COMMONWEALTH OF VIRGINIA

EDWARD W. HANSON, JR.
A. BONWILL SHOCKLEY
H. THOMAS PADRICK, JR.
STEPHEN C. MAHAN
WILLIAM R. O'BRIEN
LESLIE L. LILLEY
GLENN R. CROSHAW
STEVEN C. FRUCCI

CIRCUIT COURT JUDGES OFFICE
CITY OF VIRGINIA BEACH
JUDICIAL CENTER, BLDG. 10
2425 NIMMO PARKWAY
VIRGINIA BEACH, VA 23456-9017
(757) 385-4501
www.vbgov.com/courts
Direct Dial # 385-8680

SECOND JUDICIAL CIRCUIT

October 28, 2014

Eleanor Gaines, Esquire
Office of the Commonwealth's Attorney
2425 Nimmo Parkway
Building 10B, Second Floor
Virginia Beach, VA 23456

James O. Broccoletti, Esquire
Zoby, Broccoletti & Normile, P. C.
6633 Stoney Point South
Norfolk, VA 23502

Re: Commonwealth of Virginia v. David Charles Baust
Docket No.: CR14-1439

Dear Counsel:

This matter is before the court on the Commonwealth's Motion to Compel the Production of the Passcode or Fingerprint to Encrypted Smartphone. The hearing took place Tuesday, October 28, 2014, at which the Defendant, the Commonwealth, and the witness for the Commonwealth were present. For the reasons set forth below, the Motion is denied in part and granted in part.

David Charles Baust, Defendant, is charged by indictment with violating Code of Virginia § 18.2-51.6, Strangling Another Causing Wounding or Injury. On February 19, 2014, Defendant allegedly assaulted the victim in his bedroom at his house. The victim stated that Defendant maintained a recording device that continuously recorded in the room where the assault purportedly took place. On the morning of February 19, 2014, after being assaulted the victim states she went to grab the video equipment from its usual place and Defendant assaulted her again to prevent her from taking the equipment. The victim stated that Defendant had previously transmitted video footage to her through text messaging of the victim and himself engaging in sexual intercourse in his room. The victim additionally admitted that the video recorder transmits to Defendant's smart phone. Pursuant to a search warrant executed several days later, the police were able to recover the phone, several recording devices, assorted discs,

flash drives, and computer equipment belonging to Defendant. The victim and Defendant both affirmed to the officers at the scene that the recording device, connected to Defendant's cell phone "could have possibly" recorded the assault and the recording "may exist" on the phone. Additionally, the testimony before the court from the victim was that the device "could have recorded" the assault and therefore there "may be a recording." Entry to the phone has been prevented by encryption either by passcode or fingerprint.

The question before the court is whether the production of one's passcode or fingerprint is testimonial communication and therefore subject to the defendant's Fifth Amendment privilege against self-incrimination. The Commonwealth argues that the passcode and the fingerprint are not testimonial because the existence of the recording is a "foregone conclusion." Defense Counsel argues that both are testimonial in that either would provide access to all recordings or items on Defendant's phone.

Analysis

The Fifth Amendment to the Constitution of the United States provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend V. "[T]he Fourteenth Amendment secures against state invasion the same privilege that the Fifth Amendment guarantees against federal infringement – the right of a person to remain silent unless he chooses to speak in the unfettered exercise of his own will." *Schmerber v. Cal.*, 384 U.S. 757, 760 (1966) (citation omitted). "[T]he privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature." *U.S. v. Wade*, 388 U.S. 218, 221 (1967) (citation omitted). Thus the proper inquiry requires the court to resolve whether granting the motion to compel "would require (1) compulsion of a (2) testimonial communication that is (3) incriminating." *U. S. v. Authement*, 607 F.2d 1129, 1131 n. 1 (5th Cir. 1979).

It is a "settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege [against self-incrimination]." *United States v. Hubbell*, 530 U.S. 27, 35–36 (2000); *accord Fisher v. United States*, 425 U.S. 391, 401 (1976) ("[T]he *Fifth Amendment* protects against 'compelled self-incrimination, not the disclosure of private information'"). Thus the contents of the phone, obtained pursuant to a validly executed warrant are only subject to objections raised under the *Fourth Amendment*, not the *Fifth Amendment*. Additionally, there is no question that a motion to compel is compulsive and the production of the passcode or fingerprint would be incriminating.[1] The analysis turns on whether a passcode or a fingerprint is "testimonial communication."

[1] Incriminating has been defined as "any disclosures that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used." *Kastigar v. United States*, 406 U.S. 441, 445 (1972).

Passcode or Fingerprint

"An act is testimonial when the accused is forced to reveal his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the government." *U.S. v. Kirschner*, 823 F. Supp. 2d 665, 668 (2010) (citing *United States v. Doe*, 487 U.S. 201, 212 (1987)). "[T]here is a significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating." *Hubbell*, 530 U.S.at 35. "[T]he privilege offers no protection against compulsion to submit to fingerprinting, photography, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture." *Wade*, 388 U.S. at 223. "[E]ven though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief." *Hubbell*, 530 U.S. at 35.

A witness's "act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tend[s] to incriminate [him or her]." *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335, 1343 (11th Cir. 2012) (citing holding of *Fisher v. United States*, 425 U.S. 391, 410 (1976)). Nevertheless, "[w]hen the 'existence and location' of the documents under subpoena are a 'foregone conclusion' and the witness 'adds little or nothing to the sum total of the Government's information by conceding that he in fact has the [documents],' then no Fifth Amendment right is touched because the 'question is not of testimony but of surrender.'" *Doe v. United States (In re Grand Jury Subpoena)*, 383 F.3d 905, 910 (9th Cir. 2004) (citing *Fisher*, 425 U.S. at 411). "[T]he Government is in no way relying on the 'truthtelling' of the [witness] to prove the existence of or his access to the documents." *Fisher*, 425 U.S. at 411. "Whether the existence of documents is a foregone conclusion is a question of fact, subject to review for clear error." *United States v. Norwood*, 420 F.3d 888, 895 (8th Cir. 2005) (citing *United States v. Doe*, 425 U.S. 605, 613–14 (1984)).

Therefore, in *Hubbell*, the Court found the action of producing documents in response to a subpoena was testimonial in nature and therefore subject to the constitutional privilege against self-incrimination. *Hubbell*, 530 U.S. at 40. The Court was persuaded by the fact that in the act of production, the respondent had to take "the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena." Id. at 42. The Court reasoned that given this information, "[b]y 'producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.' Moreover, . . . when the [witness] responds to the subpoena, he may be compelled to take the witness stand

and answer . . . whether he has produced everything demanded by the subpoena." Id. at 36–37. The Court found notable that the text of the subpoena, often using the phrase "any and all documents related," made it obvious that the prosecutor needed respondent's assistance to identify potential sources of information and to produce those sources of information. Id. at 41. Therefore, when the respondent produced these documents in response to the subpoena, it was the "functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition." Id. at 41–42. "The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." Further, the Hubbell Court found that the "foregone conclusion" doctrine did not apply in this case, where the Government had not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent." Id. at 45.

Similarly, in the context of compelling the production of a passcode, the U.S. District Court for the Eastern District of Michigan held that compelling the defendant to provide a password is a testimonial communication. *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010). The court reasoned "forcing the Defendant to reveal the password . . . requires Defendant to communicate 'knowledge,' unlike the production of a handwriting sample or a voice exemplar." *Id.* "It is the 'extortion of information from the accused,' the attempt to force him to 'disclose the contents of his own mind' that implicates the *Self-Incrimination Clause*." *Id.* (quoting *United States v. Doe*, 487 U.S. at 211) (emphasis in original). The court found *Hubbell's* distinction between telling an inquisitor the combination to a wall safe and surrendering a key to a strongbox instructive. *Id.* Similar to having to divulge the combination to a safe, the court reasoned "the government is not seeking documents or objects – it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password." *Id.*; *accord In re Grand Jury Subpoena (Boucher)*, No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951 at *16, 2007 WL 4246473 (D. Vt. Nov. 29, 2007) ("Since the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing. If Boucher knows the password, it only exists in his mind.").[2]

In this case, the Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same. The footage itself would not be protected under the Fifth Amendment because its creation was voluntary, i.e. not compelled. As stated above, the *Fifth Amendment* only protects against "compelled" self-incrimination, therefore the contents of Defendant's

[2] However, on appeal, the District Court for the District of Vermont found that requiring Defendant to produce an unencrypted version of the documents in his encrypted hard drive that he had already provided access to previously was not testimonial because the existence of and location of the documents were a "foregone conclusion." *In re Grand Jury Subpoena to Boucher*, 2009 U.S. Dist. LEXIS 13006 at *8, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

phone, created voluntarily, are not protected against disclosure. However, compelling Defendant to provide access through his passcode is both compelled and testimonial and therefore protected. Contrary to the Commonwealth's assertion, the password is not a foregone conclusion because it is not known outside of Defendant's mind. Unlike a document or tangible thing, such as an unencrypted copy of the footage itself, if the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it. As reasoned in *Kirschner*, Defendant cannot be compelled to "divulge through his mental processes" the passcode for entry. The fingerprint, like a key, however, does not require the witness to divulge anything through his mental processes. On the contrary, like physical characteristics that are non-testimonial, the fingerprint of Defendant if used to access his phone is likewise non-testimonial and does not require Defendant to "communicate any knowledge" at all. Unlike the production of physical characteristic evidence, such as a fingerprint, the production of a password forces the Defendant to "disclose the contents of his own mind." For this reason the motion to compel the passcode should be **DENIED** but the motion to compel the fingerprint should be **GRANTED**.

Unencrypted Footage

Neither has the Commonwealth asked to compel the unencrypted video recording. However, from the testimony of the witness at the hearing, the existence and location of the recording is not a foregone conclusion and compelling Defendant to produce an unencrypted version would be self-incriminating. The most the Commonwealth knows is that the recording "could exist" because the device "may have recorded" the assault and transmitted it to the phone. The alternative is also true, that the device "may not have" recorded the assault and the recording "may not exist." This being the only reason the Commonwealth suspects there may be a recording, the existence and location of the recording is not a foregone conclusion. Defendant's production of the unencrypted recording would be testimonial because Defendant would be admitting the recording exists, it was in his possession and control, and that the recording is authentic. Therefore, the Commonwealth could not compel Defendant to produce an unencrypted version of the recording.

Sincerely,

Steven C. Frucci
Presiding Judge

SCF/alg/nc