IN THE SUPREME COURT OF THE STATE OF FLORIDA

STATE OF FLORIDA, *Petitioner*, v. JOHNATHAN DAVID GARCIA, *Respondent*.	Orange County Circuit Court Case No. 2018-CF-005112-A-O District Court of Appeals Case No. 5D19-590 Supreme Court Case No. SC20-1419

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, ELECTRONIC FRONTIER FOUNDATION, AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

Review of the Decision of the District Court of Appeals,
on Appeal from a Judgment of the Circuit Court for Orange County,
Hon. Gail A. Adams, Judge

Opinion Filed: August 28, 2020
Author of Opinion: Lambert, J.
Before: Harris, J.; Grosshans, J.; and Lambert, J.

(*Counsel listed on next page*)

Daniel B. Tilley
Florida Bar No. 102882
American Civil Liberties Union
of Florida, Inc.
4343 West Flagler St., Suite 400
Miami, FL 33134
(786) 363-2714
dtilley@aclufl.org

Counsel for Amici Curiae

Jo Ann Palchak
Florida Bar No. 22826
Vice-Chair, Amicus Committee
National Association of Criminal
Defense Lawyers
The Law Office of Jo Ann Palchak,
P.A.
1725 1/2 E. 7TH Avenue, Suite 6
Tampa, Florida 33605
(813) 468-4884
jpalchak@palchaklaw.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

AMICI STATEMENT OF INTEREST

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation's civil rights laws. The ACLU of Florida is the local affiliate of the ACLU that has a long-standing interest in protecting Floridians' rights to privacy. The ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as both counsel and *amicus* in various cases addressing the Fifth Amendment right against self-incrimination and the compelled decryption of digital devices, *see Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019) (counsel), *cert. denied*, 141 S. Ct. 237 (U.S. Oct. 5, 2020); *Eunjoo Seo v. State*, 148 N.E.3d 952 (Ind. 2020) (amicus); *State v. Andrews*, 234 A.3d 1254 (N.J. 2020) (amicus), *cert. denied*, 2021 WL 1951804 (U.S. May 17, 2021) (No. 20-937) (co-counsel).

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF represents

the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF is particularly interested in ensuring that individuals, and their constitutional rights, are not placed at the mercy of advancements in technology. EFF has appeared as both counsel and amicus in various cases addressing the Fifth Amendment right against self-incrimination and the compelled decryption of digital devices, *Eunjoo Seo*, 148 N.E.3d at 958 (amicus); *Andrews*, 234 A.3d at 1254 (amicus), *cert. denied*, 2021 WL 1951804 (co-counsel); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (amicus).

The National Association of Criminal Defense Lawyers ("NACDL" or the "Association") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates comprised of private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL has a particular interest in cases that involve surveillance technologies and programs that pose new challenges to personal privacy. NACDL operates the Fourth Amendment Center and has filed numerous

amicus briefs on issues involving digital privacy rights, including *Carpenter*, 138 S. Ct. at 2206; *Riley v. California*, 573 U.S. 373 (2014); and *United States v. Jones*, 565 U.S. 400 (2012).

ARGUMENT SUMMARY

This case presents questions of first impression in this Court: whether the privileges against self-incrimination found in Article I, Section 9 of the Florida State Constitution and the Fifth Amendment to the United States Constitution preclude the State from forcing a criminal defendant to recall and provide the passcode to his encrypted cell phone, thereby delivering the phone's contents to the government for use against him in a criminal proceeding. The Circuit Court's order authorizing such compulsion runs against long-standing precedent holding that the State cannot compel a suspect to recall and share information that exists only in his mind. *See Curcio v. United States*, 354 U.S. 118, 128 (1957). The realities of the digital age only magnify the concerns that animate these state and federal privileges. Here, the Fifth District Court of Appeal upheld those privileges, holding that Mr. Garcia could not be compelled to deliver information to be used against him in his own prosecution. *Garcia v. State*, 302 So. 3d 1051, 1057 (Fla. 5th DCA 2020).

This Court should affirm the Fifth District's decision for several reasons. First, as the court below, the First and Fourth District Courts of Appeal, and numerous other state and federal courts have held, the passcode to a cell phone is testimonial for purposes of the Fifth Amendment

because it requires the disclosure of the "contents of one's mind." *Id.* at 1055; *see also Varn v. State*, No. 1D19-1967, 2020 WL 5244807, at *3–*4 (Fla. 1st DCA Sept. 3, 2020); *Pollard v. State*, 287 So. 3d 649, 651 (Fla. 1st DCA 2019); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1064 (Fla. 1st DCA 2018). Second, as the court below and several other state supreme and appellate courts have also held, the narrow foregone-conclusion limitation to the act-of-production doctrine—only once ever applied by the United States Supreme Court to excuse government compulsion over a claim of the Fifth Amendment privilege—has no application beyond "already known and existing business or financial documents." *Garcia*, 302 So. 3d at 1056. Third, despite the government's dire-sounding warnings, there are alternative methods to access encrypted phones.

The Fifth District's decision below rightfully prevented law enforcement from enlisting a criminal defendant as a witness against himself. This Court should uphold that decision and extend that protection to all Floridians.

ARGUMENT

I. COMPELLING A CRIMINAL SUSPECT TO DISCLOSE A PASSCODE IS TESTIMONY PRIVILEGED BY THE FIFTH AMENDMENT.

A. The Fifth Amendment Prohibits Compelled Disclosure of the Contents of a Suspect's Mind.

The Fifth Amendment guarantees that "[n]o person shall be … compelled in any criminal case to be a witness against himself." Amend. V, U.S. Const. To invoke the privilege, an individual must show that the evidence sought is (1) compelled, (2) testimonial, and (3) self-incriminating. *United States v. Hubbell*, 530 U.S. 27, 34 (2000). Testimonial evidence is the communication of any information, direct or indirect, verbal or non-verbal, that requires a person to, by "word or deed," *Doe v. United States* (*Doe II*), 487 U.S. 201, 219 (1988) (Stevens, J., dissenting), use "the contents of his own mind" to truthfully relay facts. *Hubbell*, 530 U.S. at 43 (citing *Curcio*, 354 U.S. at 128); *see also Doe II*, 487 U.S. at 219 n.1 (Stevens, J., dissenting) (explaining that the Fifth Amendment protects against compelled "intrusion[s] upon the contents of the mind of the accused" because they "invade the dignity of the human mind").

The Fifth District Court of Appeal correctly recognized that, by demanding that Mr. Garcia "utilize the contents of his mind" to provide the passcode to his device, the State is not seeking an act of production, but

rather compelled, self-incriminating testimony that is privileged under the Fifth Amendment. *Garcia*, 302 So. 3d at 1055.

B. Compelled Disclosure of the Passcode Is Testimonial.

The Circuit Court's order in this case violates the Fifth Amendment because it seeks to compel Mr. Garcia to provide testimony. The First District succinctly stated the issue: "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." *Pollard*, 287 So. 3d at 653. Compelled disclosure of a password constitutes a modern but straightforward form of testimony, which is categorically protected from compulsion under the state and federal privileges against self-incrimination.

Like the First, Fourth, and now Fifth District Courts of Appeal have all held, the compelled disclosure of a password is indeed testimonial. *See Garcia*, 302 So. 3d at 1055; *G.A.Q.L.*, 257 So. 3d at 1061–62; *Pollard*, 287 So. 3d at 653. All three districts recognized that, "[d]istilled to its essence," compelled decryption orders demand that a defendant "utilize the contents of his mind and disclose specific information regarding the passcode that will

likely lead to incriminating information." *Garcia*, 302 So. 3d at 1055; *see Pollard*, 287 So. 3d at 653; *G.A.Q.L.*, 257 So. 3d at 1062.

Years ago, the Eleventh Circuit Court of Appeals applied this principle, holding that "the decryption … of the hard drives would require the use of the contents of [the accused's] mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *In re Grand Jury Subpoena*, 670 F.3d at 1346. And the bulk of federal courts agree: production of computer passwords is testimonial because it requires the suspect "to divulge[,] through his mental processes[,] his password." *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); *see also, e.g.*, *Davis*, 220 A.3d at 549 (explaining that the Supreme Court's cases in this area "uniformly protect information arrived at as a result of using one's mind"); *United States v. Wright*, 431 F. Supp. 3d 1175, 1187 (D. Nev. 2020); *United States v. Warrant*, No. 19-MJ-71283-VKD-1, 2019 WL 4047615, at *2 (N.D. Cal. Aug. 26, 2019); *SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644,

at *3 (E.D. Pa. Sept. 23, 2015); *Commonwealth v. Baust*, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).

Very much an outlier among other courts across the country, this State's Second District has implied that the disclosure of a password is not testimonial. *State v. Stahl*, 206 So. 3d 124, 134 (Fla. 2d DCA 2016). In *Stahl*, the defendant was arrested for taking a voyeuristic video with his cell phone, and, after initially consenting to a search of a phone he identified as his own, he withdrew that consent. *Id.* at 127–28. Police thereafter sought a compelled decryption order to enable them to carry out a warrant to search the phone. *Id.* at 128. Reversing the trial court's denial of that request based on its conclusion that such an order would violate the defendant's Fifth Amendment privilege against self-incrimination, the Second District held that the password disclosure would not be testimonial because "the communication was sought only for its content and the content has no other value or significance." *Id.* at 134. Important to the court's conclusion was its finding that disclosure of the password "does not implicitly 'relate a factual assertion or disclose information.'" *Id.* (quoting *Doe II*, 487 U.S. at 210, 215).[1]

[1] In a holding that appears to be incompatible with this conclusion, the Second District went on to apply the foregone-conclusion rationale to the disclosure of the password, suggesting that there was a "testimonial communication implicit in the act of [producing the password]" and an

Amici disagree with the Second District's reasoning. First, compelled testimony does not require great mental effort to qualify for privilege, and next, the government need not be interested in the import of the testimony for its own sake. For example, in *Pennsylvania v. Muniz*, the United States Supreme Court held that a motorist suspected of intoxication could not be compelled to answer a question about the date of his own sixth birthday. 496 U.S. 582, 598–99 (1990). Law enforcement was not interested in the date itself (in fact, they knew it); rather, they sought his response as evidence of mental impairment. *Id.* at 599 & n.13. But the question still demanded a testimonial answer. *See also Allred v. State*, 622 So. 2d 984, 987 (Fla. 1993) (adopting *Muniz* rationale in holding that compelling a motorist to recite the alphabet would be testimonial because it was "the *content* (incorrect recitation) of the speech that is being introduced, rather than merely the *manner* (slurring) of speech" (emphasis in original)).

Moreover, as the Fourth District explained, "[t]he very act of revealing a password asserts a fact: that the defendant knows the password." *G.A.Q.L.*, 257 So. 3d at 1061. Password disclosure also inevitably implies that the defendant "knows how to access the phone." *Id.* at 1062. It most

---

exception to the Fifth Amendment privilege was needed. *Stahl*, 206 So. 3d at 135–36.

often implies that the defendant had control over the phone and was the person who created the content therein. Compelling password disclosure thus compels an individual to "relate … factual assertion[s] or disclose information." *Stahl*, 206 So. 3d at 134 (quoting *Doe II*, 487 U.S. at 210). And so long as that testimony provides a "link in the chain of evidence" needed to prosecute, it is privileged. *See Hubbell*, 530 U.S. at 38 (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951)).

Because compelled disclosure or entry of Mr. Garcia's passcode is both testimonial and self-incriminating, it is privileged by both the Fifth Amendment and Article I, Section 9—and it is constitutionally off-limits. *See State v. Horwitz*, 191 So. 3d 429, 439 (Fla. 2016) ("[T]he privilege against self-incrimination provided in the Florida Constitution offers *more* protection than the right provided in the Fifth Amendment to the United States Constitution." (emphasis in original)) (citation omitted). The analysis for such "core testimonial communications" should end here, *see Pollard*, 287 So. 3d at 657.

II. THE FIFTH DISTRICT PROPERLY DECLINED TO APPLY THE FOREGONE-CONCLUSION RATIONALE IN THIS CASE.

Even if the police know with reasonable certainty that someone committed a bank robbery, no one could credibly suggest that the suspect

could then be compelled to testify orally or in writing concerning an incriminating fact because it was a "foregone conclusion." That is because the Fifth Amendment does not allow the government to compel suspects to speak, write, type, or otherwise reproduce the contents of their minds to aid in their own prosecution. Notably, the *Muniz* Court did not conduct a foregone-conclusion inquiry when faced with the government's argument that the Fifth Amendment privilege did not protect a criminal defendant from being compelled to answer a question about his birthday. This was proper and unsurprising, since the Fifth Amendment prohibits compelled verbal testimony, regardless of whether investigators already know the answer.

Several courts, including the Fifth District below, have rightly concluded that permitting the narrow foregone-conclusion inquiry to bypass the bedrock constitutional privilege would "sound 'the death knell for a constitutional protection against compelled self-incrimination in the digital age.'" *Garcia*, 302 So. 3d at 1057 (quoting *Commonwealth v. Jones*, 117 N.E.3d 702, 724 (Mass. 2019) (Lenk, J., concurring)); *see also Eunjoo Seo*, 148 N.E.3d at 961; *Davis*, 220 A.3d at 549; *State v. Valdez*, 482 P.3d 861, 875 (Utah Ct. App. 2021); *Pollard*, 287 So. 3d at 657 (expressing skepticism about the application of the foregone-conclusion exception and noting that their analysis proceeded "[o]n the assumption that the foregone conclusion

applies to core testimonial communications"); *G.A.Q.L.*, 257 So. 3d at 1066 (Kuntz, J., concurring) (arguing foregone-conclusion should not apply where defendant compelled to "communicate to the government information maintained only in his mind"). This Court should likewise reject application of the foregone-conclusion analysis.

A. The Foregone-Conclusion Analysis Applies Only to the Production of Specified, Preexisting Business Records.

The foregone-conclusion analysis is exceedingly narrow and does not reach the compelled recollection and use of a passcode to unlock a device and deliver incriminating evidence to law enforcement. Instead, the foregone-conclusion inquiry helps define when an act of production is testimonial. In *Fisher v. United States*, the government sought to compel the production of documents created by accountants preparing the defendants' tax records and in possession of the defendants' attorneys. 425 U.S. 391, 412–13 (1976). The Supreme Court recognized that "[t]he act of producing evidence, [specifically documents,] in response to a subpoena … has communicative aspects" protected by the Fifth Amendment—including implicit admissions concerning the existence, possession, and authenticity of the documents produced. *Id.* at 410. Under the unique circumstances of the case, the Court held that the act of producing the subpoenaed documents

was not testimonial since the government had independent knowledge of the existence and authenticity of the documents. *Id.* at 412–13. However, even as the Court did so, it was careful to note that an order to "compel oral testimony" would violate the Fifth Amendment. *Id.* at 409. Thus, *Fisher* stands for the proposition that if (1) a subpoena demands production of a narrow category of business and financial documents, (2) production does not rely on or disclose the contents of one's mind, and (3) the state already has evidence of the facts communicated by the production, it may be able to compel the target's disclosure of those papers.

Unsurprisingly, given the highly specific factual circumstances in *Fisher*, in the forty-five years since the case was decided, the Supreme Court has never again held that an act of production is unprotected by the Fifth Amendment because the testimony it implies is a foregone conclusion. Indeed, the Court has only even considered foregone-conclusion arguments in two other cases where the government sought to compel the production of preexisting business or other financial records, and it rejected them both times. *See Hubbell*, 530 U.S. at 44–45 (holding that the case "plainly [fell] outside of" the foregone-conclusion rationale where the government sought "broad categories" of "general business and tax records" rather than specific, known files); *United States v. Doe* (*Doe I*), 465 U.S. 605, 612–14 (1984)

(rejecting application of the foregone-conclusion rationale where the subpoena sought several broad categories of general business records).

Comparing *Hubbell* to *Fisher* shows how limited a foregone conclusion analysis is, demonstrating that it does not apply when the state seeks to compel witnesses to speak or act in ways that rely on their memories and cognition. In *Hubbell*, the government subpoenaed broad categories of documents from the respondent. 530 U.S. at 40. The act of production established the existence, authenticity, and custody of produced documents, information the government was already able to prove, or did not need. *Id.* In other words, these matters were foregone conclusions. Nevertheless, the Court held that the Fifth Amendment privilege applied. Compliance with the subpoena required "mental and physical steps" and the obligation that the respondent "truthful[ly] reply to the subpoena." *Id*. at 42. When the Court stated that, "whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it," it was not because the facts implied by the act of production were as yet unknown to the prosecution. *Id.* at 44. Rather, in *Hubbell*, as here (and with all forced decryption cases), the

foregone-conclusion rationale does not apply because compliance requires mental effort beyond any acts of production.

It is unsurprising that the United States Supreme Court has never applied the foregone-conclusion rationale outside of cases involving specific, preexisting business and financial records. Indeed, these types of records constitute a unique category of material that, to varying degrees, have been subject to compelled production and inspection by the government for over a century. *See, e.g.*, *Braswell v. United States*, 487 U.S. 99, 104 (1988); *Shapiro v. United States*, 335 U.S. 1, 33 (1948).

Similarly, only once has this Court entertained the possibility of applying a foregone-conclusion inquiry—also in the context of corporate records—but decided the case on standing grounds instead. *See State v. Wellington Precious Metals, Inc.*, 510 So. 2d 902, 904–06 (Fla. 1987) (finding that an individual does not have standing to quash subpoena directed to a "corporate officer" seeking corporate records of a sole proprietorship). Other courts, too, have overwhelmingly applied the rationale only in cases concerning the compelled production of specific, preexisting business and financial records. *See, e.g.*, *United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (business and tax records); *United States v. Gippetti*, 153 F. App'x 865, 868–69 (3d Cir. 2005) (bank and credit-card

account records); *United States v. Bell*, 217 F.R.D. 335, 341–42 (M.D. Pa. 2003) ("tax avoidance" materials advertised on defendant business's website); *cf*. *Burt Hill, Inc. v. Hassan*, No. CIV.A.09-1285, 2010 WL 55715, at *2 (W.D. Pa. Jan. 4, 2010) (contents of electronic storage devices used by defendants while employed by plaintiff).

Here, the State sought an order compelling Mr. Garcia to recall and display or voice his memorized passcode to aid law enforcement in a search of his device. In other words, the State sought to "compel oral testimony," running against *Fisher*'s teaching that such a request violates the Fifth Amendment and is no mere act of production. *See Fisher*, 425 U.S. at 409.[2]

Some courts in this state and elsewhere have incorrectly equated such compulsion to an act of production. *See, e.g.*, *G.A.Q.L.*, 257 So. 3d at 1064 (nevertheless finding the testimonial aspects of the production privileged); *Stahl*, 206 So. 3d at 135; *Andrews*, 234 A.3d at 1273. Likewise, the Oregon Supreme Court applied *Fisher* to an order to enter (rather than speak or write) a password, in part, because it found that the act of entering the

[2] Compelling an individual to physically write down or enter a password likewise runs afoul of the Fifth Amendment, as "the protection of the privilege reaches an accused's communications, whatever form they might take." *G.A.Q.L.*, 257 So. 3d at 1066 (quoting *Schmerber v. California*, 384 U.S. 757, 763–64 (1966)).

password would not "expressly communicate a defendant's beliefs, knowledge, or state of mind." *State v. Pittman*, 479 P.3d 1028, 1044 (Or. 2021).

But these decisions fail to offer any compelling conclusions. As the Fourth District reasoned, the "object[s] of the foregone conclusion exception" are "documents, electronic or otherwise," rather than the "verbal recitation of the passcode." *G.A.Q.L.*, 257 So. 3d at 1063–64. Thus, it does not follow that the recitation itself is an act of production: the recitation divulges the contents of the mind and is pure testimonial disclosure. At bottom, these courts failed to contend with the fact that the compelled disclosure of "information from [a] person's mind" constitutes "core testimonial communication[]," not an act of production. *Pollard*, 287 So. 3d at 653, 657.

Furthermore, in rejecting the application of the foregone-conclusion rationale to a compelled decryption order, the Indiana Supreme Court outlined three additional important reasons to refrain from importing this doctrine. *Eunjoo Seo*, 148 N.E.3d at 958–59. First, the court explained that the compelled production of an unlocked smartphone implicates far greater privacy concerns than "a documentary subpoena for specific files," emphasizing that even the 13,120 pages of documents at issue in *Hubbell* "pales in comparison to what can be stored on today's smartphones." *Id.* at

959–60. Second, the court pointed out that even restricting the foregone-conclusion inquiry to those instances where the government can identify specific files with reasonable particularity may prove unworkable. *Id.* at 960–61. After all, in a wide-ranging search of a device like the one authorized here, officers may come across further password-protected websites or accounts within the device, or a cloud storage service that grants law enforcement a "windfall" of evidence they "did not already know existed." *Id.* at 961. Finally, the court adhered to the recent admonitions from the Supreme Court to tread cautiously when "confronting new concerns wrought by digital technology." *Id.* (quoting *Carpenter*, 138 S. Ct. at 2222). This Court should uphold the Fifth District and follow its counterparts in Indiana and Pennsylvania in ensuring that a rarely used exception does not "swallow the constitutional privilege." *Davis*, 220 A.3d at 549.

B. Even If the Foregone-Conclusion Rationale Could Apply in this Context, the State Must Describe with Reasonable Particularity the Incriminating Files It Seeks.

Even if the foregone-conclusion rationale could apply in cases involving passcodes, the state would have to show far more than the government says it does. Rather than simply demonstrating that an individual had *possession and control* over a passcode, the state must show with "reasonable particularity" that it "already [knows] of the materials [it will

uncover], thereby making any testimonial aspect a 'foregone conclusion.'" *In re Grand Jury Subpoena*, 670 F.3d at 1346. By contrast, where an act of production reveals information the state does not already know, compelling that act would violate the Fifth Amendment. *See Hubbell*, 530 U.S. at 45 (no foregone conclusion where government did not have "any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent").

The two federal Courts of Appeal that have applied the foregone-conclusion inquiry to password-protected digital devices have held that investigators must know and be able to describe with reasonable particularity the discrete, tangible contents of a device—not merely that the defendant knows the passcode. In *In re Grand Jury Subpoena*, the Eleventh Circuit held that an order requiring the defendant to produce a decrypted hard drive would be "tantamount to testimony by [the defendant] 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." 670 F.3d at 1346 (emphasis added). The government could not compel the defendant to produce the information under the foregone-conclusion rationale unless it could show with "reasonable particularity" the "specific file names" of the records sought, or,

at minimum, that the government seeks "a certain file," and can establish 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; *see also United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (finding the foregone-conclusion inquiry satisfied where the government had evidence *both* that contraband files existed on the devices and that the defendant could access them).

Other courts, including three within this state, have similarly held that law enforcement must know with reasonable particularity what information is on an encrypted device—not merely that the suspect knows the passcode. As the Fourth District has explained, "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." *G.A.Q.L.*, 257 So. 3d at 1063; *accord Pollard*, 287 So. 3d at 657; *Varn*, 2020 WL 5244807 at *3–*4 (unpublished). It is thus "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."

G.A.Q.L., 257 So. 3d at 1063–64; *see Huang*, 2015 WL 5611644, at *3; *see also Doe I*, 465 U.S. at 613 n.12.

The Second District erred in concluding that the government can overcome the Fifth Amendment privilege merely by showing that it has knowledge that a suspect has access to an encrypted digital device. *See Stahl*, 206 So. 3d at 136. The court concluded that this lower standard applied because the "State has not requested the contents of the phone or the photos or videos on Stahl's phone." *Id.* at 134. But *Hubbell* teaches that the government cannot compel the act of entering the password and proceed as if the contents of the device fell "like 'manna from heaven.'" 530 U.S. at 42. To get around the defendant's valid assertion of privilege, it must provide full "use and derivative-use immunity," *id.* at 46, which would place the contents of the device off limits. Even if the foregone-conclusion rationale could provide an alternative method to compel this testimony, the burden would be on the government to demonstrate it could learn of all derivative evidence through an independent, untainted source. *See, e.g.*, *Kastigar v. United States*, 406 U.S. 441, 443 (1972).

In sum, even if this Court were to conclude that a foregone-conclusion inquiry is appropriate, the State cannot compel Mr. Garcia to produce the

decrypted contents of his phone without first demonstrating with reasonable particularity that it knows what documents it will find there.

III. LAW ENFORCEMENT HAS ALTERNATIVE METHODS OF ACCESSING ENCRYPTED DEVICES.

The government claims that restricting its ability to compel defendants to produce passcodes will prove "disastrous," *see* Initial Br. on the Merits (Gov't Br.) 46, yet the technology exists for law enforcement to access information on electronic devices without compelling the production of a passcode. As the government here acknowledges, one option is to use mobile device forensic tools that are capable of breaking into devices, even those with passwords. *See* Gov't Br. 47–48 n.24; *see also* Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 27 (2020).[3] One vendor, Cellebrite, supports extraction for over 8,000 devices, and of the major phone manufacturers, its software has the most widespread support for Samsung devices. *Id.* at 26. Cellebrite listed the capability to break into the Samsung Note Galaxy 8, the

[3] Available at: https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf.

phone at issue here, as of July 2019.[4] It is unclear if the Orange County Sheriff's Office has one of these tools, but at least one of their employees claims to hold multiple credentials from Cellebrite, including as a "Cellebrite Certified Operator."[5] Similarly, a detective from the Orlando Police Department is a Cellebrite instructor. *See* Heather Mahalik, *How to Access Android and iOS System Log Files for Evidence*, Cellebrite (May 13, 2020)[6]. And the nearby city of Kissimmee also appears to have purchased one of these tools. Koepke et al. at 33.[7]

The investigating officers here appear to have made no attempt to avail themselves of such forensic tools. Nor has the State shown, given the widespread availability of forensic tools, that respecting the Fifth Amendment privilege would pose an obstacle in the vast majority of investigations. *See Riley*, 573 U.S. at 401 (constitutional rights are "not merely 'an inconvenience

---

[4] *Supporting New Samsung Devices and Data Sources*, Cellebrite (July 17, 2019), https://www.cellebrite.com/en/productupdates/supporting-new-samsung-devices-data-sources-and-encrypted-drones/.

[5] Viet Pham, *Records & Identification Manager at Orange County Sheriff's Office*, LinkedIn, https://www.linkedin.com/in/phamviet (last visited June 21, 2021).

[6] Available at: https://www.cellebrite.com/en/android-and-ios-system-log-files-ed-michael-detective-at-the-orlando-police-department/.

[7] Map available at: https://www.upturn.org/reports/2020/mass-extraction/.

to be somehow "weighed" against the claims of police efficiency.'") (citation omitted). This Court should not disregard a central constitutional protection based on such flimsy catastrophizing.

CONCLUSION

Because the disclosure of Mr. Garcia's passcodes is inherently testimonial and because the foregone-conclusion rationale does not and should not allow the government to compel disclosure of the contents of a defendant's mind, this Court should uphold the Fifth District in reversing the Circuit Court's order.

June 24, 2021

Respectfully submitted,

/s/ *Daniel B. Tilley*
Daniel B. Tilley
Florida Bar No. 102882
American Civil Liberties Union
of Florida, Inc.
4343 West Flagler St., Suite 400
Miami, FL 33134
(786) 363-2714
dtilley@aclufl.org

Counsel for Amici Curiae

/s/ *Jo Ann Palchak*
Jo Ann Palchak
Florida Bar No. 22826
Vice-Chair, Amicus Committee
National Association of Criminal
Defense Lawyers

The Law Office of Jo Ann Palchak, P.A.
1725 1/2 E. 7TH Avenue, Suite 6
Tampa, Florida 33605
(813) 468-4884
jpalchak@palchaklaw.com

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

Undersigned counsel hereby certifies that a true and correct copy of the foregoing has been furnished to all parties through the Florida Electronic Portal, this 24th day of June 2021.

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that this computer-generated amicus curiae brief was prepared in 14-point Arial font, in compliance with Florida Rules of Appellate Procedure 9.045 and 9.370, and contains fewer than 5,000 words.

/s/ *Daniel B. Tilley*
Daniel B. Tilley
Florida Bar No. 102882
American Civil Liberties Union
of Florida, Inc.
4343 West Flagler St., Suite 400
Miami, FL 33134
(786) 363-2714
dtilley@aclufl.org

Counsel for Amici Curiae