IN THE UTAH SUPREME COURT

STATE OF UTAH, *Plaintiff-Petitioner*, v. ALFONSO MARGO VALDEZ, *Defendant-Respondent.*	Case No. 20210175-SC On Writ of Certiorari to the Utah Court of Appeals Mr. Valdez is incarcerated.

BRIEF AMICI CURIAE OF THE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF UTAH, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF RESPONDENT

Emily Adams (14937)
Freyja Johnson (13762)
THE APPELLATE GROUP
P.O. Box 1564
Bountiful, UT 84011
(801) 924-0854
eadams@theappellategroup.com
fjohnson@theappelategroup.com

Attorneys for Respondent

John J. Nielsen (11736)
ASSISTANT SOLICITOR GENERAL
Sean D. Reyes (7969)
UTAH ATTORNEY GENERAL
160 East Broadway, Floor 6
P.O. Box 140854
Salt Lake City, UT 84111
(801) 466-0180

Attorneys for Petitioner

John M. Mejia (13965)
AMERICAN CIVIL LIBERTIES UNION OF UTAH FOUNDATION, INC.
355 North 300 West
Salt Lake City, UT 84103
(801) 521-9826
jmejia@acluutah.org

Jennifer S. Granick*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Andrew Crocker*
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St. San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Attorneys for Amici Curiae

* *Pro Hac Vice motion forthcoming*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Constitutional Provisions

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 Utah is the local affiliate of the ACLU and has a long-standing interest in protecting Utahns' rights to privacy. The ACLU has frequently appeared before the U.S. 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*, 141 S. Ct. 2623 (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. *See Eunjoo Seo*, 148 N.E.3d at 958 (amicus); *Andrews*, 234 A.3d at 1254 (amicus), *cert. denied*, 141 S. Ct. 2623 (co-counsel); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (amicus).

ARGUMENT SUMMARY

This case presents a question of first impression in this Court: whether the privilege against self-incrimination found in the Fifth Amendment to the United States Constitution precludes the State from using a criminal defendant's refusal to provide the passcode to his encrypted cell phone against him in a criminal proceeding. It does. 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 the Fifth Amendment's protections. In accordance with these principles, the Court of Appeals held that communicating a memorized passcode is testimonial, and thus the State's use at trial of Mr. Valdez's refusal to do so violated his privilege against self-incrimination. *State v. Valdez*, 2021 UT App 13, ¶ 47, 482 P.3d 861.

This Court should affirm the Court of Appeals' decision, which is consistent with the reasoning of numerous other state and federal courts, for several reasons.

First, 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.* ¶ 33. 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 and financial records." *Id.* ¶ 40 (citation omitted). Third, despite the government's dire-sounding warnings, there are alternative methods for law enforcement to access encrypted phones.

Despite the modern technological context, this case turns on one of the most fundamental protections in our constitutional system: an accused person's ability to exercise his Fifth Amendment rights without having his silence used against him. The Court of Appeals' decision below rightly rejected the State's circumvention of this protection. This Court should uphold that decision and extend that protection to all Utahns.

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." U.S. Const. amend. V. 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, 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").

B. Compelled Disclosure of the Passcode Is Testimonial.

The trial court's failure to exclude from evidence Mr. Valdez's refusal to provide his passcode violates the Fifth Amendment because it punishes Mr. Valdez for exercising his constitutional rights. Compelled disclosure of a password is a modern but straightforward form of testimony, which is categorically protected from compulsion under the privilege against self-incrimination.

As the court below held, the compelled disclosure of a password is indeed testimonial. *See Valdez*, 2021 UT App 13, ¶ 35, 482 P.3d 861. The appellate court recognized that the government's request would have required him to reveal to the government the "contents of his own mind." *Id*. (quoting *Doe II*, 487 U.S. at 219 n.1

(Stevens, J., dissenting)). Therefore, the prosecution may not use Mr. Valdez's silence against him. *See State v. Gallup*, 2011 UT App 422, ¶ 16, 267 P.3d 289 (admission into evidence of testimony that defendant refused to talk with police officer by hanging up phone violated defendant's Fifth Amendment right to remain silent).

Years ago, the Eleventh Circuit Court of Appeals held that "the decryption . . . of [ ] 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. Most federal courts that have addressed the issue 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); *see also Doe II*, 487 U.S. at 213 (verbal statements almost always "convey information or assert facts" and are nearly always "testimonial").

To be testimonial and trigger Fifth Amendment protection, an answer need

not require great mental effort, and the government need not be interested in the import of the testimony for its own sake. For example, in *Pennsylvania v. Muniz*, the U.S. 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 Muniz's response as evidence of mental impairment. *Id*. at 599 & n.13. Therefore, the question still demanded a testimonial answer.

Moreover, as the Court of Appeals explained, "law enforcement officers [sought] a response that is testimonial . . . because such a request asks for the code itself." *Valdez*, 2021 UT App 13, ¶ 33, 482 P.3d 861. And so long as 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. Valdez's passcode is both testimonial and self-incriminating, it is privileged under the Fifth Amendment. Thus, the State may not constitutionally assert that Mr. Valdez's invocation of his Fifth Amendment privilege constituted evidence of his guilt. *See Gallup*, 2011 UT App 422, ¶ 16, 267 P.3d 289. As the court below held, the analysis for such core

testimonial communications ends here. *See Valdez*, 2021 UT App 13, ¶ 35, 482 P.3d 861.

C. Compelled Entry of a Passcode Is Also Testimonial Because It Requires Individuals to Truthfully Use the Contents of Their Minds.

The Court of Appeals incorrectly suggested that an officer's demand that a suspect unlock a phone—whether through biometric means or by entering a passcode or swipe pattern—would not call for a fully testimonial response in the same way a demand to divulge the passcode does. *Id.* ¶ 31. Although this Court need not reach the issue to affirm the decision below, it should not endorse or otherwise suggest that this dictum is correct. Opening a lock with a memorized passcode is testimonial regardless of whether the State actually learns the combination.

As we know from *Muniz*, 496 U.S. 582, "testimony" need not take great mental effort, and the government need not be interested in the import of the testimony for its own sake. Moreover, testimony need not be verbal. Non-verbal acts such as nodding in response to a question are testimonial because they communicate the contents of the mind without speaking.[1] *See Schmerber v. California*, 384 U.S. 757, 761 n.5 (1966) ("A nod or head-shake is as much a 'testimonial' or 'communicative' act . . . as are spoken words."). The Eleventh Circuit applied this

[1] This is in contrast to mere physical acts that do not reveal the contents of an individual's mind, such as putting on a shirt. *Holt v. United States*, 218 U.S. 245 (1911).

principle in holding that "the *act* of [the accused's] decryption and production of the contents of [ ] hard drives . . . would be testimonial." *In re Grand Jury Subpoena*, 670 F.3d at 1346 (emphasis added). In sum, "the protection of the [Fifth Amendment] privilege reaches an accused's communications, whatever form they might take." *Schmerber*, 384 U.S. at 763–64.

This Court need not reach the question of whether physically decrypting a device with biometrics, or through swiping, typing, or other passcode entry, is testimonial, as that scenario is not raised by the facts of this case. *Valdez*, 2021 UT App 13, ¶ 34, 482 P.3d 861. But if the Court credits the State's assertion that the officer demanded that Mr. Valdez enter his passcode, this Court should hold that the Court of Appeals' reasoning applies with equal force to such a demand. *See, e.g.*, Pet. Br. at 25–26 (discussing entry of a passcode)."

II. THE COURT OF APPEALS 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 that fact was a "foregone conclusion." That is because the Fifth Amendment does not allow the government to compel suspects to speak, write, type, or otherwise communicate the contents of their minds to aid in their own prosecution. Notably, in *Muniz*, the U.S. Supreme 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 court below, have rightly concluded that permitting the narrow foregone-conclusion inquiry to bypass the Fifth Amendment's bedrock privilege is inconsistent "with governing, binding case law." *Valdez*, 2021 UT App 13, ¶ 42, 482 P.3d 861.

> [The Supreme] Court . . . has not mentioned the foregone conclusion exception in over two decades, when the Court referred to it simply as 'this "foregone conclusion" rationale,' and noted that "whatever [its] scope . . . , the facts of this case plainly fall outside of it." *See Hubbell*, 530 U.S. at 44 [ ]. The Court has never applied the exception outside of the context of assessing the testimoniality of a nonverbal act of producing documents. *See id*.; *see also Fisher* [*v. United States*], 425 U.S. [391,] 411–12 [(1976)]. Yet the Court's instruction regarding the testimoniality of verbal statements, as well as the strongbox key/safe combination illustration, appear to be as robust as ever. (citation omitted).

Id.; *see also Commonwealth v. Jones*, 117 N.E.3d 702, 724 (Mass. 2019) (Lenk, J., concurring); *Eunjoo Seo*, 148 N.E.3d at 961; *Davis*, 220 A.3d at 549; *Pollard v. State*, 287 So. 3d 649, 657 (Fla. Ct. App.) (expressing skepticism about the application of the foregone-conclusion exception and noting that their analysis proceeded "[o]n the assumption that the foregone conclusion exception applies to core testimonial communications"). This Court should likewise reject application of the foregone-conclusion analysis here.

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*, the government sought to compel the production of documents that were created by accountants preparing the defendants' tax records and that were in possession of the defendants' attorneys. 425 U.S. at 412–13. 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 that case, the Court further held that the act of producing the subpoenaed documents was not testimonial since the government had independent knowledge of the documents' existence and authenticity. *Id.* at 412–13. 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, then the State 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 invoked the foregone-conclusion rationale to hold that an act of production is unprotected by the Fifth Amendment. Indeed, the Court has only even considered foregone-conclusion arguments in two other cases, both of which involved the government's attempts to compel the production of preexisting business or other financial records, and it rejected those arguments 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, and demonstrates 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 producing the subpoenaed documents would have established their existence, authenticity, and custody, information the government was already able to prove or did not need. *Id.* In other words, these

matters were known to the government. Nevertheless, the Court held that the Fifth Amendment privilege excused compliance with the subpoena because complying would have required "mental and physical steps" and would have obliged the respondent to "truthful[ly] reply to the subpoena." *Id*. at 42. In stating that "whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it," the Court was not suggesting the facts implied by the act of production were as yet unknown to the prosecution. *Id.* at 44. Rather, in *Hubbell*, the foregone-conclusion rationale did not apply because compliance would have required mental effort beyond a mere act of production. The same is true here (and in all forced decryption cases requiring the disclosure or use of a password).

Given the narrow application of a foregone-conclusion rationale, it is unsurprising that the United States Supreme Court has never applied that rationale outside of cases involving specific, preexisting business and financial records. These types of records constitute 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).

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 used Mr. Valdez's silence about his memorized passcode against him at trial. This runs against *Fisher*'s teaching that a request for oral testimony violates the Fifth Amendment and is no mere act of production. *See Fisher*, 425 U.S. at 409.

Some courts have incorrectly viewed compulsion for a memorized passcode as implicating an act of production, rather than pure testimony. *See, e.g.*, *G.A.Q.L. v. State*, 257 So. 3d 1058, 1064 (Fla. Ct. App. 2018) (nevertheless finding the testimonial aspects of the production privileged); *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Ct. App. 2016); *Andrews*, 234 A.3d at 1273. These courts' reasoning is not compelling. As the Court of Appeals explained, "'prohibition of application of the foregone conclusion rationale to areas of compulsion of one's mental processes' as opposed to acts of production 'would be entirely consistent with the Supreme Court decisions . . . which uniformly protect information arrived at as a result of using one's mind.'" *Valdez*, 2021 UT App 13, ¶ 42, 482 P.3d 861 (quoting *Davis*, 220

A.3d at 547–49). Ultimately, 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.

The Indiana Supreme Court has outlined three additional important reasons to reject application of the foregone-conclusion rationale to demands to decrypt electronic information. *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 admonition from the Supreme Court to tread cautiously when "confronting new concerns wrought by digital technology." *Id.* (quoting *Carpenter*, 138 S. Ct. at 2222). As the appellate court in this case noted, the Supreme

Court, "has been careful not to uncritically extend existing precedents . . . ." *Valdez*, 482 P.3d at 875 (citing *Carpenter*, 138 S. Ct. at 2222 & *Riley v. California*, 573 U.S. 373, 401–02 (2014)). This Court should uphold the Court of Appeals and follow its counterparts in Indiana and Pennsylvania by 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 more than that an individual had possession and control over a passcode. Rather, 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. 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 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. *See Huang*, 2015 WL 5611644, at *3 (foregone-conclusion analysis did not apply because the government could not show with "reasonable particularity" that any of requested documents actually existed on the

encrypted smartphones); *see also Doe I*, 465 U.S. at 613 n.12 (foregone-conclusion analysis inappropriate where the government failed to independently establish the documents were in target's possession or subject to his control). *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, the State cannot compel an individual to produce the decrypted contents of a 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 State claims that restricting its ability to compel defendants to produce passcodes will seriously interfere with its ability to conduct investiations. *See* Pet'r Br. at 2 ("[T]he digital locks on these devices are often unbreakable. This means that the suspect must help open them if they are to be opened."). Yet the technology exists for law enforcement to access information on electronic devices without

compelling the production of a passcode. One option is to use mobile device forensic tools that are capable of breaking into devices, even those with passwords. *See* Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 27 (2020).[2] One vendor, Cellebrite, sells tools that can extract and interpret data from at least 181 apps on Android's operating system.[3] *Id.* at 16. Moreover, a large percentage of cellphone searches are based on the consent of the owner. *Id.* at 46–47. Given the widespread availability of forensic tools, and the relative ease that officers appear to have in obtaining consent from suspects, respecting the Fifth Amendment privilege is unlikely to pose a catastrophic obstacle in the vast majority of investigations. *See also Riley*, 573 U.S. at 401 (Constitutional rights are "not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'") (citation omitted).

CONCLUSION

Because the officer's demand for Mr. Valdez's passcode in this case calls for an inherently testimonial response, and because the foregone-conclusion rationale does not and should not allow the government to compel a verbal statement or any

[2] Available at https://www.upturn.org/reports/2020/mass-extraction/.

[3] The State protests that these forensic tools are often expensive. *See* Pet'r Br. at 30 n.2. Research shows that many smaller law enforcement agencies can afford them. *See* Koepke et al., *Mass Extraction* 36–37. In any case, application of the Fifth Amendment privilege does not involve a balancing test, and courts do not weigh the monetary cost of alternative approaches when analysing the accused's claim that the government seeks to violate his right to act as a witness against himself.

disclosure of the contents of a defendant's mind, this Court should adopt the Court of Appeals' reasoning.

RESPECTFULLY SUBMITTED this 19th day of October, 2021.

/s/ John M. Mejia

John M. Mejia (13965)
AMERICAN CIVIL LIBERTIES
UNION OF UTAH FOUNDATION, INC.
355 North 300 West
Salt Lake City, UT 84103
(801) 521-9826
jmejia@acluutah.org

Jennifer S. Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Andrew Crocker*
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St. San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Attorneys for Amici Curiae

* *Pro Hac Vice motion forthcoming*

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that:

1. This brief complies with the word limits set forth in Utah R. App. P. 24(g)(1) because this brief contains 4,515 words, excluding those parts of the brief exempted under Utah R. App. P. 24(g)(2).

2. This brief complies with Utah R. App. P. 21(g) regarding public and non-public filings.

DATED this 19th day of October, 2021.

/s/ John M. Mejia
John M. Mejia (13965)

CERTIFICATE OF SERVICE

Undersigned counsel hereby certifies that on the 19th day of October, 2021, two copies of the foregoing **BRIEF AMICI CURIAE OF THE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF UTAH, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF RESPONDENT** were served via U.S. Mail, postage prepaid, on the following:

Emily Adams (14937)
Freyja Johnson (13762)
THE APPELLATE GROUP
P.O. Box 1564
Bountiful, UT 84011
(801) 924-0854
eadams@theappellategroup.com
fjohnson@theappelategroup.com
Attorneys for Respondent

John J. Nielsen (11736)
ASSISTANT SOLICITOR GENERAL
Sean D. Reyes (7969)
UTAH ATTORNEY GENERAL
160 East Broadway, Floor 6
P.O. Box 140854
Salt Lake City, UT 84111
(801) 466-0180
Attorneys for Petitioner

/s/ John M. Mejia
John M. Mejia