contents of the phone or the photos or videos on Stahl's phone. The State established that the phone could not be searched without entry of a passcode. A passcode therefore must exist. It also established . . . that the phone was Stahl's and therefore the passcode would be in Stahl's possession. That leaves only authenticity. And as

² Admittedly, it is unclear whether the majority still adheres to this view. In its opinion, the majority ruled that the State's failure to "describe with reasonable particularity" the information it sought on Pollard's phone made its request a "mere fishing expedition," which invalidated the applicability of the foregone conclusion exception to Fifth Amendment rights. *Pollard*, 44 Fla. L. Weekly at D1576. But in its opinion on rehearing, the majority contends "whether the probable cause affidavit . . . was proper or a fishing expedition matters not," and that the specificity of the warrant is irrelevant to Pollard's Fifth Amendment protections. Maj. op. on rehearing at 2. If the majority now contends that a supposed lack of specificity of the warrant does not matter to the outcome of this case, then I agree. However, without this fact, the foregone conclusion exception requires disclosure.

has been seen, the act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating—no other means of authentication may exist. If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.

206 So. 3d at 136 (citations omitted).

Similarly here, it is undisputed that the passcode existed and that Pollard knew it; the answers to the determinative questions in *Stahl* are the same. However, the majority applied a different analysis by questioning how precisely the State could identify the evidence it sought on the phone, rather than by focusing on the passcode as *Stahl* did. The majority consequently came to a different conclusion, finding that “unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communications, data and images ‘amount[s] to a mere fishing expedition.’” *Pollard*, 44 Fla. L. Weekly at D1576 (quoting *G.A.Q.L.*, 257 So. 3d at 1064). Had this Court applied the holding of *Stahl*, we would have denied the petition for certiorari, but the majority employed a different analysis and granted certiorari. As such, the majority’s opinion directly conflicts with *Stahl*.

The majority attempted to distinguish *Stahl* by stating that Stahl “initially agreed to allow police to search the phone, thereby inferring his knowledge of the passcode and its authenticity,” finding that the Second District held “that the suspect’s actions disclosed or authenticated the password sought (here by Stahl initially agreeing to allow police to access the phone),” thus making authentication a foregone conclusion, and concluding that Pollard, conversely, had never “previously given up his privilege in the password sought.” *Id.* at D1575. This argument fails for two reasons.

First, Stahl initially consented to a search of his cellphone before withdrawing his consent after police recovered the

cellphone from his house, thus requiring the State to obtain a search warrant. *Stahl*, 206 So. 3d at 128. The State then found that it could not view the contents of the phone and moved to compel Stahl to produce his passcode. *Id.* It is clear that Stahl's initial consent was a waiver of his Fourth Amendment rights against unreasonable searches, requiring the State to obtain a search warrant. If Stahl had maintained his consent and handed his phone to the State, the State still could not have viewed the information inside it without obtaining the passcode. Thus, the majority's assertion that Stahl "had previously given up his privilege in the password sought," *Pollard*, 44 Fla. L. Weekly at D1575, is without support and further conflates the Fourth Amendment and Fifth Amendment protections. Regardless, *even if* Stahl had stated that he would provide his passcode before changing his mind, the majority provides no logical reason why we would use a passcode-centric approach to the foregone conclusion exception then, while utilizing a completely different content-centric approach when a defendant like Pollard simply admits that he knows the passcode to his phone (but does not briefly say he will provide it before changing his mind). This factual distinction is unsupported and would be meritless if it was.

Second, contrary to the majority opinion's assertion, *Stahl* did not hold that the authenticity requirement was satisfied because he "disclosed or authenticated the password sought" when he initially provided consent to search his phone; as discussed above, he never mentioned a passcode when he waived his Fourth Amendment rights. *Id.* The Second District found that the foregone conclusion exception "cannot be seamlessly applied to passcodes and decryption keys" without "recogniz[ing] that the technology is self-authenticating—no other means of authentication may exist." *Stahl*, 206 So. 3d at 136. *Stahl* concluded that "[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." *Id.* Despite the majority's contention, *Stahl* is clear that its ruling is based on the passcode's self-authentication rather than any purported disclosure of the password. This ruling is in clear conflict with the majority's conclusion that "simply because a compelled password unlocks a cellphone after the fact doesn't make it authentic ex ante." *Pollard*, 44 Fla. L. Weekly at D1575.

The majority decision is in direct conflict with *Stahl*, so I would grant the State's motion to certify conflict.³

Stacy A. Scott, Public Defender, and Logan P. Doll, Assistant Public Defender, Gainesville, for Petitioner.

Ashley Moody, Attorney General, Benjamin L. Hoffman, Assistant Attorney General, Edward Wenger, Chief Deputy Solicitor General, and Christopher Baum, Deputy Solicitor General, Tallahassee, for Respondent.

³ The majority suggests I have turned my back on “the Founders” and their commitment to personal liberty and sees my position as “defend[ing] state powers to extract testimony.” Maj. op. on rehearing at 2-3. I disagree with the majority that this case turns on one’s “vision” of the Fifth Amendment. Rather, it turns on the application of the foregone conclusion exception established by the United States Supreme Court, which we cannot contradict even if it conflicts with our personal conception of the United States Constitution.



DISTRICT COURT OF APPEAL
FIRST DISTRICT
STATE OF FLORIDA
2000 DRAYTON DRIVE
TALLAHASSEE, FLORIDA 32399-0950
(850) 488-6151

KRISTINA SAMUELS
CLERK OF THE COURT

DANA SHARMAN
CHIEF DEPUTY CLERK

January 22, 2020

Re: Matthew Tyler Pollard vs State of Florida
Appeal No: 1D18-4572
Trial Court No.: 01-2018-CF-2174-A
Trial Court Judge: Hon. N/A

Dear Mr. Tomasino:

Attached is a certified copy of the Notice Invoking the Discretionary Jurisdiction of the Supreme Court, pursuant to Rule 9.120, Florida Rules of Appellate Procedure. Attached also is this Court's opinion or decision relevant to this case.


- ☐ The filing fee prescribed by Section 25.241(2), Florida Statutes, was received by this court and is attached.
- ☐ The filing fee prescribed by Section 25.241(2), Florida Statutes, was not received by this court.
- ☒ Petitioner/Appellant has previously been determined insolvent by the circuit court or our court in the underlying case.
- ☐ Petitioner/Appellant has already filed, and this court has granted, petitioner/appellant's motion to proceed without payment of costs in this case.

No filing fee was required in the underlying case in this court because it was:

- ☐ A summary Appeal, pursuant to Rule 9.141
- ☐ From the Unemployment Appeals Commission
- ☐ A Habeas Corpus proceeding
- ☐ A Juvenile case
- ☐ Other _____

If there are any questions regarding this matter, please do not hesitate to contact this Office. **A motion postponing rendition pursuant to Florida Rule of Appellate Procedure 9.020(i) _____ is or ☒ is NOT pending in the lower tribunal at the time of filing this notice.**

Sincerely yours,


Kristina Samuels
Clerk of the Court

By: 
Deputy Clerk