2017 PA Super 376

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF PENNSYLVANIA
v.	:	
JOSEPH J. DAVIS,	:	No. 1243 MDA 2016
Appellant	:	

Appeal from the Order Entered June 30, 2016,
in the Court of Common Pleas of Luzerne County
Criminal Division at Nos. CP-40-CR-0000291-2016,
CP-40-MD-0000011-2016

BEFORE: GANTMAN, P.J., PANELLA, J., AND FORD ELLIOTT, P.J.E.

OPINION BY FORD ELLIOTT, P.J.E.: **FILED NOVEMBER 30, 2017**

Joseph J. Davis appeals from the June 30, 2016 order granting the Commonwealth's pre-trial motion to compel appellant to provide the password that will allow access to his lawfully-seized encrypted computer. After careful review, we affirm.

The relevant facts and procedural history of this case are as follows. On October 10, 2015, law enforcement officials executed a search warrant at appellant's residence after it was determined that a computer with an IP address subscribed to appellant utilized peer-to-peer file sharing network, eMule, to share videos depicting child pornography. During the course of the search, law enforcement officials seized a password-encrypted HP Envy 700 desktop computer. The Forensic Unit of the Pennsylvania

Office of Attorney General ("POAG") was unable to examine the contents of this computer due to the "TrueCrypt" encryption program installed on it and appellant has refused to provide the password to investigating agents.

On December 17, 2015, the Commonwealth filed a pre-trial "Motion to Compel Defendant to Provide Password for Encryption Enabled Device." On January 14, 2016, the trial court conducted an evidentiary hearing on the Commonwealth's motion. The testimony adduced at this hearing was summarized by the trial court as follows:

> **TESTIMONY OF SPECIAL AGENT [JUSTIN] LERI**
>
> On July 14, 2014, [POAG] Agent Leri was conducting an online investigation on the eDonkey2000[1] network for offenders sharing child pornography. On that date a computer was located that was sharing files believed to be sharing other files of child pornography. When the computer is located that is suspected of sharing these files, the IP address of that computer is recorded and one-to-one connection is made.
>
> Agent Leri testified that the focus of the investigation was a device at IP address 98.235.69.242. This device had a 1-to-1 connection to the [POAG] as a suspect file, depicting child pornography. The agent was undercover in a peer to peer connection. Later that same day, the file from the suspect device was made available and downloaded through the direct connection to the law enforcement computer.

[1] We note that the terms "eDonkey2000" and "eMule" are used interchangeably throughout the transcript of the January 14, 2016 hearing to describe the peer-to-peer file sharing network. (***See*** notes of testimony, 1/14/16 at 5.)

> Special Agent Leri personally viewed the file identified as [boy+man][MB]NEW!!Man&Boy 13Yo.mpg. He described it as a video, approximately twenty[-]six (26) minutes and fifty[-] four (54) seconds in length, depicting a young prepubescent boy. [Agent Leri's description of the contents of the video clearly established its extensive pornographic nature.] Officer Leri is certain that the video he watched came from [appellant's] computer. He attested that the law enforcement software is retrofitted for law enforcement and the software logs in the activity. The retrofit allows for one-to-one connection only. According to Agent Leri, what this means is that law enforcement is directly connected to the subject's computer and only the suspect's computer.
>
> The IP address was registered to Comcast Communication. After obtaining a court order directing Comcast Cable to release the subscriber information, [appellant] was identified as the subscriber. The [POAG] then obtained a search warrant for the listed address. The warrant was executed on September 9, 2014. The agent testified that [appellant] waived his ***Miranda***[2] rights and admitted that he did his time for prior pornography arrests. He then refused to answer any questions.
>
> **SPECIAL AGENT [DANIEL] BLOCK**
>
> Agent Block testified that he is a special agent assigned to the Child Predator Section of the [POAG]. On October 4, 2015, an online investigation on the eMule network for offenders sharing child pornography was being conducted. The internet provider was determined to be Comcast and an administrative subpoena was issued which revealed the billing information belonged to the billing address. The focus of the investigation was IP address 174.59.168.185, port 6350. The file was downloaded and viewed.

[2] ***Miranda v. Arizona***, 384 U.S. 436 (1966).

> [Agent Block's testimony indicated that the video in question depicted a prepubescent boy between the ages of nine and eleven years old and clearly described the extensive pornographic content of the video.]
>
> Special Agent Block indicated that the Log File provides the date and time of the download and the client user's hashtag which is unique to [appellant]. Again Comcast Cable identified, through a Court Order, the subscriber was [appellant]. A search warrant was prepared and executed at [appellant's] home. Agent Block executed a search warrant on [appellant] at his residence and gave [appellant] his ***Miranda*** warnings. While he was at [appellant's] home, [appellant] spoke to Agent Block telling him he resided alone at the apartment since 2006 and that he was hardwired internet services which are password protected. According to Agent Block, [appellant] stated he uses this service so no one else can steal his Wi-Fi. There was only one computer in the house and that [no]one else uses it.
>
> [Appellant] told Agent Block that he was previously arrested for child pornography related crimes. His reasoning was that it is legal in other countries like Japan and [the] Czech Republic, and he does not know why it is illegal here. He stated "what people do in the privacy of their own homes is their own business. It's all over the Internet. I don't know why you guys care so much about stuff when people are getting killed and those videos are being posted."
>
> Agent Block testified that [appellant's] IP address was used during downloads on the following dates: July 4, 2015; July 5, 2015; July 6, 2015; July 19, 2015; July 20, 2015, August 2, 2015; August 9, 2015; August 16, 2015; September 5, 2015; September 12, 2015; September 13, 2015; September 14, 2015; September 19, 2015; September 20, 2015; September 23, 2015; September 26, 2015; September 27, 2015; October 4, 2015; October 5, 2015; October 10,

> 2015; October 17, 2015; October 18, 2015 and October 19, 2015.
>
> While transporting [appellant] to his arraignment, [appellant] spoke about gay, X-rated movies that he enjoyed watching. He stated that he liked 10, 11, 12 & 13 year olds, referring to them as, "[a] perfectly ripe apple." Agent Block requested that [appellant] give him his password. [Appellant] replied that it is sixty-four (64) characters and "Why would I give that to you?" "We both know what's on there. It's only going to hurt me. No f[***]ing way I'm going to give it to you."
>
> **TESTIMONY OF AGENT BRADEN COOK**
>
> After [appellant] was arrested and the various devices were confiscated, Agent Cook previewed the computer. The hard drive was found to contain a "TrueCrypt" encrypted protected password setup with TrueCrypt 7.1 aBootloader. The user must input the password for the TrueCrypt encrypted volume in order to boot the system into the Operating System.
>
> Agent Cook stated that [appellant] told him that he could not remember the password. Moreover [appellant] stated that although the hard drive is encrypted, Agent Cook knows what is on the hard drive.

Trial court opinion, 6/30/16 at 3-7 (citations to notes of testimony omitted).

On February 11, 2016, appellant was charged with two counts of distribution of child pornography and two counts of criminal use of a communication facility.[3] Thereafter, on June 30, 2016, the trial court granted the Commonwealth's motion to compel and directed appellant to

[3] 18 Pa.C.S.A. §§ 6312(c) and 7512(a), respectively.

supply the Commonwealth with the password used to access his computer within 30 days. (Trial court order, 6/30/16; certified record at no. 4.) In reaching this decision, the trial court reasoned that appellant's argument under the Fifth Amendment right against self-incrimination is meritless because "[his] act of [providing the password in question] loses its testimonial character because the information is a for[e]gone conclusion." (***See*** trial court opinion, 6/30/16 at 13 (internal quotation marks omitted).)

On July 15, 2016, appellant filed a motion to immediately appeal the trial court's June 30, 2016 order. On July 19, 2016, the trial court granted appellant's motion by amending its June 30, 2016 order to include the 42 Pa.C.S.A. § 702(b) language.[4] On July 21, 2016, appellant filed a timely

[4] 42 Pa.C.S.A. § 702(b) provides as follows:

> **(b) Interlocutory appeals by permission.--** When a court or other government unit, in making an interlocutory order in a matter in which its final order would be within the jurisdiction of an appellate court, shall be of the opinion that such order involves a controlling question of law as to which there is substantial ground for difference of opinion and that an immediate appeal from the order may materially advance the ultimate termination of the matter, it shall so state in such order. The appellate court may thereupon, in its discretion, permit an appeal to be taken from such interlocutory order.

42 Pa.C.S.A. § 702(b).

notice of appeal, pursuant to Pa.R.A.P. 313(b).[5] The trial court ordered appellant to file a concise statement of errors complained of on appeal, in accordance with Pa.R.A.P. 1925(b), on July 29, 2016. Thereafter, on August 8, 2016, this court entered an order directing appellant to show cause why the appeal should not be quashed. On August 17, 2016, appellant filed a timely Rule 1925(b) statement. Appellant then filed a response to our show-cause order on August 22, 2016. On September 27, 2016, the trial court filed a one-page Rule 1925(a) opinion that incorporated by reference its prior June 30, 2016 opinion. On October 5, 2016, this court entered an order denying appellant's July 15, 2016 motion, which we treated as a petition for permission to appeal, discharging the show-cause order, and referring the issue of appealability to the merits panel.

Appellant raises the following issue for our review:

> Whether [a]ppellant should be compelled to provide his encrypted digital password despite the rights and protection provided by the Fifth Amendment to the United States Constitution and Article 1, Section 9 of the Pennsylvania Constitution?

Appellant's brief at 4.

[5] We note that appellant should have filed a petition for permission to appeal, since the trial court granted his petition to amend the underlying June 30, 2016 order. ***See*** Pa.R.A.P. 1311(b) (stating, "[p]ermission to appeal from an interlocutory order containing the statement prescribed by 42 Pa.C.S. § 702(b) may be sought by filing a petition for permission to appeal with the prothonotary of the appellate court within 30 days after entry of such order in the lower court . . . .").

Before we may entertain the merits of appellant's underlying claim, we must first determine whether this court has jurisdiction to consider the appeal under Pa.R.A.P. 313. Although the Commonwealth has not raised a question regarding our jurisdiction over the trial court's interlocutory order, we may nevertheless raise the issue of jurisdiction ***sua sponte***. ***Commonwealth v. Shearer***, 882 A.2d 462, 465 n.4 (Pa. 2005).

> It is well settled that, generally, appeals may be taken only from final orders; however, the collateral order doctrine permits an appeal as of right from a non-final order which meets the criteria established in Pa.R.A.P. 313(b). Pa.R.A.P. 313 is jurisdictional in nature and provides that "[a] collateral order is an order [1] separable from and collateral to the main cause of action where [2] the right involved is too important to be denied review and [3] the question presented is such that if review is postponed until final judgment in the case, the claim will be irreparably lost." Pa.R.A.P. 313(b). Thus, if a non-final order satisfies each of the requirements articulated in Pa.R.A.P. 313(b), it is immediately appealable.

Commonwealth v. Blystone, 119 A.3d 306, 312 (Pa. 2015) (case citations omitted; quotation marks in original).

Upon review, we conclude that the order in question satisfies each of the three requirements articulated in Rule 313(b). Specifically, the trial court's June 30, 2016 order is clearly "separable from and collateral to the main cause of action" because the issue of whether the act of compelling appellant to provide his computer's password violates his Fifth Amendment right against self-incrimination can be addressed without consideration of

appellant's underlying guilt. ***See*** Pa.R.A.P. 313(b). Second, courts in this Commonwealth have continually recognized that the Fifth Amendment right against self-incrimination is the type of privilege that is deeply rooted in public policy and "too important to be denied review." ***Id.***; ***see***, ***e.g.***, ***Veloric v. Doe***, 123 A.3d 781, 786 (Pa.Super. 2015) (stating that, "the privilege against self-incrimination is protected under both the United States and Pennsylvania Constitutions . . . and is so engrained in our nation that it constitutes a right deeply rooted in public policy[]"(citations and internal quotation marks omitted)); ***Ben v. Schwartz***, 729 A.2d 547, 552 (Pa. 1999) (holding that orders overruling claims of privilege and requiring disclosures were immediately appealable under Rule 313(b)). Lastly, we agree with appellant that if review of this issue is postponed and appellant is compelled to provide a password granting the Commonwealth access to potentially incriminating files on his computer, his claim will be irreparably lost. ***See Commonwealth v. Harris***, 32 A.3d 243, 249 (Pa. 2011) (concluding that appeal after final judgment is not an adequate vehicle for vindicating a claim of privilege and reaffirming the court's position in ***Ben*** "that once material has been disclosed, any privilege is effectively destroyed[]"). Accordingly, we deem the order in question immediately appealable and proceed to address the merits of appellant's claim.

The question of whether compelling an individual to provide a digital password is testimonial in nature, thereby triggering the protections afforded

by the Fifth Amendment right against self-incrimination, and is an issue of first impression for this court. As this issue involves a pure question of law, "our standard of review is ***de novo*** and our scope of review is plenary." ***Commonwealth v. 1997 Chevrolet & Contents Seized from Young***, 160 A.3d 153, 171 (Pa. 2017) (citation omitted).

> The Fifth Amendment provides "no person . . . shall be compelled in any criminal case to be a witness against himself[.]" U.S. Const. amend. V. This prohibition not only permits an individual to refuse to testify against himself when he is a defendant but also privileges him not to answer official questions put to him in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate him in future criminal proceedings.

Commonwealth v. Cooley, 118 A.3d 370, 375 (Pa. 2015) (case citations and some internal quotation marks omitted). "To qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating and compelled." ***Commonwealth v. Reed***, 19 A.3d 1163, 1167 (Pa.Super. 2011) (citation omitted), ***appeal denied***, 30 A.3d 1193 (Pa. 2011).[6]

Although not binding on this court, the Supreme Judicial Court of Massachusetts examined the Fifth Amendment implications of compelling an individual to produce a password key for an encrypted computer and its

[6] We note that our supreme court has recognized that Article I, § 9 of the Pennsylvania Constitution "affords no greater protections against self-incrimination than the Fifth Amendment to the United States Constitution." ***Commonwealth v. Knoble***, 42 A.3d 976, 979 n.2 (Pa. 2012) (citation omitted).

relation to the "forgone conclusion" doctrine in ***Commonwealth v. Gelfgatt***, 11 N.E.3d 605 (2014). The ***Gelfgatt*** court explained that,

> [t]he "foregone conclusion" exception to the Fifth Amendment privilege against self-incrimination provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government, such that the individual "adds little or nothing to the sum total of the Government's information." For the exception to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence.

Id. at 614, citing ***Fisher v. United States***, 425 U.S. 391, 410-413 (1976) (quotation marks in original; remaining citations omitted).

More recently, in ***United States v. Apple MacPro Computer***, 851 F.3d 238 (3d. Cir. 2017), the Third Circuit Court of Appeals explained that in order for the foregone conclusion exception to apply, the Commonwealth "must be able to describe with reasonable particularity the documents or evidence it seeks to compel." ***Id.*** at 247, citing ***United States v. Bright***, 596 F.3d 683, 692 (9th Cir. 2010).

Additionally, in ***State v. Stahl***, 206 So.3d 124 (Fla. Dist. Ct. App. 2016), the Second District Court of Appeals of Florida addressed a similar issue in the context of a motion to compel a defendant charged with video voyeurism to produce the passcode for his iPhone. The ***Stahl*** court held that requiring a defendant to produce his passcode did not compel him to

communicate information that had testimonial significance. ***Id.*** at 135. The ***Stahl*** court reasoned as follows:

> To know whether providing the passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has established that it knows with reasonable particularity that the passcode exists, is within the accused's possession or control, and is authentic.
>
> . . . .
>
> The State established that the phone could not be searched without entry of a passcode. A passcode therefore must exist. It also established, with reasonable particularity based upon cellphone carrier records and Stahl's identification of the phone and the corresponding phone number, that the phone was Stahl's and therefore the passcode would be in Stahl's possession. That leaves only authenticity. And as has been seen, the act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating—no other means of authentication may exist. If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.

Id. at 136 (citations omitted). With these principles in mind, we turn to the issue presented.

Appellant contends that the act of compelling him to disclose the password in question is tantamount to his testifying to the existence and location of potentially incriminating computer files, and that contrary to the trial court's reasoning, it is not a "foregone conclusion" that the computer in question contains child pornography because the Commonwealth conceded it

does not actually know what exact files are on the computer. (Appellant's brief at 7-8.) We disagree.

As noted, the United States Supreme Court has long recognized that the Fifth Amendment right against self-incrimination is not violated when the information communicated to the government by way of a compelled act of production is a foregone conclusion. ***See Fisher***, 425 U.S. at 409. Instantly, the record reflects that appellant's act of disclosing the password at issue would not communicate facts of a testimonial nature to the Commonwealth beyond that which he has already acknowledged to investigating agents.

Specifically, the testimony at the January 14, 2016 hearing established that the Commonwealth "knows with reasonable particularity that **the passcode exists**, **is within the accused's possession** or control, and **is authentic**." ***See Stahl***, 206 So.3d at 136 (emphasis added). First, the Commonwealth clearly established that the computer in question could not be searched without entry of a password. The computer seized from appellant's residence was encrypted with "TrueCrypt" software that required a 64-character password to bypass. (Notes of testimony, 1/14/16 at 26, 30, 42.) Second, the Commonwealth clearly established that the computer belonged to appellant and the password was in his possession. Appellant acknowledged to both Agent Leri and Agent Block that he is the sole user of the computer and the only individual who knows the password in question.

(***Id.*** at 11, 26-28.) As noted, appellant repeatedly refused to disclose said password, admitting to Agent Block that "we both know what is on [the computer]" and stating "[i]t's only going to hurt me." (***Id.*** at 30.) Additionally, appellant informed Agent Leri that giving him the password "would be like . . . putting a gun to his head and pulling the trigger" and that "he would die in jail before he could ever remember the password." (***Id.*** at 36, 37.) Third, we agree with the court in ***Stahl*** that "technology is self-authenticating." ***Stahl***, 206 So.3d at 136. Namely, if appellant's encrypted computer is accessible once its password has been entered, it is clearly authentic.

Moreover, we recognize that multiple jurisdictions have recognized that the government's knowledge of the encrypted documents or evidence that it seeks to compel need not be exact. ***See Securities and Exchange Commission v. Huang***, 2015 WL 5611644, at *3 (E.D. Pa. 2015) (stating, "the Government need not identify exactly the underlying documents it seeks[.]" (citation and internal quotation marks omitted)); ***Stahl***, 206 So.3d at 135 (stating, "the State need not have perfect knowledge of the requested evidence[.]" (citation and internal quotation marks omitted)).

Herein, the record reflects that there is a high probability that child pornography exists on said computer, given the fact that the POAG's investigation determined that a computer with an IP address subscribed to appellant utilized a peer-to-peer file sharing network, eMule, approximately

25 times in 2015 to share videos depicting child pornography (notes of testimony, 1/14/16 at 5-8, 19-24, 28-29); the sole computer seized from appellant's residence had hard-wired internet that was inaccessible via a WiFi connection and contained a Windows-based version of the eMule software (***see id.*** at 7, 12, 26); and as noted, appellant implied as to the nefarious contents of the computer on numerous occasions (***see id.*** at 30, 36-37).

Based on the forgoing, we agree with the trial court that appellant's act of providing the password in question is not testimonial in nature and his Fifth Amendment right against self-incrimination would not be violated. Accordingly, we discern no error on the part of the trial court in granting the Commonwealth's pre-trial motion to compel appellant to provide the password that will allow access to his lawfully seized encrypted computer.

Order affirmed.

Judgment Entered.

Joseph D. Seletyn, Esq.
Prothonotary

Date: 11/30/2017