[J-42-2019] [MO: Todd, J.]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

COMMONWEALTH OF PENNSYLVANIA,	:	No. 56 MAP 2018
	:	
Appellee	:	Appeal from the Order of the Superior
	:	Court at No. 1243 MDA 2016 dated
	:	November 30, 2017, Reconsideration
v.	:	denied February 5, 2018, Affirming the
	:	Order of the Luzerne County Court of
	:	Common Pleas, Criminal Division, at
JOSEPH J. DAVIS,	:	Nos. CP-40-CR-291-2016 and CP-40-
	:	MD-11-2016 dated June 30, 2016
Appellant	:	
	:	ARGUED: May 14, 2019

DISSENTING OPINION

JUSTICE BAER **DECIDED: November 20, 2019**

I respectfully dissent from the majority's decision, which holds that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination does not apply to the compelled disclosure of a computer password because the password manifests from one's mind. I further disagree with the majority's alternative holding that if the foregone conclusion exception would apply under the circumstances presented, the Commonwealth failed to satisfy the requisites thereof because it did not establish that it had knowledge of the various files stored on Appellant's computer hard drive in addition to the single previously identified file that contained child pornography.

Preliminarily, I acknowledge that the issue presented in this appeal is one of first impression, with which courts across the nation have struggled. *See generally* Marjorie A. Shields, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*,

84 A.L.R. 6th 251 (2019) (compiling Fifth Amendment cases involving "compelled disclosure of an individual's password, means of decryption, or unencrypted copy of electronically stored data"). Upon review of the High Court's seminal decision in *Fisher v. United States*, 425 U.S. 391 (1976), which first recognized the foregone conclusion exception, and its progeny, I would hold that the foregone conclusion analysis applies to the compelled disclosure of a password to an electronic device, which the Commonwealth has seized pursuant to a warrant.

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. Trial Court Order, 6/30/2016. 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.

I. The Fifth Amendment As Applied To Acts of Production

As noted by the majority, the Fifth Amendment provides, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S.

CONST. amend V. Courts have interpreted the privilege as protecting a citizen "from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature." *Pennsylvania v. Muniz*, 496 U.S. 582, 588-89 (1990) (citations omitted). The Fifth Amendment "does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating." *Fisher*, 425 U.S. at 408. To be testimonial, a communication must either "explicitly or implicitly . . . relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210 (1988).

In *Fisher*, the High Court explained that in addition to traditional testimony, acts of production may implicate the Fifth Amendment because the "act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced." 425 U.S. at 410. The Court explained that compliance with a request for evidence "tacitly concedes" the existence of the evidence, possession or control of the evidence by the individual, and the belief that the evidence is, in fact, the item requested by the government. *Id.* Whether the act of production has a testimonial aspect sufficient to warrant Fifth Amendment protection "depends on the facts and circumstances of particular cases or classes thereof." *Id.*

It is well established that some compelled acts have no testimonial aspects and, thus, no Fifth Amendment protection, as the acts do not require an accused to relate a factual assertion, disclose knowledge, or "speak his guilt." *Doe v. United States*, 487 U.S. 201, at 210-11 (1988). These include, for example, furnishing a blood sample, providing a voice or handwriting exemplar, or standing in a line-up. *Id.* (collecting cases). Other compelled acts, such as the production of certain subpoenaed documents, may have a compelled testimonial aspect warranting Fifth Amendment protection where the

government's demand is akin to a "detailed written interrogatory or a series of questions at a discovery deposition," characterized as a "fishing expedition." *United States v. Hubbell*, 530 U.S. 27, 36, 41-42 (2000).[1]

Finding that an act of production has testimonial aspects, however, does not necessarily mean that the Fifth Amendment privilege precludes compulsion of the evidence sought. As the majority cogently observes, the United States Supreme Court has found that information, otherwise testimonial in nature, is unprotected where the production of such information is a foregone conclusion. Majority Opinion at 20. The foregone conclusion exception applies where the existence and location of the compelled evidence "adds little or nothing to the sum total of the government's information." *Fisher,* 425 U.S. at 410. The High Court in *Fisher* explained that a foregone conclusion exists where "[t]he question is not of testimony but of surrender." *Id*. at 411 (quoting *In re Harris*, 221 U.S. 274, 279 (1911)). Thus, as the majority recognizes, "what is otherwise testimonial in nature is rendered non-testimonial, as the facts sought to be compelled are a foregone conclusion." Majority Opinion at 21.

In my opinion, the compulsion of Appellant's password is an act of production, requiring him to produce a piece of evidence similar to the act of production requiring one to produce a business or financial document, as occurred in *Fisher*.[2] *See* Trial Court Order, 6/20/2016 (directing Appellant to "supply the Commonwealth with any and all

[1] In *Hubbell,* the Supreme Court held that the act of producing thousands of subpoenaed documents had testimonial aspects in that the act of production communicated information about the documents' existence, custody, and authenticity. The High Court concluded that, unlike in *Fisher*, the government had shown no prior knowledge of either the existence or whereabouts of the documents, thus, the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination did not apply.

[2] The summonses in *Fisher* directed the defendants' attorneys to produce documents relating to the defendants' tax returns in connection with an investigation into possible civil or criminal liability under federal income tax laws.

passwords used to access the HP Envy 700 desktop computer with serial # MXX4100000042C containing Seagate 2 TB hard drive with serial # Z4Z1AAAEFM"). An order compelling disclosure of the password, here a 64-character password, has testimonial attributes, not in the characters themselves, but in the conveyance of information establishing that the password exists, that Appellant has possession and control of the password, and that the password is authentic, as it will decrypt the encrypted computer files. The Commonwealth is not seeking the 64-character password as an investigative tool, as occurred in *Hubbell*, where the government compelled the disclosure of thousands of documents to engage in a fishing expedition to discover evidence of the defendant's guilt. To the contrary, the Commonwealth already possesses evidence of Appellant's guilt, which it set forth in an affidavit of probable cause to obtain a warrant to search Appellant's computer. Stated differently, the Commonwealth is not asking Appellant to "speak his guilt," but merely to allow the government to execute a warrant that it lawfully obtained.

Because I view the compulsion order as requiring the "surrender" of Appellant's password to decrypt his computer files, I would apply *Fisher's* act-of-production test. The majority declines to apply the foregone conclusion rationale to the compelled disclosure of Appellant's computer password, finding that to do so would constitute a "compulsion of one's mental processes" in violation of the Fifth Amendment. Majority Opinion at 22. There is 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.[3]

[3] 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

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. Under the majority's reasoning, the compelled production of documents would be tantamount to placing the defendant on the stand and requiring him to testify as to the location of the documents sought. 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.

II. Application of the Foregone Conclusion Test

Having determined that the foregone conclusion rationale may potentially apply to cases involving the compelled disclosure of a computer password, significant questions arise regarding how to administer the three-part test. As observed by the majority, to satisfy the foregone conclusion exception to the Fifth Amendment privilege, "the government must establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence." Majority Opinion at 21.

As an alternative holding, the majority opines that if the Court were to find that the foregone conclusion exception could apply to the compelled disclosure of a password, it would apply *Fisher's* act-of-production test to the computer files stored on Appellant's computer. *See* Majority Opinion at 25 n.9 (holding that "because the Commonwealth has failed to establish that its search is limited to the single previously identified file [containing child pornography], and has not asserted that it is a foregone conclusion as to the existence of additional files that may be on the computer, which would be accessible to

---

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.

the Commonwealth upon Appellant's compelled disclosure of the password, we find the Commonwealth has not satisfied the foregone conclusion exception").

Respectfully, it is my position that the 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 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, testimonial 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 point 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 exception by focusing only on the compelled

evidence itself, *i.e.*, the computer password, and not the decrypted files that the password would ultimately reveal. *See, e.g., United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n.7 (3rd Cir. 2017) ("[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. In this case, the fact known to the government that is implicit in the act of providing the password for the device is 'I, John Doe, know the password for these devices.'"); *State v. Johnson*, 576 S.W.3d 205, 277 (Mo. Ct. App. 2019) (holding that the focus of the foregone conclusion exception as applied to the compelled entering of one's cell phone passcode is the extent of the government's knowledge about the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014) (holding that the compelled decryption of computer files satisfied the elements of the foregone conclusion exception because the government already knew the implicit facts conveyed through the act of entering the encryption key, such as the defendant's ownership and control of the computers, knowledge of the encryption, and knowledge of the encryption key); *State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. 2018) (holding that whether the government was aware of the possible contents of the defendant's cell phones was immaterial "because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes").

III. Application to Future Cases

Finally, it is my belief that the majority's approach could render inconsistent results as the determination of whether there was a Fifth Amendment violation in compelled decryption cases could depend upon the type of password that the individual employed to protect his encrypted files. For example, according to the majority, if the accused used

a multi-character password to encrypt computer files, as occurred here, and the government compelled the individual to supply the password, a Fifth Amendment violation would result because the password manifests through the use of one's mind. Majority Opinion at 23. However, if the individual employed a biometric password, such as facial recognition or a fingerprint, the majority's analysis would arguably lose its force. Under those circumstances, the individual is not using the contents of his mind but, rather, is performing a compelled act of placing his finger or face in the appropriate position to decrypt the files. Additional questions arise when the act of compulsion is not the disclosure of the password itself, but the entry of the password into the computer. It is my position that all these examples constitute acts of production that would be subject to the foregone conclusion rationale in the appropriate case. The same legal analysis should apply to the underlying act of compelled decryption of digital information when the government has obtained a warrant to search the digital container. To hold to the contrary would create an entire class of evidence, encrypted computer files, that is impervious to governmental search. This could potentially alter the balance of power between governmental authorities and criminals, and render law enforcement incapable of accessing relevant evidence.

IV. Conclusion

Accordingly, I would hold that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination applies to render non-testimonial Appellant's compelled act of producing the password to his encrypted, lawfully seized computer. As the majority observes, when government agents attempted to execute the search warrant, Appellant voluntarily informed them that he was the sole user of the computer, that he used hardwired Internet services that were password protected, that

only he knew the password to decrypt his computer files, and that he would never disclose the password, as it would incriminate him.

In addition to Appellant's voluntary disclosure to government agents that he knew the password that would decrypt the files stored on the computer that the Commonwealth lawfully seized, there is ample circumstantial evidence demonstrating Appellant's knowledge of the password. Before seizing the computer, government agents conducted an investigation of the "eMule" peer-to-peer network to identify internet users sharing child pornography. Agents made a direct connection with a device that used a particular IP address over the eMule network, which agents subsequently linked to Appellant. Using this direct connection, agents downloaded one child pornography video file from Appellant's IP address. Affidavit of Probable Cause, 10/20/2015, at 7. Based on this download, the agents obtained the search warrant for Appellant's residence. *Id.* at 9.

Upon executing the search warrant, agents seized a single desktop computer, as that was the only device connected to Appellant's IP address. N.T., 1/14/2016, at 33. Forensic analysis revealed that Appellant's IP address had used the eMule file-sharing program on 23 dates from July 4, 2015, through October 19, 2015, to share files indicative of child pornography. Affidavit of Probable Cause, 10/20/2015, at 10-11; N.T., 1/14/2016, at 29. Agent Daniel Block explained that the government reached this conclusion based upon the "SHA value," which is essentially a "digital fingerprint" that corresponds with known SHA values of child pornography files. N.T., 1/14/2016, at 20. This evidence demonstrates that Appellant possessed the password to decrypt files on the computer seized by the Commonwealth, as his own words established that he was the sole user of the computer and forensic analysis demonstrated that he was accessing the encrypted files on the days leading up to his arrest.

Under these circumstances, it was a foregone conclusion that the government knew that the password to decrypt the files existed, that Appellant had exclusive control over the password, and that the password was authentic.[4] Accordingly, the testimonial aspects of the password disclosure "adds little or nothing to the sum total of the government's information." *Fisher*, 425 U.S. at 410. Thus, I would find that the compelled disclosure of Appellant's password does not violate his Fifth Amendment privilege against self-incrimination.

Justices Dougherty and Mundy join this dissenting opinion.

[4] I would hold that the authenticity prong of the foregone conclusion exception requires the government to establish that the compelled information is what it purports to be, *i.e.*, a password that will decrypt the computer files on Appellant's hard drive. The Commonwealth may prove the authenticity of the password by Appellant's own voluntary statements. *See* Pa.R.E. 901(b) (providing that the requirement of authenticating an item of evidence may be satisfied by testimony of a witness with knowledge that an item is what it is claimed to be). Here, Appellant's voluntary statements establish that the password would decrypt the files on his hard drive; thus, I would conclude that the authenticity requirement has been satisfied.