No. 00-0000

IN THE SUPREME COURT OF THE UNITED STATES

PENNSYLVANIA

Petitioner

v.

JOSEPH J. DAVIS

Respondent

ON PETITION FOR WRIT OF *CERTIORARI* TO THE SUPREME COURT OF PENNSYLVANIA

PETITION FOR WRIT OF *CERTIORARI*

JOSH SHAPIRO
Attorney General
Commonwealth of Pennsylvania

JENNIFER C. SELBER
Executive Deputy Attorney General
Director, Criminal Law Division

JAMES P. BARKER
Chief Deputy Attorney General
Appeals & Legal Services Section

WILLIAM R. STOYCOS *
Senior Deputy Attorney General
Counsel of Record

Office of Attorney General
16th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 787-6348

QUESTIONS PRESENTED

For more than forty years, courts have allowed law enforcement authorities to compel an individual to disclose information when the information adds little or nothing to the sum total of information already possessed by the government and is a foregone conclusion. During that same time, advances in technology have changed the ways information may be stored to include electronic media as opposed to paper documents, which were the exclusive manner of keeping business records in former days. Concurrent with the development of electronic media has been the creation of the means of making information inaccessible through virtually unbreakable encryption technology. Both developments have given rise to criminal activity that takes advantage of new technology and an urgent need for law enforcement to access data and information kept beyond its lawful reach by the encryption technology. This Court has not considered the foregone conclusion doctrine in the context of electronic media and encryption.

1. Does the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination established in *Fisher v. United States*, 425 U.S. 391 (1976) and its progeny apply to the compelled production of passwords to encrypted electronic devices when the government has seized a device pursuant to a valid search warrant and has independent knowledge that the password exists, is known by

the suspect, and will decrypt the device, such that the compelled information itself lacks testimonial significance and any testimony implied by the compelled act is already known by the government, not in issue, and adds little or nothing to the sum total of the government's information?

2. Assuming the foregone conclusion exception applies, what is the government's burden of proof to support the exception, and more specifically, must the government demonstrate knowledge relating solely to the password sought or must it also demonstrate knowledge of the contents of the encrypted device for which a judge has already authorized a search?

PARTIES TO THE PROCEEDING

All parties appear in the caption of the case on the cover page.

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

Page(s)

Cases

Constitutional Provisions and Statutes

Rules

Other Authorities

OPINIONS BELOW

The opinion of the four-justice majority of the Supreme Court of Pennsylvania reversing the decision of the Superior Court of Pennsylvania and holding that the compelled production by Davis to the government of the digital password to his encrypted, lawfully-seized computer violated the Fifth Amendment to the Constitution of the United States is published at *Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019), and is reprinted at Pet. App. 1a. The opinion of the three-justice minority of the state Supreme Court dissenting from the majority's decision also is published at *Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019), and is reprinted at Pet. App. 1b. The unanimous opinion and order of the three-judge panel of the Superior Court of Pennsylvania holding that the foregone conclusion doctrine applies to render Davis' compelled act of production of the password to his encrypted, lawfully-seized computer non-testimonial and therefore not violative of the Fifth Amendment is published at *Commonwealth v. Davis*, 176 A.3d 869 (Pa. Super. 2017), and is reprinted at Pet. App. 1c. The opinion of the Court of Common Pleas of Luzerne County, Pennsylvania, holding that the foregone conclusion doctrine applies to render Davis' compelled act of production of the password to his encrypted, lawfully-seized computer non-testimonial and not violative of the Fifth Amendment is unpublished and is reprinted at Pet. App. 1d.

STATEMENT OF JURISDICTION

On November 20, 2019, a four-justice majority of the Supreme Court of Pennsylvania ruled that "until the United States Supreme Court holds otherwise," the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination established in *Fisher v. United States*, 425 U.S. 391 (1976) and its progeny does not apply in the context of compelled production of digital passwords to encrypted electronic devices seized pursuant to a judicially-authorized search warrant and such compelled acts of production violate the Fifth Amendment. The jurisdiction of this Court is invoked under 28 U.S.C. § 1257(a).

CONSTITUTIONAL PROVISION INVOLVED

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; *nor shall be compelled in any criminal case to be a witness against himself,* nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

U.S.C.A. Const. Amend. V (emphasis added).

STATEMENT OF THE CASE

In July 2014, agents from the Pennsylvania Office of Attorney General ("OAG") conducted an undercover investigation into the possession and distribution of child pornography via the internet. The investigation focused on individuals using an online, peer-to-peer electronic file-sharing network known as "eMule." More specifically, agents determined that a computer at a specific internet protocol ("IP") address was used to share child pornography. Agents used computers running specially-designed, investigative software to make a direct connection to the device at that IP address and downloaded an electronic file believed to be child pornography that was transferred from the device. Thereafter, Special Agent Justin Leri viewed the file and determined that it was a video depicting a prepubescent child engaging in unlawful sexual activity.

Agent Leri subsequently determined that the IP address was registered to Comcast Cable Company ("Comcast"). OAG agents then obtained and served upon Comcast a court order directing the disclosure to law enforcement of the subscriber information related to that particular IP address, with which Comcast complied. As a result, OAG agents determined that the subscriber for the IP address was the Respondent, Joseph Davis.

Agent Leri thereafter obtained a warrant from a local magistrate judge to search Davis' residence. Agents executed the warrant on September 9, 2014. The only occupant, Davis, acknowledged understanding and voluntarily waived his *Miranda* rights, admitted to being the sole user of the Dell computer system found in the

residence, and denied the existence of any child pornography on the computer. He also stated that he had previously been arrested for child pornography offenses and "did my time for that."

Agents seized the Dell computer and two DVDs. Agents from the OAG Computer Forensics Unit ("CFU") attempted without success to analyze the computer system in the residence. The computer had no readable data. The search was ended and no arrest was made. Agents subsequently learned from Davis that he wiped his computer clean with a DVD known as "DBAN" just days prior to the execution of the search warrant.

Fifteen months later, on October 4, 2015, OAG agents conducted another undercover investigation of persons using the eMule network to share child pornography. At that time, agents observed that a specific IP address was distributing electronic files of child pornography. A direct connection was made from OAG computers using investigative software to the IP address and agents downloaded one electronic file transferred to them that contained suspected child pornography. Special Agent Daniel Block viewed the file and determined that the file was a video of a prepubescent child engaging in prohibited sexual activity.

Agent Block subsequently determined that the IP address was registered to Comcast. He sent an administrative subpoena to Comcast directing the disclosure of the subscriber information related to that particular IP address, with which Comcast complied. As a result, OAG agents determined that the subscriber for the IP address was the same Joseph Davis.

OAG agents thereafter obtained a warrant from a court to search that residence, which the agents executed on October 20, 2015. Davis, the sole occupant of the residence, voluntarily waived his *Miranda* rights and agreed to speak with the agents. He informed the agents that: (1) he had lived alone in the apartment since 2006; (2) he had not had any long-term guests during his time at the residence; (3) he utilized Comcast internet and had done so on and off for many years; (4) he did not have Wi-Fi and only used hardwired internet services so that no one could steal his Wi-Fi; (5) he was the sole user of the desktop computer in the residence; and (6) the desktop computer was password-protected and only he knew the password allowing access to the computer (R. at 39a). Agent Block asked Davis to give him (Agent Block) the password and Davis refused to do so.

Davis also informed the agents that: (1) he watched pornography on the computer, which is legal; (2) he was previously arrested for child pornography; (3) child pornography is legal in other countries like Japan and the Czech Republic; (4) he did not understand why it is illegal here; and (5) what people do in the privacy of their own homes is their own business.

Agents located the desktop computer, an HP Envy 700 ("the computer"), in the home. CFU agents attempted to analyze it, but Special Agent Braden Cook determined that the computer was encrypted via software known as "TrueCrypt" that prevented OAG agents from accessing the contents of the computer. In order for the computer to "boot" into the Windows operating system, a user-created password must be input into the "TrueCrypt" volume. According to Agent Cook, "when the computer

power is [turned] on, it goes directly to a screen that says, 'TrueCrypt Boot Version 7.1' and it requires a password to be entered in order to have the computer function."[1]

Following his arrest, Davis told the agents his computer was encrypted with "TrueCrypt" and he claimed he could not remember the password. He also told Agent Block that "even if he could ... it would be like, quoting him exactly, putting a gun to his head and pulling the trigger." Thereafter, when Agent Block asked him if he remembered the password, Davis said "he would die in jail before ever remembering the password."

About an hour or two after the agents entered Davis' residence, following his arrest, agents transported him to court for an arraignment. During the transport, Davis voluntarily spoke with Agent Block. According to Agent Block:

---

[1] "Encryption technology allows a person to transform plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process. Only those who possess a corresponding 'key' can return the information into its original form, i.e. decrypt that information. Encrypted information remains on the device in which it is stored, but exists only in its transformed, unintelligible format. Although encryption may be used to hide illegal material, it also assists individuals and businesses in lawfully safeguarding the privacy and security of information. Many new devices include encryption tools as standard features, and many federal and state laws either require or encourage encryption to protect sensitive information." *United States v. Apple MacPro Computer,* 851 F.3d 238, 242 n. 1 (3rd Cir. 2017).

> While we were in transport to his arraignment, Mr. Davis was talking about gay x-rated movies he likes to watch and stated he liked 10, 11, 12, and 13 year olds, referring to them as "a perfectly ripe apple." He further stated he didn't see what the big deal was. He's not taking kids and raping them. There's nothing wrong with watching kids that age in the privacy of your own home ...
>
> ...Then I asked if he would give the password [to me]. He replied, "It's 64 characters and why would I give that to you? We both know what's on there [the computer]. It's only going to hurt me. No [expletive] way I'm going to give it to you." Then he made several jokes referring to the password but did not give us the password.

OAG agents observed that the IP address belonging to Davis was active on the peer-to-peer file sharing network eMule twenty-five times during the year 2015. The investigation determined that, on those occasions, the file-sharing had qualities that were indicative of child pornography.

On December 17, 2015, the Commonwealth of Pennsylvania ("the Commonwealth") filed a pretrial motion in the Luzerne County Court of Common Pleas ("the trial court") seeking an order compelling Davis to provide OAG agents with the password to the encryption software on his computer so that they could execute the search warrant. In support of the motion, the Commonwealth argued that Davis' act of producing

the password would not communicate any facts of testimonial significance beyond what he had already admitted to investigators, namely that a password existed that will decrypt Davis' computer, that he had possession and control of that password, and that the computer contained images of child pornography. The Commonwealth argued that the act of production falls under the foregone conclusion exception to the Fifth Amendment right against self-incrimination articulated in *Fisher v. United States*, 425 U.S. 391 (1976), and is constitutionally permissible. The Commonwealth requested "that Joseph Davis be ordered to assist the Commonwealth in the execution of the previously executed search warrant by providing his TrueCrypt password to his HP Envy computer or by inputting the password into the device."

Davis responded that such government compulsion would violate his right against self-incrimination under the Fifth Amendment.[2] Central to his argument was the assertion that, because the government could not state with any specificity what is contained in the computer files, the foregone conclusion exception established in *Fisher* is inapplicable.

While the motion was pending, the Commonwealth filed a Criminal Information charging Davis with two counts of sexual abuse of children (distribution of child

---

[2] Davis also contended that it would violate his right against self-incrimination under Article I, Section 9 of the state Constitution. However, he conceded that the Pennsylvania Supreme Court construes the state and federal constitutional provisions coextensively and follows this Court's lead on the proper analysis to be utilized.

pornography)[3] and two counts of criminal use of a communication facility.[4]

Following an evidentiary hearing, the trial court entered an order granting the Commonwealth's motion to compel. It specifically required that "Defendant supply the Commonwealth with any and all passwords used to access the HP Envy 700 desktop computer with serial # Z4Z1AAAEFM or [sic] within thirty (30) days from the date of this order." The trial court filed an opinion in support of its order which cited to *Fisher* as well as decisions of this Court and other courts applying *Fisher* and found that the foregone conclusion exception applies to the record facts. Notably, the court focused not only on the fact that the Commonwealth proved it had knowledge independent of the act of production that Davis has possession and control of the decryption password but also had independent knowledge regarding the existence and whereabouts of child pornography on the computer. For these reasons, the court held that Davis' act of production would lose its testimonial significance because the information is a "foregone conclusion."

Davis appealed that determination to the Superior Court of Pennsylvania. On November 30, 2017, a three-judge panel of that Court filed a unanimous, published Opinion affirming the trial court order compelling Davis to produce the password pursuant to the foregone conclusion exception. Davis subsequently

---

[3] 18 Pa.C.S.A. § 6312(c)

[4] 18 Pa.C.S.A. § 7512(a)

filed an application for reargument *en banc* that was denied.

On March 7, 2018, Davis filed a petition for allowance of appeal in the Supreme Court of Pennsylvania. On October 3, 2018, the Court granted that petition, articulating the issue as:

> May [Petitioner] be compelled to disclose orally the memorized password to a computer over his invocation of privilege under the Fifth amendment to the Constitution of the United States, and Article I, [S]ection 9 of the Pennsylvania Constitution?

Following briefing and oral argument, the state Supreme Court filed its decision on November 20, 2019. A four-justice majority reversed the Superior Court, holding that the foregone conclusion exception to the right against self-incrimination does not apply to the compelled disclosure of a computer password because the password is a mental construct stored in the suspect's mind rather than a physical object and the compelled production would require the suspect to use the contents of his own mind.

The majority relied in large part on this Court's prior decisions indicating that a compelled surrender of the key to a strongbox survives Fifth Amendment scrutiny but the compelled production of a lock combination does not. In the words of the majority:

> [C]onsistent with this historical repulsion of the prospect of compelling a defendant to reveal his or her mental impressions, we find it particularly revealing that, when addressing

> Justice Steven's dissent in *Doe II*, the majority of the Court noted that compelling the defendant to sign the bank disclosure forms was more akin to "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it was to "be[ing] compelled to reveal the combination to [petitioner's] wall safe." ...This is a critical distinction. Consistent with a physical/mental production dichotomy, in conveying the combination to a wall safe, versus surrendering a key to a strongbox, a person must use the "contents of [their] own mind." If one is protected from telling an inquisitor the combination to a wall safe, it is a short step to conclude that one is protected from telling an inquisitor the password to a computer.

220 A.3d at 547-548.

The majority held in the alternative that, even if the foregone conclusion exception is applicable under the circumstances presented, the Commonwealth failed to satisfy a prerequisite to that application because it failed to establish that it had knowledge of the contents of the files stored on Davis' computer hard drive, which it had already received judicial permission to search. In the words of the majority, "until the United States Supreme Court holds otherwise, we construe the foregone conclusion rationale to be one of limited application, and, consistent with its teachings in other decisions, believe the exception to be inapplicable to compel the disclosure of a defendant's

password to assist the Commonwealth in gaining access to a computer." *Id.* at 551.

A three-justice minority of the Court dissented, holding that the foregone conclusion analysis articulated in *Fisher* and its progeny logically applies to the compelled disclosure of a digital password to an electronic device seized pursuant to a warrant. According to the minority:

> My analysis focuses on the compulsion order, which directed Appellant to "supply the Commonwealth with any and all passwords used to access" a specific desktop computer and hard drive seized from his residence...." In my view, this order compels an act of production that has testimonial aspects in that it conveys, as a factual matter, that Appellant has access to the particular computer seized by the Commonwealth pursuant to a warrant, and that he has possession and control over the password that will decrypt the encrypted files stored on that computer. As discussed in detail *infra*, because the Commonwealth was already aware of these facts based upon its own investigation and Appellant's candid discussion with government agents, the password falls within the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination, and may be constitutionally compelled. Notably, critical to my position is the recognition that this case does not involve a Fourth Amendment challenge based upon Appellant's privacy rights in his encrypted computer files but,

> rather, solely a challenge to the compelled disclosure of his password based upon his Fifth Amendment privilege against self-incrimination.

Id. at 553.

With regard to the majority's concern that compelled disclosure of the password would compel that suspect to utilize his mental processes, the minority stated:

> There is an appeal to this conclusion, as requiring Appellant to supply his password involves some mental effort in recalling the 64 characters used to encrypt the computer files. However, one would expend similar mental effort when engaging in virtually any other act of production, such as the disclosure of business or financial records, as the individual must retrieve the contents of his mind to recall the documents' location before disclosing them to the government... The mere fact that Appellant is required to think in order to complete the act of production, in my view, does not immunize that act of production from the foregone conclusion rationale.

Id. at 555.

Regarding the physical/mental dichotomy noted by this Court in its pre-digital era Fifth Amendment decisions, the minority observed:

> I recognize that the majority's conclusion in this regard finds support in commentary found

> in federal cases, suggesting a constitutional distinction between the compelled surrender of a key and the compelled disclosure of a combination to a wall safe. For the reasons set forth herein, however, I do not find any such distinction dispositive in a case involving current day technology relating to the compelled disclosure of a password to encrypted digital information, where the Commonwealth has a warrant to search the digital container. Only the High Court can make the final determination in this regard for purposes of the Fifth Amendment, and the present case offers an attractive vehicle by which the Court could do so.

Id. at 555 n.3.

The minority also observed that adopting the majority's approach would produce a bizarre anomaly in which the type of encryption password chosen by a user would dictate whether production of that password could be constitutionally compelled. Although an alphanumerical password committed to memory would be off limits, the government could require the production of a biometric password such as facial recognition or a fingerprint because those types of gateways to a device do not require use of the contents of one's mind.[5] The minority warned that the

---

[5] *See, e.g., State v. Diamond*, 905 N.W.2d 870, 877 (Minn. 2018) (ordering defendant to provide his fingerprint to unlock his cell phone did not violate right against self-incrimination); *Matter of Search of [Redacted] Washington, District of Columbia*, 317 F.Supp.3d 523, 539 (D.D.C. 2018) (compelled use of biometric

majority's approach would "create an entire class of evidence, encrypted computer files, that is impervious to government search" and "potentially alter the balance of power between governmental authorities and criminals, and render law enforcement incapable of accessing relevant evidence." *Id.* at 557.

The minority also disagreed with the majority about the extent of the government's burden under the foregone conclusion exception, noting that requiring the Commonwealth to prove knowledge of the contents of the computer files is an untenable application of *Fisher* that conflates the meaning and purposes of the Fourth and Fifth Amendments to the Constitution:

> [T]he foregone conclusion exception as applied to the facts presented relates not to the computer files, but to the password itself. Appellant's computer files were not the subject of the compulsion order, which instead involved only the password that would act to

---

features to open digital device found during execution of search warrant did not violate privilege against self-incrimination); *Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F.Supp.3d 785 (D. Idaho 2019) (compelled placement of suspect's finger on cellphone to unlock phone did not violate right against self-incrimination); *Matter of Search Warrant Application for Cellular Telephone in United States v. Barrera*, 415 F.Supp.3d 832 (N.D. Ill. East. Div. 2019) (same); *contra Matter of Residence in Oakland, California*, 354 F.Supp.3d 1010 (N.D. Cal. 2019) (foregone conclusion exception does not apply to permit government to compel use of biometric features to unlock cellphone; biometric features are the equivalent of a digital password); *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (N.D. Ill. West. Div. 2017) (same); *United States v. Wright*, -- F.Supp.3d –, 2020 WL 60239 (D. Nevada Jan. 6, 2020) (same).

decrypt those files. This change of focus is subtle, but its effect is significant. While the government's knowledge of the specific files contained on Appellant's computer hard drive would be central to any claim asserted pursuant to the Fourth Amendment, the same is not dispositive of the instant claim based upon the Fifth Amendment right against self-incrimination, which focuses upon whether the evidence compelled, here, the password, requires the defendant to provide incriminating evidence. *See Doe v. United States* (*In re Grand Jury Subpoena*), 383 F.3d 905, 910 (9th Cir. 2004) (providing that "it is the government's knowledge of the existence and possession of the actual documents [subpoenaed by the government], not the information contained therein, that is central to the foregone conclusion inquiry"). This Court should not alleviate concerns over the potential overbreadth of a digital search in violation of Fourth Amendment privacy concerns by invoking the Fifth Amendment privilege against self-incrimination, which offers no privacy protection. The High Court in *Fisher* made this clear by stating, "We cannot cut the Fifth Amendment loose from the moorings of its language, and make it serve as a general protector of privacy – a word not mentioned in its text and a concept directly addressed in the *Fourth Amendment.*" 425 U.S. at 401 (quoting *United States v. Nobles*, 422 U.S. 225, 233 n. 7 (1975) (emphasis in original).

> Accordingly, I would align myself with those jurisdictions that examine the requisites of the foregone conclusion by focusing only on the compelled evidence itself, i.e., the computer password, and not the decrypted files that the password would ultimately reveal...

Id. at 556.

Succinctly stated, the majority of the state Supreme Court reached the conclusion that the Fifth Amendment bars a court from ordering disclosure of the password to an encrypted computer or other electronic device. The foregone conclusion doctrine does not apply because revealing the password would communicate implicitly the suspect's knowledge and possession of the password and ability to access the contents of the computer. The majority also held that being compelled to disclose the password was equivalent to providing the incriminating evidence contained in files on the computer. The dissent concluded that the government already had the information concerning the suspect's knowledge and control of the password and so the foregone conclusion exception applied. Also, discussion of the files contained within the computer are a matter for Fourth Amendment, not Fifth Amendment, analysis. Most courts considering the question to date have agreed with the dissent's position, but there is substantial division on the issue.

REASONS FOR GRANTING THE WRIT

The Court should grant the petition for writ of *certiorari* for the following reasons.

A. The Pennsylvania Supreme Court's decision addresses an important and pressing federal question in a manner that directly conflicts with the decisions of United States courts of appeals and decisions of other state courts of last resort.

This Court has previously noted that the sophisticated encryption technology that has recently emerged can render electronic devices "all but 'unbreakable' unless police know the password." *Riley v. California*, 573 U.S. 373, 389 (2014). Courts at all levels are now grappling with the dilemma created when an investigative search of a digital device has been approved by a court as reasonable under the Fourth Amendment but is being thwarted by encryption software that cannot be unlocked due to the suspect's refusal to provide the password on Fifth Amendment self-incrimination grounds.

The Supreme Court of Pennsylvania determined that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination articulated in *Fisher v. United States*, 425 U.S. 391 (1976), does not extend beyond subpoenaed documents to apply to the compelled production of a password to an encrypted electronic device that is subject to a valid search warrant. This holding directly conflicts with decisions of United States courts of appeals and with decisions of other state courts of last resort on the same question. *See, e.g., United States v. Apple MacPro Computer,* 851 F.3d 238, 247 (3rd Cir. 2017); *United*

States v. Bright, 596 F.3d 683, 692 (9th Cir. 2010); *United States v. Gavegnano*, 305 Fed.Appx. 954 (4th Cir. 2009); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 612 (Mass. 2014); *see also Commonwealth v. Jones*, 117 N.E.3d 702 (Mass. 2019) (holding that state constitutional privilege against self-incrimination tracks Fifth Amendment jurisprudence permitting compelled production of digital password where government can show it has independent knowledge that suspect knows the password); *Seo v. State*, 119 N.E.3d 90 (Ind. Dec. 6, 2018) (vacating lower court decision that foregone conclusion doctrine does not apply to compelled production of a digital password).

Only one United States court of appeals has ruled in a manner consistent with the Pennsylvania Supreme Court. *See In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012). No state court of last resort has, to date, come to the same conclusion as Pennsylvania's highest court.

The lower state and federal courts are also profoundly divided on the questions presented. Many have found that the foregone conclusion exception applies to render compelled production of a digital password or compelled decryption of digital data constitutional. *See, e.g., State v. Johnson*, 576 S.W.3d 205, 277 (Mo. Ct. App. W.D. 2019); *State v. Pittman*, 452 P.3d 1011 (Or. App. 2019), *rev. allowed*, 458 P.3d 1121 (Or. 2020); *State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. 2018); *State v. Stahl*, 206 So.3d 124, 131 (Fla. 2nd DCA 2016); *Commonwealth v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014); *United States v. Spencer*, 2018 WL 1964588 (N.D. Cal. April 26, 2018); *United States v. Fricosu*, 841 F.Supp.2d 1232, 1235 (D. Col.

2012); *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

Other courts have ruled to the contrary. *See, e.g., Pollard v. State*, 287 So.3d 649 (Fla. 1st DCA 2019); *People v. Spicer*, 125 N.E.3d 1286 (Ill. App. 3d 2019); *Sec. & Exch. Comm'n v. Huang*, 2015 WL 5611644 (E.D. Pa. Sept. 23, 2015); *United States v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mich. 2010).

Not only is there a lack of consensus and uniformity on the question of the applicability of the foregone conclusion exception in the context of digital passwords, but there is also widespread disagreement on the proper construction of the law established by *Fisher*, including: (1) the nature and quantity of independent knowledge the government must prove in order to trigger applicability of the exception;[6] (2) how past precedent addressing acts of production in the

---

[6] *Compare, e.g., MacPro Computer*, 851 F.3d at 248 n. 7 (noting that although the government could establish independent of the compelled production both the suspect's knowledge of the password and the existence of child pornography on the encrypted device, "a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production...[the suspect's] stating that 'I, John Doe, know the password for these devices'"), *Gelfgatt*, 11 N.E.3d 605 (government's burden is limited to showing independent knowledge of the password's existence, possession by suspect, and authenticity; its knowledge of the contents of the device itself is irrelevant to the analysis) with *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (government's ability to establish with reasonable particularity the presence of the files on the electronic device controls disposition of the question).

physical domain can be applied to productions of digital information;[7] and (3) the significance of the physical/mental distinction between biometric data and memorized passwords, both of which can unlock an encrypted device.[8]

This doctrinal disarray in the courts has been well-documented by legal scholars who have written extensively on the subject and have advanced various theoretical models for attaining a unified and coherent

---

[7] *Compare, e.g., Stahl*, 206 So.3d 124 (questioning whether compelling the production of a key to open a strongbox is in fact distinct from telling an officer the combination to a safe and questioning the continued viability of that distinction given the advancement of technology) with *Davis*, 220 A.3d 534 (adhering to the pre-digital era key to a strongbox/combination to a wall safe distinction in the context of digital passwords); *see also Spencer*, 2018 WL 1964588 (while storing evidence on an encrypted device may be equivalent to storing items in a safe protected by a combination, it is irrelevant to a compelled decryption because forcing the suspect to open the safe with his password does not provide the combination to the government); *United States v. Oloyede*, 933 F.3d 302 (4th Cir. 2019) (same).

[8] *Compare Spencer*, 2018 WL 1964588 (determining the constitutionality of a compelled production of a digital password based on whether the defendant protected his electronic files with a fingerprint key or an alphanumeric password produces an absurd result) with *Matter of Residence in Oakland, California*, 354 F. Supp. 1010 (biometric features are the equivalent of a digital password for purposes of foregone conclusion exception).

jurisprudence on the subject. *See, e.g.,* Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019) (noting in the context of encrypted digital containers the important distinction between evidence that "opens the door" of the container [a password] and the "treasure" that resides inside it [the computer contents] and arguing that the Fifth Amendment provides no protection from compelled production of a password when the government can show it has independent knowledge that the suspect knows the password); Aloni Cohen, Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries,* 32 HJVLT 169 (2019) (examining the wide variety of technical variations in encryption technology that are relevant to the compelled decryption analysis and must be considered in order to develop a robust doctrine that will remain unequivocal and relevant over time); Joseph Jarone, *An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption*, 10 FIULR 767 (2015) (noting that difference between compelled production of decryption password and compelled production of physical documents has been the source of much confusion and that rejection of the foregone conclusion exception in the context of digital passwords provides encryption users with greater protection than the Fifth Amendment requires); Wayne R. LaFave, Jerold H. Israel, Nancy J. King, Orin S. Kerr, *Testimonial Character and the Foregone Conclusion Standard,* CRIMPROC § 8.13(a) (December 2019 Update) (collecting cases applying *Fisher* and its progeny to encrypted electronic device cases).

The disparity in the holdings of courts, state and federal, throughout the country on this subject is precisely the type of case that warrants review by this Court. The Court's governing rule provides that "[r]eview on a writ of certiorari is not a matter of right, but of judicial discretion" and "will be granted only for compelling reasons." U.S. Sup. Ct. R. 10. Among the reasons that the Court will consider is that a state supreme court "has decided an important federal question in a way that conflicts with the decision of another state court of last resort or of a United States court of appeals" or "has decided an important question of federal law that has not been, but should be, settled by this Court..." *Id.* These considerations describe this case precisely.

These intractable issues surrounding the application of *Fisher* to compelled decryption of encrypted information that is subject to a judicially-sanctioned search urgently require this Court's attention and resolution. Guidance from the Court will furnish desperately-needed clarity, uniformity, stability, and predictability of the governing Fifth Amendment jurisprudence that will stem the tide of growing judicial chaos on the subject.

CONCLUSION

The Court should grant the petition.

Respectfully submitted,

JOSH SHAPIRO
Attorney General
Commonwealth of Pennsylvania

JENNIFER C. SELBER
Executive Deputy Attorney General
Director, Criminal Law Division

JAMES BARKER
Chief Deputy Attorney General
Appeals & Legal Services Section

WILLIAM R. STOYCOS *
Senior Deputy Attorney General
Counsel of Record

Office of Attorney General
16th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 787-6348

Counsel for Petitioner

Date: April 20, 2020