DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FOURTH DISTRICT

G.A.Q.L., a minor,
Petitioner,

v.

STATE OF FLORIDA,
Respondent.

No. 4D18-1811

[October 24, 2018]

Petition for writ of certiorari to the Circuit Court for the Seventeenth Judicial Circuit, Broward County; Andrew L. Siegel, Judge; Investigation No. 18-03-000966.

Eric T. Schwartzreich of Schwartzreich & Associates, P.A., Fort Lauderdale, and Jason Alan Kaufman of Kaufman Legal Group, P.A., Fort Lauderdale, for petitioner.

Pamela Jo Bondi, Attorney General, Tallahassee, and Anesha Worthy, Assistant Attorney General, West Palm Beach, for respondent.

LEVINE, J.

Two passcodes stand in the way of the state accessing the contents of a phone alleged to belong to a minor. The state sought, and the trial court agreed, to compel the minor to provide two passcodes, finding that "the act of producing the passcodes is not testimonial because the existence, custody, and authenticity of the passcodes are a foregone conclusion." We disagree. The minor is being compelled to "disclose the contents of his own mind" by producing a passcode for a phone and a password for an iTunes account. Further, because the state did not show, with any particularity, knowledge of the evidence within the phone, the trial court could not find that the contents of the phone were already known to the state and thus within the "foregone conclusion" exception. We grant the minor's petition for writ of certiorari and quash the trial court's order compelling the disclosure of the two passcodes.

The minor was speeding when he crashed. One of the passengers in his car died in the crash. At the hospital, the police had a blood test performed, showing that the minor had a .086 blood-alcohol content.

After obtaining a search warrant for the vehicle, the police located two iPhones. One iPhone belonged to a surviving passenger. The surviving passenger told police that the group had been drinking vodka earlier in the day and that she had been communicating with the minor on her iPhone.

The second phone, an iPhone 7, was alleged to have belonged to the minor. The police obtained a warrant to search the phone for data, photographs, assigned numbers, content, applications, text messages, and other information. After obtaining a warrant to search this iPhone, the police sought an order compelling the minor to provide the passcode for the iPhone and the password for an iTunes account associated with it.

In its first motion, the state identified the iPhone and "request[ed] the court compel production of the passcode for the minor's cellular phone." In its second motion, the state sought to compel the minor to produce an iTunes password. This was necessary, the state argued, because the phone could not be searched before receiving a software update from Apple's iTunes service. Thus, the state needed both the passcode to access the phone and the iTunes password to update it.

At a hearing on the motions, the state noted that the surviving passenger from the car crash had provided a sworn statement that on the day of the crash and in the days following the crash, she had communicated with the minor via text and Snapchat. The passenger had also told police that she and the minor had been consuming alcoholic beverages the day of the crash. As such, the state needed the phone passcode and iTunes password to obtain any possible communications between the defendant and the surviving passenger.

The minor argued that compelling disclosure of the iPhone passcode and iTunes password violated his rights under the Fifth Amendment to the United States Constitution. The trial court disagreed and concluded in its order that the minor's "passcodes are not testimonial in and of themselves. *See State v. Stahl*, 206 So. 3d 124, 134 (Fla. 2d DCA 2016). The passcodes merely allow the State to access the phone, which the State has a warrant to search. *See id.*" According to the trial court, the state had established the "existence, possession, and authenticity of the documents" it sought. Thus, the "existences of the passcodes in the instant case is a foregone

conclusion." Finally, the trial court determined that the act of producing the passcode and password was not testimonial. As a result, the trial court granted the state's motions to compel.

The minor petitioned for writ of certiorari to quash the circuit court's order. This court has jurisdiction to issue a writ of certiorari under article V, section 4(b)(3) of the Florida Constitution. *See also Appel v. Bard*, 154 So. 3d 1227, 1228 (Fla. 4th DCA 2015) (granting certiorari to review order compelling answers to deposition questions and overruling Fifth Amendment privilege objections); *cf. Boyle v. Buck*, 858 So. 2d 391, 392 (Fla. 4th DCA 2003). Our standard of review when considering whether to issue such a writ is "whether the trial court . . . departed from the essential requirements of law." *Anderson v. E.T.*, 862 So. 2d 839, 840 (Fla. 4th DCA 2003) (citation omitted). To warrant a writ of certiorari, "there must exist (1) a departure from the essential requirements of the law, (2) resulting in material injury for the remainder of the case (3) that cannot be corrected on postjudgment appeal." *Reeves v. Fleetwood Homes of Fla., Inc.*, 889 So. 2d 812, 822 (Fla. 2004) (citation and internal quotation marks omitted).

Compelled Production of the Passcodes

This case is governed by the Fifth Amendment to the United States Constitution, which states: "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ." U.S. Const. amend. V; *see also* Fla. Const. art. I, § 9. The Fifth Amendment proscribes the compelled production of an incriminating testimonial communication. *Fisher v. United States*, 425 U.S. 391, 408 (1976).

"[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself." *Doe v. United States*, 487 U.S. 201, 210 (1988) (footnote omitted). As such, acts like furnishing a blood sample, providing a voice exemplar, wearing an item of clothing, or standing in a line-up are not covered by this particular Fifth Amendment protection, for they do not require the suspect to "disclose any knowledge he might have" or "speak his guilt." *Id.* at 211 (citation omitted). In other words, the Fifth Amendment is triggered when the act compelled would require the suspect "to disclose the contents of his own mind" to explicitly or implicitly communicate some statement of fact. *Curcio v. United States*, 354 U.S. 118, 128 (1957).

In his famous dissent in *Doe*, Justice Stevens utilized an analogy to describe the scope of the Fifth Amendment protection against self-incrimination: "[A defendant] may in some cases be forced to surrender a

key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed." *Doe*, 487 U.S. at 219 (Stevens, J., dissenting). Applying this analogy to the act of producing documents responsible to a subpoena, the Supreme Court once observed, "[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." *United States v. Hubbell*, 530 U.S. 27, 43 (2000). Thus, when the compelled act is one of testimony rather than simple surrender, the Fifth Amendment applies. *See Fisher*, 425 U.S. at 411.

This analogy has been invoked with some frequency as courts have grappled with whether being forced to produce a phone password is more akin to surrendering a key or revealing a combination. *See, e.g., State v. Stahl*, 206 So. 3d 124 (Fla. 2d DCA 2016); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012); *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010); *Seo v. State*, No. 29A05-1710-CR-2466, 2018 WL 4040295 (Ind. Ct. App. Aug. 21, 2018).

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

In accepting this interpretation of Fifth Amendment doctrine, we disagree with the Second District's *Stahl* opinion. In *Stahl*, officers sought to search a defendant's locked phone, but the defendant refused to give them his passcode. 206 So. 3d at 128. The Second District concluded that making the defendant reveal his passcode was not testimonial, as the passcode was "sought only for its content and the content has no other value or significance," making communication of the passcode non-testimonial. *Id.* at 134. The court explicitly rejected the notion of

passcode-as-combination under the *Doe* analogy and determined that, although it did require the use of the defendant's mind, compelled unlocking of the phone via passcode was not a protected testimonial communication under the Fifth Amendment. *Id.* We disagree.

We find the Eleventh Circuit's decision in *In re Grand Jury Subpoena* to be instructive. In that case, John Doe was served a subpoena requiring him to decrypt several hard drives in his possession.[1] 670 F.3d at 1337. There, the court determined that compelled decryption of hard drives was testimonial in nature. *Id.* at 1346. In reaching this conclusion, the court noted that "decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." *Id.* Specifically addressing the "key" and "combination" analogy, the court likened the forced decryption to production of a combination because it is "accompanied by . . . implied factual statements" and utilized the contents of the mind with the final objective not of obtaining the decryption for its own sake, but for the purpose of obtaining the files protected by the encryption. *Id.*

Thus, this case is analogous to *In re Grand Jury Subpoena*. Here, the state seeks the phone passcode not because it wants the passcode itself,

[1] That this case involves the production of a passcode and password rather than decryption is of no consequence. With iPhones and many other smartphones, inputting a passcode chosen by the user is simply an abbreviated means of decrypting the phone's contents, which are automatically encrypted by the phone whenever it is locked:

> An encryption key is basically a very long string of numbers that is stored in the encryption software's memory. The software users do not have to remember this long number; instead [they] can enter a more easily remembered password or passphrase, which in turn activates the encryption key. When the government seeks to compel an ordinary citizen to turn over the means by which he can decrypt the data, the disclosure order will typically compel him to turn over his password rather than the encryption key.

Seo, 2018 WL 4040295 at *4 (quoting Michael Wachtel, *Give Me Your Password Because Congress Can Say So*, 14 U. Pitt. J. Tech. L. & Pol'y 44, 48 (2013)). In other words, the particular type of technology used to protect the information sought is not dispositive of whether the Fifth Amendment applies. Decryption and passcode production are thus governed by the same Fifth Amendment analysis.

but because it wants to know what communications lie beyond the passcode wall. If the minor were to reveal this passcode, he would be engaging in a testimonial act utilizing the "contents of his mind" and demonstrating as a factual matter that he knows how to access the phone. *See id.* As such, the compelled production of the phone passcode or the iTunes password here would be testimonial and covered by the Fifth Amendment. *Id.*

The Foregone Conclusion Exception

Having determined that the production of the passcode and password are covered by the Fifth Amendment, we now address whether the "foregone conclusion" exception would nevertheless allow the state to compel the minor to reveal the passcode and password. We discuss this issue since the trial court applied the foregone conclusion exception below when it concluded that "the act of producing the passcodes is not testimonial because the existence, custody, and authenticity of the passcodes are a foregone conclusion." Although the foregone conclusion exception might apply in some circumstances, it does not apply here. The trial court therefore erred in relying on the foregone conclusion exception as a basis for allowing the production of the passcodes.

In general, if the state can meet the requirements of the foregone conclusion exception, it may compel otherwise ostensibly self-incriminating testimonial production of information. *Fisher*, 425 U.S. at 411; *In re Grand Jury Subpoena*, 670 F.3d at 1345-46. 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. *Id.* at 1346. 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.* at 1349 n.28.

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. *See id.* at 1349 (holding that foregone conclusion exception did not apply to compelled production of encrypted files because government could not show with "reasonable particularity" that files existed on the drive to which the individual who was subpoenaed had access). To find otherwise would expand the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment. For example, every password-

protected phone would be subject to compelled unlocking since it would be a foregone conclusion that any password-protected phone would have a passcode. That interpretation is wrong and contravenes the protections of the Fifth Amendment.

Below and on appeal, the state's argument has incorrectly focused on the passcode as the target of the foregone conclusion exception rather than the data shielded by the passcode, arguing that "because the State has established the existence of the passcode and iTunes password, evidence on the Petitioner's cell phone, and that he can access the content of his phone," the compelled search was acceptable. Similarly, the trial court specifically held that the "existence, custody, and authenticity of the passcodes are a foregone conclusion" in the order appealed. This holding, which focuses on the passcodes rather than the data behind the wall, misses the mark.

On this subject, we again disagree with the Second District. In *Stahl*, the court focused on the "reasonable particularity that the passcode exists," a fact that the state had established. 206 So. 3d at 136 (emphasis in original). However, this is not the proper focus of the inquiry—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. *See In Re Grand Jury Subpoena*, 670 F.3d at 1348-49. Contrary to the *Stahl* court's conclusion, which the trial court adopted,[2] 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 locked phone. *Compare Stahl*, 206 So. 3d at 135, *with In Re Grand Jury Subpoena*, 670 F.3d at 1347. Without reasonable particularity as to the documents sought behind the passcode wall, the facts of this case "plainly fall outside" of the foregone conclusion exception and amount to a mere fishing expedition. *Hubbell*, 530 U.S. at 44.

The concurrence, meanwhile, argues that the foregone conclusion exception could never be applied to compelled "oral testimony" in *any* case. Like *Stahl*, this view seems to misconstrue the object of the foregone conclusion exception. It is not the verbal recitation of a passcode, but rather the documents, electronic or otherwise, hidden by an electronic wall that are the focus of this exception. Further, it would seem unreasonable not to subject documents protected by a passcode to the foregone conclusion exception where the state compels the subject to orally recite a

---

[2] The trial court was obligated to follow *Stahl* below. *See Pardo v. State*, 596 So. 2d 665, 666 (Fla. 1992) ("[I]n the absence of interdistrict conflict, district court decisions bind all Florida trial courts.").

passcode, but allow the foregone conclusion exception to apply to protected documents where the state compels the subject, for example, to physically write down a password, effectively creating the document. In both scenarios the subject is compelled to disclose the "contents of his mind" by different modalities—written in one scenario and oral in the other—to the same inculpatory effect. *See Couch v. United States*, 409 U.S. 322, 328 (1973) ("It is extortion of *information* from the accused himself that offends our sense of justice.") (emphasis added). However, in any event, since the state did not know with "reasonable certainty" the electronic documents behind the wall, this is not dispositive to the resolution of this case.

Here, 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. The only possible indication that the state might be seeking anything more specific was the prosecutor's statement at the hearing that the surviving passenger had been communicating with the minor via Snapchat and text message on the day of the accident and after the accident, a fact that the trial court briefly mentioned in its order but did not appear to rely on in reaching its conclusion.

However, this stand-alone statement is not enough to meet the "reasonable particularity" requirement of the foregone conclusion exception. Even if the state had argued that the evidence on the phone was a foregone conclusion—which it did not—this record does not indicate that the state can say with reasonable particularity that the Snapchat and text files are located on the phone. 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. *Stahl*, 206 So. 3d at 135-36; *see also In re Grand Jury Subpoena*, 670 F.3d at 1347 ("[C]ategorical requests for documents the government anticipates are likely to exist simply will not suffice."). Thus, as was the case in *In re Grand Jury Subpoena*, the foregone conclusion exception is inapplicable. *See* 670 F.3d at 1349.

We also find *Seo* persuasive. Like in this case, there the state sought to compel a defendant to unlock her iPhone in order to search it. 2018 WL 4040295 at *2. After holding that doing so would implicate the Fifth Amendment, the Court of Appeals of Indiana concluded that the foregone conclusion exception did not apply. *Id.* at *11-12. It noted that the government seeking to compel the production of a passcode must "be able to describe with reasonable particularity the documents or evidence it

seeks to compel." *Id.* at *12. Importantly, the court observed that "[w]hat is being compelled here is not merely the passcode," but the contents of the phone that are instantly decrypted in their entirety upon inputting the passcode. *Id.* at *13. Because the state could not meet its burden of identifying the contents—that is, the actual phone data—sought with reasonable particularity, the foregone conclusion exception did not apply. *Id.*

The state here seeks to force the minor to produce the passcode and iTunes password for an iPhone. To do so would be to compel testimonial communications in violation of the minor's invocation of his Fifth Amendment rights. *See In re Grand Jury Subpoena*, 670 F.3d at 1346. Additionally, the trial court erred in relying on the foregone conclusion exception, as the requirements of that exception were not met. *See id.* at 1349. As such, we grant the minor's petition for writ of certiorari and quash the order of the trial court.

Petition granted; order quashed.

CIKLIN, J., concurs.
KUNTZ, J., concurs in result only with opinion.

KUNTZ, J., concurring in result.

I agree with the Court that the circuit court's order must be quashed, but I would do so on different grounds. The majority concludes that compelling the minor to reveal the passcode to his iPhone and the password to an unidentified iTunes account would require the minor to use the contents of his mind in violation of the Fifth Amendment. I agree with that conclusion. But the majority also holds that the State may overcome this violation of the minor's Fifth Amendment rights if the foregone conclusion exception applies. Slip Op. 6 (citing *Fisher v. United States*, 425 U.S. 391, 411 (1976); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1345-46 (11th Cir. 2012)).

"[A] person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the [Fifth Amendment] privilege." *United States v. Hubbell*, 530 U.S. 27, 35-36 (2000). But that same person cannot be compelled to offer oral incriminating testimony. *See, e.g.*, *United States v. Spencer*, 17-CR-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018) (footnote omitted) ("[T]he government could not compel Spencer to state the

password itself, whether orally or in writing."); *Virginia v. Baust*, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) ("[T]he Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same."); *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) ("[T]he government is not seeking documents or objects—it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password—that will be used to incriminate him.").

The foregone conclusion exception is a judicially created exception. *See Hubbell*, 530 U.S. at 44; *Fisher*, 425 U.S. at 411. It is not found within the Fifth Amendment. It is also a doctrine of limited application. *See Hubbell*, 530 U.S. at 44 ("Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it."). The Supreme Court has applied the foregone conclusion exception only when the compelled testimony has consisted of existing evidence such as documents.

But, here, the State sought to compel the oral production of the requested information. The foregone conclusion exception has not been applied to oral testimony, and for good reason. In *Fisher*, the court explained that compelling a taxpayer to produce documents "involves substantial compulsion. But it does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought." 425 U.S. at 409. Based on what the production in *Fisher* would not do, the Supreme Court allowed the government to compel the production of documents. *Id.* Requiring the accused to orally communicate to the government information maintained only in his mind would certainly compel oral testimony. So, in my view, the basis for granting the petition is not that the State failed to satisfy the requirements of the foregone conclusion exception. Rather, the petition should be granted because the foregone conclusion exception is inapplicable to the compelled oral testimony sought in this case.

In response, the majority states that "it would seem unreasonable not to subject documents protected by a passcode to the foregone conclusion exception where the state compels the subject to orally recite a passcode, but allow the foregone conclusion exception to apply . . . where the state compels the subject . . . to physically write down a password . . . ." Slip Op. 8. I agree it would be unreasonable to treat the two situations differently, as "the protection of the privilege reaches an accused's communications, whatever form they might take." *Schmerber v. California*, 384 U.S. 757, 763–64 (1966); *see also Spencer*, 2018 WL 1964588, at *2. I would therefore treat both situations identically and conclude the

foregone conclusion exception is inapplicable to both.

Finally, because I would conclude that the foregone conclusion doctrine cannot apply to compelled oral testimony, I would go no further. We need not address whether the forced decryption of a device would also violate the Fifth Amendment. *See* Slip Op. 5 n.1. That question should be left for another case, one where the State has sought the forced decryption of a device as a remedy.

* * *

Not final until disposition of timely filed motion for rehearing.