

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

SECURITIES AND EXCHANGE : CIVIL ACTION
COMMISSION :
 :
 :
 v. :
 : NO. 15-269
BONAN HUANG, et al. :

OPINION

KEARNEY, J.

September 23, 2015

We now consider another perspective on the interplay of mobile technology, employer rights and former employees' Fifth Amendment protections from disclosing personal secret passcodes created by Defendants, with their former employer's consent, to access the smartphones owned by their former employer. In the accompanying Order, we deny Plaintiff's motion to compel Defendants to disclose their secret personal passcodes for smartphones owned by their former employer who, as a matter of policy, required their employees to keep their personal passcodes secret from everyone.

Background relating to this discovery dispute.

Plaintiff Securities and Exchange Commission ("SEC") seeks penalties, disgorgement and equitable relief arising from Defendants' trading on certain retail stocks based on allegedly material nonpublic information available to Defendants while they worked as data analysts for Capital One, a large credit card issuer bank ("Bank").¹ Bank provided Defendants with smartphones but allowed them to create and set their own passcodes to access the smartphone.

¹ To date, the SEC has not answered Defendants' request as to whether there is any ongoing criminal investigation. Defendants, presently residing in the Far East, are evaluating possible criminal prosecution for the same conduct.

Bank's policies confirmed it owned the smartphone and any corporate documents on the smartphones. Consequently, Bank also requested its employees to not keep records of their personal passcodes for security reasons. Upon leaving the Bank, Defendants returned their smartphones. The Bank provided the smartphones to the SEC. SEC cannot access the data on the smartphones as it does not know the passcode. SEC believes the smartphones contain unidentified Bank documents and issued an interrogatory or document request requiring Defendants "[i]dentify the Passcode for the [smartphone] that you used during the course of your employment". Defendants responded by invoking their Fifth Amendment right.

SEC now moves to compel production of Defendants' passcodes for their work-issued smartphones. (ECF Doc. No. 36-1, Mem. in Supp., 2.) The SEC argues Defendants, as former Bank data analysts, are corporate custodians in possession of corporate records, and as such cannot assert their Fifth Amendment privilege in refusing to disclose their passcodes. (*Id.*) Defendants disagree they are corporate custodians and argue providing the passcodes to their phones is "testimonial" in nature and violates the Fifth Amendment. (ECF Doc. No. 43, Defs.' Resp., 1, 3-4.)

Analysis

Each party argues based on established legal precedent in non-smartphone contexts involving the interplay between corporate records and encrypted information on computers. As we find the personal thought process defining a smartphone passcode not shared with an employer is testimonial, we deny the SEC's motion to compel.

SEC claims the "corporate records" cases govern our analysis. *See Bellis v. United States*, 417 U.S. 85 (1974); *Braswell v. United States*, 487 U.S. 99 (1988). In *Bellis*, a partner of a then dissolved law firm was subpoenaed to appear and testify before a grand jury and to bring all

partnership records within his possession. 417 U.S. at 86. The former partner appeared but refused to bring the records and asserted his Fifth Amendment privilege against compulsory self-incrimination. *Id.* The district court compelled the records' production and the court of appeals affirmed. *Id.* at 86-87. In affirming the district court's decision, the United States Supreme Court relied on the "collective entity" doctrine. *Id.* at 88. The doctrine prevents an individual from "rely[ing] upon the privilege to avoid producing records of a collective entity which are in his possession in a representative capacity, even if these records might incriminate him personally." *Id.*

In *Braswell*, the Government subpoenaed books and records of two corporations, of which petitioner served as president and sole shareholder. 487 U.S. at 101. The petitioner refused to produce the documents asserting his Fifth Amendment privilege. *Id.* Citing the "collective entity" doctrine, the district court compelled production and the court of appeals affirmed. The Supreme Court affirmed after recounting the Court's Fifth Amendment jurisprudence in the context of corporate custodians. *Id.* at 105-08. The Court again reiterated a corporate custodian may not invoke the Fifth Amendment to avoid producing corporate records. *Id.* at 119.

Defendants point to more recent cases, albeit none from the Supreme Court. In *In re Grand Jury Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012), the Eleventh Circuit found a person accused of possessing child pornography may assert his Fifth Amendment privilege to avoid decrypting a hard drive. 670 F.3d at 1352-53. In reaching this conclusion, the court of appeals did not focus on whether the privilege applies to underlying documents but on whether the act of decryption and production were testimonial. *Id.* at 1343. The court of appeals held decryption and production of the hard drives "would require the use of

the contents of Doe’s mind and could not be fairly characterized as a physical act that would be nontestimonial in nature.” *Id.* at 1346. Thus, the decryption and production were testimonial and within the scope of the Fifth Amendment. *Id.*²

Defendants also rely on *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010) where the Government subpoenaed “all passwords” associated with defendant’s computer. *Id.* at 666. The district court found revealing the password akin to providing the combination of a wall safe—an act deemed to be testimonial by the Supreme Court. *Id.* at 669 (citing *United States v. Hubbell*, 530 U.S. 27, 43 (2000)). Accordingly, the district court denied the Government’s request to compel defendant produce his computer passcodes.

We find, as the SEC is not seeking business records but Defendants’ personal thought processes, Defendants may properly invoke their Fifth Amendment right. SEC does not necessarily disagree with the courts’ conclusions in *In re Grand Jury* and *Kirschner* arguing these cases involve child pornography and do not involve records of a third party entity, as here. The SEC focuses on the contents of the underlying documents contained on the device, claiming without any cited evidence, there are Bank records on the smartphones. We agree with the SEC as to Defendants’ inability to preclude production of the Bank’s documents.

However, the SEC’s reliance on the content of the documents is misplaced. *In re Grand Jury* persuades us to not look at the underlying documents to determine whether the act of producing a passcode is testimonial. 670 F.3d at 1342 (“Whether the drives’ contents are testimonial, however, is not the issue.”). By relying on the corporate records cases of *Bellis* and *Braswell*, the SEC would have us focus on the nature of the documents allegedly contained in the

² Unlike the defendant compelled to disclose his password for a social networking website in *United States v. Smalcer*, 464 Fed.Appx. 469 (6th Cir. 2012), Defendants apprehend an imminent threat of prosecution and have not already been convicted.

phone rather than what they have requested, which are passcodes to the phones. Here, the SEC seeks to compel production of the passcodes which require intrusion into the knowledge of Defendants and no one else. There is no evidence the Bank assigned Defendants passcodes to their phones or kept track of Defendants' passcodes. To the contrary, the Bank asked employees not to keep records of their passwords for safety reasons.³

Absent waiver of the confidentiality attendant to this personal thought process, we cannot find the personal passcodes to the Bank's smartphones to be corporate records falling under the collective entity cases. We find Defendants' confidential passcodes are personal in nature and Defendants may properly invoke the Fifth Amendment privilege to avoid production of the passcodes.⁴

The SEC then argues the "foregone conclusion" doctrine applies to override Defendants' invocation of the Fifth Amendment privilege. An act of production is not testimonial if the proponent of production can show with "reasonable particularity," "at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a foregone conclusion." *In re Grand Jury*, 670 F.3d at 1345-56. Thus, "where the location, existence, and authenticity of the purported evidence is known with reasonable

³ The SEC notes the Bank allows employees to keep records only if the storage method is approved by the Bank. This fact does not change our analysis.

⁴ Because the Court finds the passcodes are not corporate records, it need not reach the issue of whether Defendants are corporate custodians. Compare *In re Three Grand Jury Subpoenas Duces Tecum Dated January 29, 1999*, 191 F.3d 173, 179-83 (2d Cir. 1999) (refusing to extend *Braswell* to cover former employees), and *United States v. McLaughlin*, 126 F.3d 130, 133-34 (3d Cir. 1997) ("[A] former employee . . . who produces purloined corporate documents is obviously not within the scope of the *Braswell* rule."), with *In re Grand Jury Dated November 12, 1991*, 957 F.2d 807 (11th Cir. 1992) (declining to draw distinction between current employees and former employees with regard to Fifth Amendment privilege).

particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available." *Id.* at 1344.

The SEC argues any incriminating testimonial aspect to Defendants' production of their personal passcodes already is a foregone conclusion because it can show Defendants were the sole users and possessors of their respective work-issued phones. (ECF Doc. No. 45, Pl.'s Reply, 5.) The SEC's argument misses the mark in this regard. The court of appeals' reasoning in *In re Grand Jury* again persuades our analysis. There, the Court of Appeals for the Eleventh Circuit refused to apply the "foregone conclusion" doctrine because the Government could not meet its burden of showing with "reasonable particularity" what "if anything, was hidden behind the encrypted wall." 670 F.3d at 1349. While the Government need not "identify exactly" the underlying documents it seeks, "categorical requests for documents the Government anticipates are likely to exist simply will not suffice." *Id.* at 1348. There, the Government could not show the encrypted drives actually contained any files, nor could it show which files would if any prove to be useful. *Id.* at 1347.

Here, the SEC proffers no evidence rising to a "reasonable particularity" any of the documents it alleges reside in the passcode protected phones. Instead, it argues only possession of the smartphones and Defendants were the sole users and possessors of their respective work-issued smartphones. SEC does not show the "existence" of any requested documents actually existing on the smartphones. Merely possessing the smartphones is insufficient if the SEC cannot show what is actually on the device. *See id.* ("In short, the Government physically possess the media devices, but it does not know what, if anything, is held on the device."). Neither *In re Boucher*, No. 06-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) nor *United States v. Gavegnano*, 305 F. App'x 954 (4th Cir. 2009), militate a different result. In *Boucher*, an ICE

agent accessed the encrypted part of the drive at issue, viewed the contents of the drive, and ascertained it may contain images and videos of child pornography. 2009 WL 424718, at *3. Thus, the defendant providing access to the encrypted portion of the drive “add[ed] little or nothing” to the Government’s information. *Id.* Likewise, in *Gavegnano*, the Government could independently verify the defendant was the sole user and that he accessed child pornography websites because the computer was monitored for all activity. 305 F. App’x at 955-56.

Here, the SEC has no evidence any documents it seeks are actually located on the work-issued smartphones, or that they exist at all. Thus, the foregone conclusion doctrine is not applicable.

Conclusion

Since the passcodes to Defendants’ work-issued smartphones are not corporate records, the act of producing their personal passcodes is testimonial in nature and Defendants properly invoke their fifth Amendment privilege. Additionally, the foregone conclusion doctrine does not apply as the SEC cannot show with “reasonable particularity” the existence or location of the documents it seeks. Accordingly, the SEC’s motion to compel the passcodes is denied.