

**IN THE
INDIANA SUPREME COURT
CAUSE NO. 18S-CR-595**

KATELIN EUNJOO SEO,)
)
) Appeal from the Hamilton Superior
) Court No. 1
)
) Cause No. 29D01-1708-MC-5640
)
STATE OF INDIANA,) The Hon. Steven R. Nation, Judge
)
) Appellee.)

**BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER
FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND
AMERICAN CIVIL LIBERTIES UNION OF INDIANA
IN SUPPORT OF APPELLANT**

Kenneth J. Falk
No. 6777-49
ACLU OF INDIANA
1031 E. Washington St.
Indianapolis, IN 46202
317-635-4059
fax: 317/635-4105
kfalk@aclu-in.org

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....3

STATEMENT OF INTEREST6

SUMMARY OF ARGUMENT.....6

ARGUMENT.....9

I. Compelled Password Entry By the Target of a Criminal Investigation is Testimony Privileged By the Fifth Amendment.9

 A. The Fifth Amendment Prohibits the Compelled Disclosure or Use of the Contents of a Suspect’s Mind.9

 B. The Fifth Amendment Prohibits Compelled Recollection and Entry of a Memorized Password.10

II. *Fisher’s* Limited Foregone-Conclusion Exception Has No Application In This Case.12

 A. The Foregone-Conclusion Exception Applies Only to the Production of Specified, Preexisting Business Records.14

 B. Even If the Foregone-Conclusion Exception Could Apply in this Context, the Government Has Not Shown Both That the Phone Belongs to Appellant and Also What Incriminating Files Are Stored There.17

CONCLUSION23

CERTIFICATE OF WORD COUNT COMPLIANCE24

CERTIFICATE OF SERVICE.....24

TABLE OF AUTHORITIES

Cases

<i>Braswell v. United States</i> , 487 U.S. 99 (1988).....	15
<i>Burt Hill, Inc. v. Hassan</i> , No. CIV.A. 09-1285, 2010 WL 55715 (W.D. Pa. Jan. 4, 2010).....	16
<i>Carpenter v. United States</i> , 138 S. Ct. 2214 (2018).....	22
<i>Commonwealth v. Baust</i> , No. 14-cr-1439, 89 Va. Cir. 267, 2014 WL 10355635 (Va. Cir. Ct. Oct. 28, 2014).....	11
<i>Commonwealth v. Gelfgatt</i> , 11 N.E.3d 605 (Mass. 2014)	21
<i>Commonwealth v. Hughes</i> , 380 Mass. 583 (1980).....	16
<i>Curcio v. United States</i> , 354 U.S. 118 (1957).....	7, 9, 10
<i>Doe v. United States</i> , 487 U.S. 201 (1988).....	7, 10, 12
<i>Fisher v. United States</i> , 425 U.S. 391 (1976).....	<i>passim</i>
<i>G.A.Q.L. v. State</i> , 257 So. 3d 1058 (Fla. Dist. Ct. App. 2018)	<i>passim</i>
<i>Hoffman v. United States</i> , 341 U.S. 479 (1951).....	12
<i>In re Boucher</i> , No. 2:06-MJ-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).....	11, 20
<i>In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011</i> , 670 F.3d 1335 (11th Cir. 2012).....	<i>passim</i>
<i>In re Grand Jury Subpoenas Served Feb 27, 1984</i> , 599 F. Supp. 1006 (E.D. Wash. 1984).....	16

Matter of Residence in Oakland, Cal,
No. 4-19-70053, 2019 WL 176937 (N.D. Cal. Jan. 10, 2019) 20, 22

Pennsylvania v. Muniz,
496 U.S. 582 (1990).....9

Riley v. California,
134 S. Ct. 2470 (2014)22

SEC v. Huang,
No. 15-cv-269, 2015 WL 5611644 (E.D. Pa. Sept. 23, 2015)..... 11, 19, 21

Seo v. State,
109 N.E.3d 418 (Ind. Ct. App. 2018), *transfer granted and opinion vacated*, --
N.E.3d --, 2018 WL 6565988 (Ind. Dec. 6, 2018) 12, 18, 20, 22

Shapiro v. United States,
335 U.S. 1 (1948).....16

State v. Stahl,
206 So. 3d 124 (Fla. Dist. Ct. App. 2016)21

United States v. Apple MacPro Computer,
851 F.3d 238 (3d Cir. 2017)..... 19, 20

United States v. Bell,
217 F.R.D. 335 (M.D. Pa. 2003).....16

United States v. Bright,
596 F.3d 683 (9th Cir. 2010).....16

United States v. Doe,
465 U.S. 605 (1984)..... 13, 15, 22

United States v. Gippetti,
153 F. App'x 865 (3d Cir. 2005)16

United States v. Green,
272 F.3d 748 (5th Cir. 2001).....11

United States v. Hubbell,
530 U.S. 27 (2000)..... *passim*

United States v. Kirschner,
823 F. Supp. 2d 665 (E.D. Mich. 2010).....11

Brief of Amici Curiae EFF, ACLU and ACLU of Indiana

United States v. Sideman & Bancroft, LLP,
704 F.3d 1197 (9th Cir. 2013).....16

United States v. Spencer,
No. 17-CR-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018)21

Constitutional Provisions

U.S. Const. amend. V.....9

STATEMENT OF INTEREST

The Electronic Frontier Foundation (“EFF”) is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 39,000 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.

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. Since its founding in 1920, the ACLU has appeared before the Supreme Court and other federal courts in numerous cases implicating Americans’ right to privacy, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). The ACLU of Indiana is the Indiana affiliate of the ACLU.

SUMMARY OF ARGUMENT

This case presents a question of first impression in this Court: whether the right against self-incrimination in the Fifth Amendment to the U.S. Constitution prevents the State from forcing a defendant to decrypt the contents of her iPhone,

thus delivering them to the State for use against her in a criminal proceeding.

Centuries of precedent and practice support the conclusion that, in cases like this one, a suspect cannot be compelled to recall and use information that exists only in her mind in order to aid the State's prosecution of her. *See Curcio v. United States*, 354 U.S. 118, 128 (1957). This is no technicality; it is a fundamental protection of human dignity, agency, and integrity that the Framers enshrined in the Fifth Amendment to the U.S. Constitution.

The State can never require a defendant to remember, enter, use, or disclose the contents of her mind, such as a memorized password, to assist a prosecution against her. The “foregone-conclusion exception” cannot justify a different result in this case. *See United States v. Hubbell*, 530 U.S. 27, 44 (2000) (citing *Curcio*, 354 U.S. at 128); *Doe v. United States (Doe II)*, 487 U.S. 201, 208 n. 6 (1988). The U.S. Supreme Court has applied this exception just a single time and in a starkly different context—the mere act of producing subpoenaed business documents prepared by and in the possession of third parties. *See Fisher v. United States*, 425 U.S. 391 (1976).

Even if this Court chooses to expand the foregone-conclusion exception far beyond the unique circumstances in *Fisher*, it would still not justify the trial court's order here. Applying that doctrine here, the State would be required to show with reasonable particularity that the existence of relevant individual files on

the phone, Appellant’s control over them, and their authenticity are foregone conclusions. *See Hubbell*, 530 U.S. at 45. But the State has not established that it already knows the information it seeks to force Appellant to disclose here—specifically the existence or content of any particular files or documents on the decrypted iPhone. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012).

The State’s argument that the foregone-conclusion exception focuses on the passcode—rather than on what the State is truly after, the iPhone’s contents—would vitiate Fifth Amendment protection for digital devices. Numerous courts, including the Court of Appeals in the now-vacated-decision below, have rightly rejected the State’s view. Allowing the State to force a suspect to disclose or enter the password for decrypting the sensitive contents of a personal device on a mere showing that the individual knows the device’s password would render protections for the “privacies of life” hollow by effectively “expand[ing] the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment.” *G.A.Q.L. v. State*, 257 So. 3d 1058, 1063 (Fla. Dist. Ct. App. 2018). Pursuant to the State’s reasoning, “any password-protected [device] would be subject to compelled unlocking since it would be a foregone conclusion that any password-protected [device] would have a passcode.” *Id.* The Constitution

demands more before a suspect may be forced to expose her most private information for use in her own prosecution by the government.

This Court should reverse the trial court's contempt order.

ARGUMENT

I. **COMPELLED PASSWORD ENTRY BY THE TARGET OF A CRIMINAL INVESTIGATION IS TESTIMONY PRIVILEGED BY THE FIFTH AMENDMENT.**

A. **The Fifth Amendment Prohibits the Compelled Disclosure or Use 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.” U.S. Const. amend. V. To come within the self-incrimination privilege, an individual must show three things: that the evidence is (1) compelled, (2) testimonial, and (3) self-incriminating. *Hubbell*, 530 U.S. at 34. Only the second factor is at issue here.

Privileged testimony includes communications or any information, direct or indirect, verbal or non-verbal, that require a person to 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 *Pennsylvania v. Muniz*, 496 U.S. 582, 595 & n.9 (1990) (Fifth Amendment right spares an accused from “having to share his thoughts and beliefs with the Government”). The testimonial nature of a communication does not turn on whether it is spoken, but whether it requires, by “word or deed,” a truthful “expression of the contents of an individual’s mind.” See *Curcio*, 354 U.S. at 128

(Fifth Amendment prohibits compelling individual to testify orally as to the whereabouts of non-produced records because it requires him to disclose the contents of his own mind); *see also Doe II*, 487 U.S. at 219 & n.1 (1988) (Stevens, J., dissenting). Thus, physical acts can be testimonial and protected under the Fifth Amendment if performing them expresses or relies on the contents of a person’s mind. *Fisher*, 425 U.S. at 409 (government may not compel a witness to give oral testimony or to restate, repeat, or affirm the truth of the contents of documents sought); *Hubbell*, 530 U.S. at 43 (Fifth Amendment applies to production of documents where witness must “make extensive use of ‘the contents of his own mind’ to identify responsive materials.”).

B. The Fifth Amendment Prohibits Compelled Recollection and Entry of a Memorized Password.

The order issued by the trial court requires Appellant to type in her passcode and unlock her iPhone in violation of the Fifth Amendment. First, compelled entry of a password constitutes a modern form of written testimony, which is categorically protected. Second, even if the Court views this as a demand for action rather than for written testimony, it is protected because Appellant is incapable of performing the act without using the contents of her mind. *Curcio*, 354 U.S. at 128.

Reciting, writing, typing, entering, or otherwise reproducing a password from memory are all testimony protected by the Fifth Amendment. As the Eleventh Circuit has held, “the decryption . . . of the hard drives would require the use of the

contents of Doe’s mind and could not be fairly characterized as a physical act that would be nontestimonial in nature.” *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1346. Many other courts agree: production of computer passwords 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., In re Boucher*, No. 2:06-MJ-91, 2007 WL 4246473, at *1 (D. Vt. Nov. 29, 2007) (Magistrate Judge op.); *SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015); *G.A.Q.L. v. State*, 257 So.3d 1058, 1061-62 (Fla. Dist. Ct. App. Oct. 24, 2018); *Commonwealth v. Baust*, No. 14-cr-1439, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).

The State argues that compelling Appellant to produce her decrypted iPhone is not testimonial because the police will not learn the passcode. Pet. for Transfer

9. But opening locks with memorized passcodes is testimonial regardless of whether the suspect reveals the combination. *United States v. Green*, 272 F.3d 748, 753 (5th Cir. 2001). For example, there is “no serious question” that asking an arrestee to disclose the locations of and open the combination locks to cases containing firearms compels “testimonial and communicative” acts as to his “knowledge of the presence of firearms in these cases and of the means of opening these cases.” *Id.* at 753. The majority below was correct to “reject the State’s attempt to distinguish between compelling [Appellant] to convey her passcode . . .

and compelling [her] to . . . unlock her phone”; “[i]t is a distinction without a difference.” *Seo v. State*, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018), *transfer granted and opinion vacated*, --N.E.3d.--, 2018 WL 6565988 (Ind. Dec. 6, 2018). Additionally, decryption is akin to converting, translating, or “recreat[ing]the existing, unreadable files into new, legible ones. *Id.* (“In a very real sense, the files do not exist on the phone in any meaningful way until the passcode is entered and the files sought are decrypted.”).

Because compelled entry of Appellant’s passcode is testimonial and self-incriminating,¹ it is privileged by the Fifth Amendment. The analysis should end here.

II. FISHER’S LIMITED FOREGONE-CONCLUSION EXCEPTION HAS NO APPLICATION IN THIS CASE.

Even if the police know with reasonable certainty that a defendant committed a bank robbery, no one could credibly suggest that he could then be compelled to testify orally or in writing to that fact. “Whatever the scope of this ‘foregone conclusion’ rationale,” *Hubbell*, 530 U.S. at 44, it does not allow the government to compel a suspect to speak, write, type, or otherwise reproduce the contents of her mind to aid in its prosecution. Some courts have erroneously

¹ The compelled testimony need not *itself* be incriminating to fall within the privilege, so long as the testimony provides a “link in the chain of evidence” needed to prosecute. *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *Hubbell*, 530 U.S. at 38; *Doe II*, 487 U.S. at 208 n.6.

considered, however, whether the foregone-conclusion exception can nevertheless compel witnesses to enter their memorized passcodes into digital devices. This Court should decline to do so.

Even if this Court decides to expand a foregone-conclusion analysis to the compulsory entry of a memorized password, that exception does not apply here. The Supreme Court allowed a foregone-conclusion exception in a single unique case, *Fisher v. United States*, 425 U.S. 391 (1976), and has never again allowed the government to compel a testimonial act of production on those grounds. *See Hubbell*, 530 U.S. at 44; *United States v. Doe*, (“*Doe I*”), 465 U.S. 605, 612–14 (1984).

In over forty years since *Fisher*, lower courts, with few exceptions, have applied the foregone-conclusion exception only in the context of the production of specific, tangible business and financial records. The few courts that have found an order to recall or use a memorized password to be a foregone conclusion have erroneously stretched this rationale far beyond its limits.

Even if the foregone-conclusion exception could apply in cases involving passcodes, the State would have to show with reasonable particularity that it has independent knowledge of any and all information disclosed by the compelled act of production—including that the phone belongs to the witness and also that the

specific, identifiable files it seeks are stored on that device. The State has not shown that here.

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

The Supreme Court has long recognized that producing records in response to a subpoena or court order can have testimonial aspects protected by the Fifth Amendment—including implicit admissions concerning the existence, possession, and authenticity of the documents produced. *See Fisher*, 425 U.S. at 410. In *Fisher*, the government had independent knowledge of the existence and authenticity of documents created by accountants preparing the defendants’ tax records and in possession of the defendants’ attorneys. *Id.* at 412–13. Under these unique circumstances, the Court concluded that the Fifth Amendment did not immunize that act of producing these business documents. *Id.* at 411. The Court called out the “[s]pecial problems of privacy” that might arise in the case of a subpoena seeking production of more sensitive documents, like a personal diary, noting that such problems were not an obstacle to compelled production under *Fisher*’s facts. *Id.* at 394-95 nn.2–3, 401 n.7 (citing *United States v. Bennett*, 409 F.2d 888, 897 (2d Cir. 1969)).

Thus, *Fisher* stands for the proposition that if (1) the target of an investigation is asked only for an act of production and not to otherwise disclose or rely on the contents of her mind, (2) the target neither created nor possesses the

documents sought, *and* (3) the documents are not private in the way that a personal diary is, then the state may be able to compel the target’s disclosure of those papers.

Unsurprisingly, given these constraints, in the nearly 43 years since *Fisher* was decided, the Supreme Court has never again held that an act of disclosure 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 cases—both of which involved the government seeking to compel the production of preexisting business or other financial records. In each case, it refused to apply the exception. *Hubbell*, 530 U.S. at 44–45 (holding that the case “plainly [fell] outside of” the foregone conclusion exception where the government sought “general business or tax records that [fell] within the broad categories described in this subpoena” rather than specific, known files); *Doe I*, 465 U.S. at 612–14 (rejecting application of the foregone conclusion exception where the subpoena sought several broad categories of general business records).

That the Court has never considered the foregone-conclusion exception outside of cases involving specific, preexisting business and financial records is unsurprising. These records are a unique category of material that, to varying degrees, has 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). Lower courts, too, have overwhelmingly applied the exception 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. Bright*, 596 F.3d 683, 689 (9th Cir. 2010) (credit-card records); *United States v. Gippetti*, 153 F. App'x 865, 869 (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); *In re Grand Jury Subpoenas Served Feb 27, 1984*, 599 F. Supp. 1006, 1012 (E.D. Wash. 1984) (business-partnership records); *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).²

Here, the State did not seek an order compelling the production of specific, tangible business or financial records, but rather an order compelling Appellant to use her memorized passcode to aid law enforcement in a wide-ranging search of her most private photos, communications, notes, and associations. Application of a

² Courts routinely decline to apply the foregone-conclusion exception to cases involving the compelled production of physical evidence, such as guns or drugs, because the act of production in such cases would constitute an implicit admission of guilty knowledge. *See, e.g., Commonwealth v. Hughes*, 380 Mass. 583, 592 (1980); *State v. Dennis*, 16 Wash. App. 417, 423 (1976).

foregone-conclusion exception beyond its typical narrow confines risks a broad erosion of the privilege against self-incrimination.

B. Even If the Foregone-Conclusion Exception Could Apply in this Context, the Government Has Not Shown Both That the Phone Belongs to Appellant and Also What Incriminating Files Are Stored There.

Even assuming the foregone-conclusion exception could ever be applied to an order compelling a defendant to decrypt a digital device, the State must demonstrate knowledge of the existence, location, ownership, and authenticity of the device and also identify with reasonable particularity what files it will find stored there. *In re Grand Jury Subpoena*, 670 F.3d at 1346. It has not done so here.

The foregone-conclusion exception only applies where the State can show with “reasonable particularity” that it “already [knows] of the materials, thereby making any testimonial aspect a ‘foregone conclusion’.” *See id.* at 1345 (*citing Hubbell*, 530 U.S. at 38 & n.19). By contrast, where an act of production implies a statement of fact 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 State erroneously characterizes the opinion below as “idiosyncratic.” Pet. for Transfer 9. The Court of Appeals, however, followed the *majority of courts*

that have considered application of the foregone-conclusion exception in holding that investigators must know and be able to describe with reasonable particularity the discrete, tangible contents of a device—not merely that the device belongs to the defendant. *See*, 109 N.E.3d at 433–34. For example, 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 exception 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. The Eleventh Circuit emphasized that because disk encryption generates “random characters if there are files *and* if there is empty space, we simply do not know what, if anything, was hidden based on the facts before us.”³ *Id.* at 1347 (emphasis in original). Thus, the

³ The Eleventh Circuit rejected the government’s assertion that use of encryption alone demonstrated that the suspect “was trying to hide something.” *In re Grand Jury Subpoena*, 670 F.3d at 1347. Rather, “[j]ust as a vault is capable of storing

government did not know “the existence or the whereabouts” of the records it sought. *Id.*; see also *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (finding the foregone-conclusion exception satisfied where the government had evidence *both* that contraband files existed on the devices and that the defendant could access them).

A number of lower courts 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 Florida Court of Appeals 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. 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.” *Id.* at 1063–64. “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.” *Id.* (quoting *Hubbell*, 530 U.S. at 44); see also *Huang*, 2015 WL 5611644, at *3 (SEC

mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all.” *Id.* Indeed, encryption is designed to protect the owner from thieves, fraud, hackers, and abusive spouses. Far from creating a “zone of lawlessness,” encryption *prevents* crime.

Brief of Amici Curiae EFF, ACLU and ACLU of Indiana

could not establish with “reasonable particularity” that any documents sought resided in the locked phones); *Boucher*, 2009 WL 424718, at *2 (subpoena for unencrypted hard drive enforceable where defendant admitted illegal downloads and agents observed thousands of file names reflecting apparent child pornography); *Apple MacPro Computer*, 851 F.3d 238 at 248 (“Unlike *In re Grand Jury Subpoena*, the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that Doe can access them.”); *Matter of Residence in Oakland, Cal.*, No. 4-19-70053, 2019 WL 176937, at *4 (N.D. Cal. Jan. 10, 2019) (government lacks requisite prior knowledge of files on digital devices it anticipates seizing because “smartphones contain large amounts of data, including GPS location data and sensitive records, the full contents of which cannot be anticipated by law enforcement”).

Here, the State does not know whether or not the information it seeks exists. The State hypothesizes that, since the investigator’s “forensic download” of Appellant’s phone data, she might have used her phone to send additional threatening messages to the victim. It also guesses that Appellant may have installed some kind of application to spoof her phone number. Neither of these guesses are supported by evidence nor are the files and applications identified with reasonable particularity. *See*, 109 N.E.3d at 434-35. Encryption is not an obstacle to this investigation. The State could use harassing text messages on the victim’s

device as evidence. It could obtain a list of installed applications from Apple. *Id.* at 434 n. 21. This factual record does not justify the foregone-conclusion exception.

A few courts in recent years have misconstrued the standard necessary for application of the foregone-conclusion exception in the context of compelled decryption orders. These courts have accepted the argument made by the State here that the foregone-conclusion exception is satisfied where investigators can show knowledge of the existence, location, and authenticity of a device and that the suspect has the ability to decrypt it—rather than the evidence the State actually seeks. *See, e.g., State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016) (“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”); *United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 622 (Mass. 2014) (Lenk, J., dissenting) (majority compelled defendant to enter encryption key even though “the government has not shown that it has any knowledge as to the existence or content of any particular files or documents on any particular computer”).

But focusing only on the passcode misses the point. The State is seeking both the passcode *and* the underlying data. As a result, the State must know what “if anything, [is] hidden behind the encrypted wall.” *See Huang*, 2015 WL

5611644, *3; *see also Doe I*, 465 U.S. at 614 n. 12. Otherwise, a witness' Fifth Amendment rights could be overcome merely by "categorical requests for documents the Government anticipates are likely to exist." *Huang*, 2015 WL 5611644, at *3. This "simply will not suffice." *Id.* (citing *In re Grand Jury*, 670 F.3d at 1348). Every password-protected device "would be subject to compelled unlocking since it would be a foregone conclusion that any password-protected [device] would have a passcode." *G.A.Q.L.*, 257 So. 3d at 1063. The State could, as investigators unsuccessfully sought to do in *Matter of Residence in Oakland, California*, overcome a roomful of individuals' Fifth Amendment rights without any basis. 2019 WL 176937, at *4. Given that electronic devices today contain "a digital record of nearly every aspect of [users'] lives[.]" *Riley v. California*, 134 S. Ct. 2470, 2490 (2014), the Court of Appeals below correctly identified that "when the State seeks to compel a person to unlock a smartphone so that it may search the phone without limitations, the privacy implications are enormous[.]" *Seo*, 109 N.E.3d at 420.

The State's position in this case would impermissibly leave individuals "at the mercy of advancing technology." *Carpenter v. United States*, 138 S. Ct. 2214 (2018) (citation omitted). The Constitution, however, demands more. The State cannot compel Appellant to recall and enter her password, and even assuming the general application of the foregone-conclusion exception, it cannot compel her to

Brief of Amici Curiae EFF, ACLU and ACLU of Indiana

produce the decrypted contents of her iPhone without first demonstrating with reasonable particularity that every testimonial element of this act is already known to the State. It has not done so here.

CONCLUSION

This Court should reverse the trial court's contempt order.

/s/ Kenneth J. Falk

Kenneth J. Falk

No. 6777-49

ACLU of Indiana

1031 E. Washington St.

Indianapolis, IN 46202

317-635-4059

Fax: 317-635-4105

kfalk@aclu-in.org

Counsel for Amici Curiae

CERTIFICATE OF WORD COUNT COMPLIANCE

I verify that this brief contains no more than 4,200 words.

/s/ Kenneth J. Falk

Kenneth J. Falk
Attorney at Law

CERTIFICATE OF SERVICE

I certify that on January 31, 2019, I electronically filed the foregoing document using the Indiana E-filing System (IEFS).

I also certify that on January 31, 2019, the foregoing document was served upon the following persons via IEFS.

William J. Webster
Carla V. Garino
Webster & Garino
104 N. Union Street
Westfield, IN 46074

Ellen H. Meilaender
Stephen R. Creason
Office of the Attorney General
IGCS-5th Floor
302 W. Washington St.
Indianapolis, IN 46204

/s/ Kenneth J. Falk

Kenneth J. Falk
Attorney at Law