

**IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES**

UNITED STATES,)	APPELLEE'S ANSWER
Appellant)	
)	Crim. App. Dkt. No. 20150776
v.)	
)	USCA Dkt. No. 17-0153/AR
Sergeant (E-5))	
Edward J. Mitchell, II,)	
United States Army,)	
Appellee)	

JOSHUA B. FIX
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road, Room 2014
Fort Belvoir, VA 22060
(703) 693-0658
joshua.b.fix2.mil@mail.mil
USCAAF Bar No. 36775

KATHERINE L. DEPAUL
Captain, Judge Advocate
Acting Branch Chief,
Defense Appellate Division
USCAAF Bar No. 36536

CHRISTOPHER D. CARRIER
Lieutenant Colonel, Judge Advocate
Chief, Capital and
Complex Litigation Branch
USCAAF Bar Number 32172

Index of Brief

I. WHETHER THE FIFTH AMENDMENT’S SELF-INCRIMINATION CLAUSE IS VIOLATED WHEN A SUSPECT VOLUNTARILY UNLOCKS HIS PHONE WITHOUT GIVING HIS PERSONAL IDENTIFICATION NUMBER TO INVESTIGATORS.

II. WHETHER THE EDWARDS RULE IS VIOLATED WHEN INVESTIGATORS ASK A SUSPECT, WHO HAS REQUESTED COUNSEL AND RETURNED TO HIS PLACE OF DUTY, TO UNLOCK HIS PHONE INCIDENT TO A VALID SEARCH AUTHORIZATION.

III. WHETHER, ASSUMING INVESTIGATORS VIOLATED APPELLANT’S FIFTH AMENDMENT PRIVILEGE OR THE EDWARDS RULE, THE MILITARY JUDGE ERRED BY SUPPRESSING THE EVIDENCE.

Issues Certified	1
Statement of Statutory Jurisdiction	2
Statement of the Case	2
Statement of Facts	3
Standard of Review	8
Summary of the Argument	8
Argument	10

I. This Court should affirm the military judge’s ruling because her findings of fact are well-supported, her conclusions of law are correct, and suppression is appropriate under Edwards and Mil. R. Evid. 305(c)(2)	10
---	----

A. Sergeant Mitchell did not voluntarily unlock his iPhone.	16
--	----

B. Sergeant Mitchell made a testimonial act by unlocking his cell phone	17
1. Sergeant Mitchell’s entry of his PIN and production of the decrypted contents of his iPhone was testimonial	18
2. The “foregone conclusion” exception does not apply	20
(a) This Court should decline to extend the “foregone conclusion” exception to evidence obtained in violation of the <i>Edwards</i> rule.....	21
(b) This court should not disturb the military judge’s finding that the foregone conclusion exception does not apply unless it is clearly erroneous .	22
(c) The existence, possession, control, and authenticity of the iPhone and its contents were not a foregone conclusion	23
C. The military judge’s remedy was appropriate	26
1. Suppression of the physical iPhone was appropriate	26
2. Suppression of the iPhone’s contents was appropriate.....	27
II. The investigators in this case violated the Edwards rule	29
A. Sergeant Mitchell was in custody when the investigators asked him multiple questions about his iPhone.....	30
B. The investigators further interrogated SGT Mitchell after he invoked his right to counsel and while he was in custody.....	33
III. The military judge did not abuse her discretion by suppressing the iPhone and its decrypted contents.....	35
A. The exclusionary rule is appropriately applied to derivative evidence of an involuntary statement.....	35
B. The doctrine of inevitable discovery is inapplicable to this case	39
Conclusion.....	41

Table of Authorities

United States Supreme Court

<i>Chavez v. Martinez</i> , 538 U.S. 760 (2003).....	39
<i>Curcio v. United States</i> , 354 U.S. 118 (1957)	13, 17
<i>Doe v. United States</i> , 487 U.S. 201 (1988).....	14
<i>Edwards v. Arizona</i> , 451 U.S. 477 (1981)	passim
<i>Fisher v. United States</i> , 425 U.S. 391 (1976)	20-23
<i>Hoffman v. United States</i> , 341 U.S. 479 (1951).....	28
<i>Kastigar v. United States</i> , 406 U.S. 441 (1972).....	28
<i>Maryland v. Shatzer</i> , 559 U.S. 98 (2009)	16, 38
<i>Rhode Island v. Innis</i> , 446 U.S. 291 (U.S. 1980).....	34
<i>Smith v. Illinois</i> , 469 U.S. 91 (1984).....	29
<i>Thompson v. Keohane</i> , 516 U.S. 99 (1995)	30
<i>Unites States v. Doe</i> , 465 U.S. 605 (1984)	17, 22-23
<i>United States v. Hubbell</i> , 530 U.S. 27 (2000).....	passim
<i>United States v. Patane</i> , 542 U.S. 630 (2004)	35, 38-39

United States Court of Appeals for the Armed Forces / Court of Military Appeals

<i>United States v. Ayala</i> , 43 M.J. 296 (C.A.A.F. 1995)	8-9
<i>United States v. Baker</i> , 70 M.J. 283 (C.A.A.F. 2011)	9
<i>United States v. Chatfield</i> , 67 M.J. 432 (C.A.A.F. 2009)	30-33

<i>United States v. Cossio</i> , 64 M.J. 254 (C.A.A.F. 2007)	10
<i>United States v. Cowgill</i> , 68 M.J. 388 (C.A.A.F. 2010)	9
<i>United States v. Freeman</i> , 65 M.J. 451 (C.A.A.F. 2008)	8-9
<i>United States v. Hutchins</i> , 72 M.J. 294 (C.A.A.F. 2013)	29
<i>United States v. Kozak</i> , 12 M.J. 389 (C.M.A. 1982)	39
<i>United States v. Leedy</i> , 65 M.J. 208 (C.A.A.F. 2007)	10
<i>United States v. Lewis</i> , 65 M.J. 85 (C.A.A.F. 2007)	35
<i>United States v. Lloyd</i> , 69 M.J. 95 (C.A.A.F. 2010)	9
<i>United States v. Maxwell</i> , 45 M.J. 406 (C.A.A.F. 1996)	38
<i>United States v. McNutt</i> , 62 M.J. 16, 20 (C.A.A.F. 2005)	40
<i>United States v. Piren</i> , 74 M.J. 24 (C.A.A.F. 2015)	9
<i>United States v. Powell</i> , 40 M.J. 1 (C.M.A. 1994)	14-15, 26
<i>United States v. Stellato</i> , 74 M.J. 473 (C.A.A.F. 2015)	9
<i>United States v. White</i> , 69 M.J. 236 (C.A.A.F. 2010)	9
<i>United States v. Wicks</i> , 73 M.J. 93 (C.A.A.F. 2014)	39

United States Courts of Appeals

<i>United States v. Bright</i> , 596 F.3d 683 (9th Cir. 2010)	22, 25
<i>United States v. Doe (In re Grand Jury Subpoena Duces Tecum)</i> , 670 F.3d 1335, (11th Cir. 2012)	passim
<i>United States v. Norwood</i> , 420 F.3d 888 (8th Cir. 2005)	22

<i>United States v. Ponds</i> , 454 F.3d 313 (D.C. Cir. 2006).....	23, 25
--	--------

United States Trial Courts

<i>In re Grand Jury Subpoena (Boucher)</i> , 2009 U.S. Dist. LEXIS 13006 (D. Vt., Feb 19, 2009).....	15
--	----

<i>SEC Civil Action v. Huang</i> , 2015 U.S. Dist. LEXIS 127853 (E.D. Pa., Sep. 23, 2015)	14
---	----

<i>United States v. Fricosu</i> , 841 F. Supp. 2d 1364 (S.D. Fl. 2012)	15
--	----

<i>United States v. Kirschner</i> , 823 F. Supp. 2d 665 (E.D. Mich., 2010)	14
--	----

State Courts

<i>Commonwealth v. Gelfgatt</i> , 468 Mass. 512 (2014)	15
--	----

<i>State v. Trant</i> , 2015 Me. Super. LEXIS 272 (Super. Ct. Me., Oct. 27, 2015)...	14-15
--	-------

Constitutional Provisions, Statutes, Rules, and Other Authorities

U.S. CONST. AMEND V	passim
---------------------------	--------

Article 62, UCMJ, 10 U.S.C. § 862 (2012)	2
--	---

Article 67, UCMJ, 10 U.S.C. § 867 (2012)	2
--	---

Mil. R. Evid. 301(a)	35, 37
----------------------------	--------

Mil. R. Evid. 304.....	34-38
------------------------	-------

Mil. R. Evid. 305(c)(2).....	passim
------------------------------	--------

<i>Manual for Courts Martial</i> (2008 Ed.)	36-37
---	-------

Exec. Order 13643 of May 15, 2013, 78 Fed. Reg. 29559 (May 21, 2013).....	36-37
---	-------

**IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES**

UNITED STATES,)	APPELLEE'S ANSWER
Appellant)	
)	Crim. App. Dkt. No. 20150776
v.)	
)	USCA Dkt. No. 17-0153/AR
Sergeant (E-5))	
Edward J. Mitchell, II,)	
United States Army,)	
Appellee)	

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE
ARMED FORCES:

Issues Presented

**I. WHETHER THE FIFTH AMENDMENT'S SELF-
INCRIMINATION CLAUSE IS VIOLATED WHEN
A SUSPECT VOLUNTARILY UNLOCKS HIS
PHONE WITHOUT GIVING HIS PERSONAL
IDENTIFICATION NUMBER TO
INVESTIGATORS.**

**II. WHETHER THE EDWARDS RULE IS
VIOLATED WHEN INVESTIGATORS ASK A
SUSPECT, WHO HAS REQUESTED COUNSEL
AND RETURNED TO HIS PLACE OF DUTY, TO
UNLOCK HIS PHONE INCIDENT TO A VALID
SEARCH AUTHORIZATION.**

**III. WHETHER, ASSUMING INVESTIGATORS
VIOLATED APPELLANT'S FIFTH AMENDMENT
PRIVILEGE OR THE EDWARDS RULE, THE
MILITARY JUDGE ERRED BY SUPPRESSING
THE EVIDENCE.**

Statement of Statutory Jurisdiction

The Army Court of Criminal Appeals (Army Court) had jurisdiction over this matter pursuant to Article 62, Uniform Code of Military Justice, 10 U.S.C. § 862 (2012) [hereinafter UCMJ]. This Honorable Court has jurisdiction over this matter under Article 67(a)(2), UCMJ, 10 U.S.C. § 867(a)(2) (2012).

Statement of the Case

On August 17, 2015, various charges against Sergeant (SGT) Mitchell were referred to a general court martial. On October 29, 2015, the military judge in SGT Mitchell's case issued a ruling suppressing, *inter alia*, the iPhone and its contents at issue in this appeal. The government appealed that ruling under Article 62, UCMJ. On March 18, 2016, the Army Court returned the record of trial to the military judge for clarification on the issues of whether SGT Mitchell was in custody when interrogated about his iPhone passcode, and whether SGT Mitchell unlocked his iPhone with a passcode or "PIN." On May 17, 2016, the military judge issued clarified findings in accordance with the Army Court's guidance and reiterated her ruling suppressing the iPhone and its contents. The government again appealed under Article 62, UCMJ. On August 29, 2016, the Army Court summarily affirmed the military judge's ruling. On December 22, 2017, the government filed the Judge Advocate General of the Army's certificate for review

with this Court and the brief on behalf of the appellant. The appellee herein responds to the government's brief.

Statement of Facts

On the morning of January 8, 2015, SGT Edward Mitchell was escorted to the Fort Hood military police station for questioning pertaining to the alleged violation of an order not to contact his wife, and harassment of his wife, through cell-phone text messages and other communications. (R. at 202, 203; App. Ex. XXXVI; App. Ex. LIV, p. 1). Soon after arriving, Detective MK talked to SGT Mitchell for about five minutes. (R. at 203). Detective MK told SGT Mitchell that his wife alleged he was harassing her (R. at 202-203) and then told SGT Mitchell, "knock this off if it's you." (R. at 204). He was then handed over to Investigator (INV) BT.

Investigator BT advised SGT Mitchell of his right to an attorney, which SGT Mitchell invoked at 10:50 a.m. (R. at 61; App. Ex. XXXIII at 10:02:03; App. Ex. XXVI; App. Ex. LXXXV, p.2). After SGT Mitchell invoked his right to counsel, INV BT patted him down, and escorted him to the desk sergeant for another search at 11:12 a.m. (R. at 62; App. Ex. LXXXV). At 11:45 a.m., SGT Mitchell was escorted back to his unit by a Staff Sergeant (SSG) GK, a senior noncommissioned officer (NCO) from SGT Mitchell's unit, who also escorted him to the police station. (App. Ex. LXXXV, p.2). Upon arrival to the unit, SSG GK ordered SGT Mitchell to stay in SSG GK's office, (App. Ex. Ex. LXXXIII, p. 7), while SSG GK spoke with the

company commander, CPT DH. (App. Ex. LXXXV, p. 3; R. at 218). While SSG GK was talking to the commander, SGT TW brought SGT Mitchell something to eat. (App. Ex. LXXXIII, p. 7). Sergeant Mitchell “remained in SSG [GK’s] office for approximately thirty minutes with SSG [JV]. Sergeant First Class (SFC) [SC] came to SSG [GK’s] office and told [SGT Mitchell] to report to the commander, CPT [DH], in his office. SFC [SC] escorted [SGT Mitchell] to CPT [DH’s] office.” (App. Ex. LXXXIII, p. 7). The commander told SGT Mitchell to wait in his office because “the ‘MPs are on their way’, or substantially words to that effect.” (App. Ex. LXXXIII, p. 7; R. at 509, 512).

At the police station, INV BT called a part-time military magistrate to obtain a search authorization. (R. at 63). The search authorization was for “cell phones, computers, and other data storage devices that can store and send electronic communications via email, text or other applications.” (App. Ex. XXIV).

Once INV BT received the vocal search authorization, he proceeded to SGT Mitchell’s unit with INV JC. (R. at 63). Before arriving to the unit, INV BT “back-briefed” INV JC “[they] had a VOCO Warrant” and that the “VOCO warrant detailed that any kind of electronic devices, anything that could transmit any kind of messages . . .” would be subject to the search authorization. (R. at 40). The investigators arrived at SGT Mitchell’s unit around 1:00 p.m. (R. at 68; App. Ex. LXXXV, p. 3). When they arrived, the investigators found SGT Mitchell in his

company commander's office. (R. at 68). There, SGT Mitchell's commander "signed him over" to the investigators. (R. at 512).

Both investigators informed SGT Mitchell that they had a "verbal warrant to take his phone" and that he had "to render [his] phone over to [the investigators]." (R. at 68; App. Ex. LXXXIII, p. 7). The investigators then asked SGT Mitchell if he had a cellphone on him. (R. at 41). Sergeant Mitchell did, and surrendered his iPhone to INV BT. (App. Ex. LXXXIII, p. 7; App. Ex. LXXXV, p.4). At some point in this exchange, SSG JV arrived to escort SGT Mitchell. (R. at 255). The investigators tried to access the iPhone but it was "locked" (R. at 41) thereby making its contents inaccessible to investigators unless they had the passcode SGT Mitchell created to encrypt it. (App. Ex. LXXXV, p. 5). The investigators told SGT Mitchell "that the verbal warrant required [SGT Mitchell] to unlock his phone." (R. at 287). The investigators asked SGT Mitchell for his passcode, but SGT Mitchell "refused" to provide it. (R. at 41, 43; App. Ex. LIV, p. 3; App. Ex. LXXXV, p. 4). The investigators asked for SGT Mitchell's passcode multiple times and "told [SGT Mitchell] that it was part of the warrant that he [give] them the password and unlock the phone." (R. at 287; App. Ex. LXXXIII, p. 7). The military judge found that the warrant authorized the seizure of SGT Mitchell's phone, but it did not authorize the agents to seize the passcode needed to access the phone. (App. Ex. LXXXV, p. 4).

According to SSG Vaughn, the investigators “badgered [SGT Mitchell]” multiple times until SGT Mitchell provided the passcode or unlocked his phone. (R. at 275). Ultimately, SGT Mitchell complied with the investigators repeated demands and unlocked his phone for the investigators, but did not inform the investigators of his passcode. (R. at 53, 69-70; App. Ex. LXXXV, pp. 4-5). At the investigators’ insistence, SGT Mitchell disabled the security features on his phone by changing the iPhone’s settings and reentering his passcode. (App. Ex. LXXXIII, p.7; App. Ex. LXXXV, p. 5). The only way to permanently unlock the iPhone is for the accused to access his phone’s settings and enter his passcode “two more times” to fully disable the phone’s protections. (App. Ex. LXXXV, p. 5). If SGT Mitchell had not entered his passcode two more times, the investigators would not have acquired the permanent access needed to perform the digital forensic examination. The military judge found SGT Mitchell was “required” to do this, and such action was not voluntary. (App. Ex. LXXXV, p. 5, n. 5.).

Although the iPhone had a biometric capability, and could be unlocked by submission of the proper fingerprint, SGT Mitchell did not use this feature to unlock the iPhone for the investigators. (App. Ex. LXXXIII, p. 7). Further, the government was unaware the iPhone could be unlocked with the appropriate fingerprint until April 20, 2015, and this was only confirmed by examining the decrypted phone after its security was disabled by SGT Mitchell. (App. Ex. LXXIX, pp. 9-10).

Similarly, the military judge found that while SGT Mitchell was in his commander's office and throughout the following search of his person, car, and barracks room, SGT Mitchell "was not free to leave" and "a reasonable man in the same position would have believed his freedom of action was significantly curtailed – as if to be under arrest." (App. Ex. LXXXV, p. 8).

The military judge also found that INV BT "asked the accused if he could provide the PIN to unlock the phone" since the iPhone was password protected. (App. Ex. LIV, p. 3). She found that INV BT asked SGT Mitchell "if you could unlock it, great, if you could help us out. But if you don't we'll wait for a digital forensic expert to unlock it" or words to that effect. (App. Ex. LXXXV). Additionally, she found "[SGT Mitchell] eventually complied with the nature of [law enforcement's] request by entering his PIN and permanently unlocking the phone." (App. Ex. LIV, p. 4; App. Ex. LXXXV, p. 5). The military judge found that, at the time the investigators asked the accused for his passcode, the investigators did not know and were not aware that SGT Mitchell's phone had biometric capacities. (App. Ex. LXXXV, p. 5). And they did not become aware of these capabilities until April 20, 2015. (App. Ex. LXXXV, p. 4).

The military judge also found that SGT Mitchell "was not provided sufficient time or opportunity to seek counsel" because he was "escorted to and from the military police station and remained either inside or right outside of his company

commander's office until the investigator's reapproached him." (App. Ex. LIV, p. 9). The "1-1 1/2 hour break in custody [was] insufficient to terminate any lingering effect of the prior interrogation" at the police station. (App. Ex. LXXXV, p. 6). "[O]nce the investigator reinitiated 'communications, exchanges, or conversations' about matters more than routinely incident of the custodial relationship, he was in violation of *Edwards* and the accused's Fifth Amendment right to counsel." (App. Ex. LIV, p. 9; App. Ex. LXXXV, p. 7-8).

Summary of Argument

Repeated questioning by police, while SGT Mitchell was in their custody and after he requested to speak with an attorney, violated SGT Mitchell's rights under the Fifth Amendment, *Edwards v. Arizona*, 451 U.S. 477 (1981), and Mil. R. Evid. 305(c)(2). As a result of this illegal questioning, SGT Mitchell made involuntary statements about his possession and control of the iPhone, and performed testimonial acts for police, such as decrypting and unlocking the iPhone at their direction. The military judge did not err in finding the police violated the Fifth Amendment and *Edwards*, and she did not err by suppressing the decrypted iPhone and its contents under Mil. R. Evid. 305(c)(2).

Standard of Review

A military judge's decision to admit or exclude evidence is reviewed for an abuse of discretion. *United States v. Freeman*, 65 M.J. 451, 453 (C.A.A.F.

2008)(citing *United States v. Ayala*, 43 M.J. 296, 298 (C.A.A.F. 1995). This standard of review “recognizes that a judge has a range of choices and will not be reversed so long as the decision remains within that range.” *Freeman*, 65 M.J. at 453 (citations omitted). The abuse of discretion standard requires more “than a mere difference of opinion. The challenged action must be ‘arbitrary, fanciful, clearly unreasonable, or clearly erroneous.’” *United States v. White*, 69 M.J. 236, 239 (C.A.A.F. 2010)(quoting *United States v. Lloyd*, 69 M.J. 95, 99 (C.A.A.F. 2010). “[A]n abuse of discretion occurs when [the military judge’s] findings of fact are clearly erroneous, the court’s decision is influenced by an erroneous view of the law, or the military judge’s decision on the issue at hand is outside the range of choices reasonably arising from the applicable facts and the law.” *United States v. Stellato*, 74 M.J. 473, 480 (C.A.A.F. 2015)(internal citation omitted).

Conclusions of law, such as the trial court’s finding of a violation of the Fifth Amendment, are reviewed de novo. *United States v. Piren*, 74 M.J. 24, 27 (C.A.A.F. 2015)(citation omitted). Significantly, however, when reviewing a ruling on a motion to suppress, this Court considers the evidence in the light most favorable to the prevailing party. *United States v. Baker*, 70 M.J. 283, 287-88 (C.A.A.F. 2011)(quoting *United States v. Cowgill*, 68 M.J. 388, 390 (C.A.A.F. 2010)). Here, SGT Mitchell is the prevailing party at trial and at the intermediate level of appellate review.

This Court is therefore “bound by the military judge’s findings of fact unless they were clearly erroneous.” *United States v. Cossio*, 64 M.J. 254, 256 (C.A.A.F. 2007). “The clearly erroneous standard is a very high one to meet . . . If there is ‘some evidence’ supporting the military judge’s findings [this Court] will not hold them . . . ‘clearly erroneous.’” *United States v. Leedy*, 65 M.J. 208, 213 n. 4 (C.A.A.F. 2007)(citations omitted).

Argument

I. This Court should affirm the military judge’s ruling because her findings of fact are well-supported, her conclusions of law are correct, and suppression is appropriate under *Edwards* and Mil. R. Evid. 305(c)(2).

This Court does not need to reach the questions presented by the first and second certified issues in this case because the issues certified assume facts contrary to the correct findings and conclusions of the military judge. Specifically, the first certified issue assumes that SGT Mitchell “voluntarily” unlocked the iPhone. The military judge, however, found that investigators “required” SGT Mitchell to disable the security on the iPhone, and that such action was not voluntary. (App. Ex. LXXXV, p. 5, n. 5). This finding is more than adequately supported by multiple sources, including testimony that, after SGT Mitchell invoked his right to counsel and was subject to continued custodial interrogation, investigators were “badgering” SGT Mitchell about his iPhone, and investigators told SGT Mitchell he was “required” to unlock the iPhone because of a search warrant. (R. at 279-80,

87; App. Ex. LXXXIII, p. 7). Similarly, the second certified issue states that SGT Mitchell had “returned to his place of duty” at the time of his second interrogation. The military judge, however, found that SGT Mitchell was “not free to leave” his commander’s office, or the presence of the investigators, and “[u]nder the circumstances of this case a reasonable man in the same position would have believed his freedom of action was significantly curtailed – as if to be under arrest.” (App. Ex. LXXXV, p. 8). This finding is more than adequately supported by evidence that SGT Mitchell was told to “report to” and “stay” in his commander’s office, (App. Ex. LXXXIII, p. 7); SGT Mitchell’s commander “signed him over correctly” to the investigators, (R. at 512); and SGT Mitchell was in the presence of two investigators and either his commander, or a senior NCO escort the entire time. (R. at 272-73). Finally, this Court need not address the third certified issue – whether the military judge erred by suppressing the evidence – in great detail as it is conclusively answered in the negative by Mil. R. Evid. 305(c)(2).

This brief shall address each of the government’s arguments in turn, but as a preliminary matter encourages this Court to affirm the court below because the plain language of Mil. R. Evid 305(c)(2), and the repeated *Edwards* violations by police in this case warrant suppression of the decrypted cell phone and its contents.

There are compelling and nuanced arguments for how the Fifth Amendment applies to the testimonial decryption of data and the use of passcodes to “unlock” digital media. This Court need not rely on such arguments in this case, however, because a straightforward application of Mil. R. Evid. 305(c)(2) conclusively supports the order of the military judge suppressing the evidence at issue.

It is undisputed that SGT Mitchell was subjected to custodial interrogation and invoked his right to counsel at 10:50 a.m. on January 8, 2015. (App. Ex. XXXIII; App. Ex. XXXVI). After additional processing in police custody, SGT Mitchell was returned to his unit’s control and escorted back to his company area. Approximately an hour and a half after he left the police station, SGT Mitchell was ordered to report to his company commander’s office. There he was confronted by two police officers, including the investigator to whom he previously asserted his right to counsel. Of this encounter, the military judge found:

When the accused was in the commander’s office prior to [the investigators’] arrival, he was not free to leave, as the commander was aware that investigators needed to serve a search and seizure authorization upon the accused. Although the accused was not physically restrained, he was under moral restraint in the commander’s office and not free to leave until dismissed. Further, the accused was in custody during the execution of the search warrant in the commander’s office, at the vehicle, in his barracks room and at all times in between. The investigators would not have allowed the accused drive away in his vehicle or any by any other means until they completed their search and seizure of the accused and his property.

(App. Ex. LXXXV, p. 8). In these statements, the military judge interweaves findings of fact and conclusions of law; both are correct, and well-supported in the record.

While again in police custody, the investigator to whom SGT Mitchell previously asserted his right to counsel asked if SGT Mitchell had a cell phone. In response, SGT Mitchell produced the iPhone at issue. (R. at 41). Upon realizing that the iPhone was password protected, the same investigator asked SGT Mitchell what his personal identification number or passcode was. SGT Mitchell declined to answer the question, and the police asked SGT Mitchell for the passcode “multiple times.” (R. at 292). After multiple requests by the police, SGT Mitchell, while still in police custody, unlocked the iPhone by entering his passcode, accessing the iPhone’s security settings, changing the phone’s security measures, and entering the passcode again. (App. Ex. LXXXV, p. 5). As a result, the government gained total access to the unencrypted contents of the iPhone.

The investigators’ questions to SGT Mitchell about his passcode clearly sought for SGT Mitchell “to disclose the contents of his own mind,” *Curcio v. United States*, 354 U.S. 118, 128 (1957). Sergeant Mitchell’s eventual capitulation by entering his passcode and changing his iPhone’s settings was a direct consequence of his production of the phone, his initial refusal to provide his passcode, and ongoing interrogation by police. Therefore, the unencrypted iPhone

and its contents were derived from continued custodial interrogation after SGT Mitchell invoked his right to counsel. As such, the iPhone and all contents thereof are inadmissible under Mil. R. Evid. 305(c)(2) as evidence “derived from the interrogation.”

Further, SGT Mitchell entering his passcode, changing the iPhone’s settings, entering his passcode again, and returning the iPhone to the police was a testimonial act. “[I]n order to be testimonial, an accused’s communication must itself, explicitly or implicitly, relate a factual assertion or disclose information.” *Doe v. United States*, 487 U.S. 201, 210 (1988) [hereinafter “*Doe [1988]*”]. Testimonial acts can include such things as: the production of a perfume bottle concealed on an individual’s person, *United States v. Powell*, 40 M.J. 1, 7-8 (C.M.A. 1994); the production of documents, *United States v. Hubbell*, 530 U.S. 27, 45 (2000); and the decryption of digital media. *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335, 1352-53 (11th Cir. 2012) [hereinafter “*Doe [11th Cir.]*”].¹ Sergeant Mitchell’s production of his iPhone

¹ As of the writing of this brief, *Doe [11th Cir.]* is the only United States Circuit Court of Appeals opinion the undersigned appellate defense counsel have found that squarely address this issue of whether compelled decryption or passcode production is testimonial and therefore protected by the Fifth Amendment. Various other courts have reached similar results. *See, e.g., United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich., 2010)(passcode production); *SEC Civil Action v. Huang*, 2015 U.S. Dist. LEXIS 127853 (E.D. Pa., Sep. 23, 2015)(unpublished opinion)(passcode production); *State v. Trant*, 2015 Me. Super.

when asked if he had a cell phone was a testimonial act just like the production of the perfume bottle in *Powell*. This act indicated to investigators that SGT Mitchell was in possession of the iPhone and that he knew he was in possession of the iPhone. After police asked him for the passcode to the iPhone, SGT Mitchell's refusal to answer the question and disclose his passcode was a statement that implicitly admitted that he knew the passcode, and explicitly asserted he would not divulge it. When the police continued to question SGT Mitchell about the passcode, his eventual capitulation was another testimonial act because it explicitly admitted that SGT Mitchell knew the passcode to the iPhone, which implicitly suggested: (1) the iPhone was password-protected; (2) without the password the iPhone could not be used; (3) SGT Mitchell created the password; (4) SGT Mitchell was the only person who could use the iPhone; and (5) SGT Mitchell was the person responsible for anything done with the phone. This testimonial act is similar to both the classic "combination lock" hypothetical, and the compilation of data at issue in *Hubbell*. See *Hubbell*, 530 U.S. at 43, 45. The similarity to the compilation of data in *Hubbell* is reinforced by the fact that SGT Mitchell had to do more than simply type his passcode into the iPhone in order to unlock it, he also

LEXIS 272 (Super. Ct. Me., Oct. 27, 2015)(unpublished opinion)(decryption of an iPhone 6). But see, e.g., *United States v. Fricosu*, 841 F. Supp. 2d 1364 (S.D. Fl. 2012); *Commonwealth v. Gelfgatt*, 468 Mass. 512 (2014); *In re Grand Jury Subpoena (Boucher)*, 2009 U.S. Dist. LEXIS 13006 (D. Vt., Feb 19, 2009)(unpublished opinion).

had to change the iPhone's internal settings and enter his passcode again, necessitating extensive use of his own personal knowledge of how the device worked. The decryption of encrypted information was also found to be testimonial by the Eleventh Circuit in *Doe* [11th Cir.], as discussed in more detail later in this brief.

For these reasons, SGT Mitchell suffered not one *Edwards* violation, but several successive *Edwards* violations, each successive violation derivative of its predecessor. This Court should affirm the court below based on the investigators' repeated violations of the Fifth Amendment, the *Edwards* rule, and Mil. R. Evid. 305(c)(2).

This brief shall now address the arguments of the government, in turn.

A. Sergeant Mitchell did not voluntarily unlock his iPhone.

Statements made in response to questioning that violates the rule in *Edwards* are presumed to be involuntary. *Maryland v. Shatzer*, 559 U.S. 98, 100, 105 (2009). This presumption holds unless: (1) at least two weeks have lapsed since the suspect invoked his or her right to counsel, *id.* at 110; (2) the suspect reinitiated communication with police, *Edwards*, 451 U.S. at 484-85; or (3) the suspect has an attorney present. *Id.* None of the exceptions to the well-settled rule in *Edwards* applies in this case.

The military judge correctly found that SGT Mitchell was “required to disable the cell phone’s passcode protection” and such act was not voluntary. (App. Ex. LXXXV, p. 5, n. 5). The military judge’s findings in this regard are not erroneous considering the surrounding circumstances: the initial custodial interrogation; SGT Mitchell’s commander again “signed him over” to police in his office; the police disregarded SGT Mitchell’s invocation of his rights; and police “badgering” SGT Mitchell for his passcode and stating it was “required by the warrant.” The totality of this evidence supports the military judge’s findings, which are not erroneous, but in fact are correct.

B. Sergeant Mitchell made a testimonial act by unlocking his cell phone.

An act of production is testimonial if it implicitly conveys incriminating statements of fact, such as the existence, possession, control, or authenticity of documents. *Hubbell*, 530 U.S. at 36. One of the touchstones of whether an act is testimonial is whether it requires an individual to use “the contents of his own mind.” *Doe [11th Cir.]*, 670 F.3d at 1345 (citing *Curcio*, 354 U.S. at 128).

Whether an act is testimonial in nature is highly fact-specific and should not be overturned unless the factual findings of the trial court are clearly erroneous. *See United States v. Doe*, 465 U.S. 605, 613-14 (1984) [hereinafter “*Doe [1984]*.”]

1. Sergeant Mitchell's entry of his PIN and production of the decrypted contents of his iPhone was testimonial

In this case, the military judge determined that “[t]he remembering, recalling and entering a password is not a simple physical act. Such remembering, recalling and entering the password requires the use of the contents of the accused’s mind and is testimonial in nature.” (App Ex. LIV p. 8). The military judge later elaborated that: “The accused entered his numeric passcode (PIN) to unlock the phone. The accused was also required to permanently disable the cell phone’s passcode protection. In order to do so, the accused was required to access the phone’s settings and enter his numeric passcode (PIN) two more times to fully disable the phone’s protections.” (App. Ex. LXXXV, p. 5). By performing this sequence of actions at the behest of investigators, SGT Mitchell was compelled to use the contents of his own mind in a manner that implicitly conveyed numerous incriminating statements of fact.

While the government attempts to draw an artificial distinction between SGT Mitchell entering his passcode into his iPhone, and his production of the unencrypted contents of his phone for investigators, these testimonial acts are inextricably intertwined in the facts of this particular case. As the military judge explains, investigators first asked SGT Mitchell if he had a cell phone, next they asked for the passcode to his cell phone, next they negotiated for him to unlock the cell phone instead of giving them the passcode; SGT Mitchell then followed the

procedure as explained by the military judge for unencrypting and permanently unlocking the phone. This sequence of statements and acts by SGT Mitchell, all in response to custodial interrogation, implicitly and explicitly conveyed numerous incriminating facts. These facts include: (1) Sergeant Mitchell owned an iPhone; (2) the iPhone was encrypted; (3) because it was encrypted, individuals who did not know the Passcode could not access the iPhone; (4) SGT Mitchell knew the passcode; (5) SGT Mitchell could access the iPhone; (6) SGT Mitchell would not tell the passcode to other individuals; (7) SGT Mitchell knew how to change the security settings on the iPhone; and finally, (8) the iPhone contained certain files. These implicit and explicit statements amounted to admission of the existence, authenticity and SGT Mitchell's control of his iPhone and all its contents. The implicit statements inherent in his acts also indicate that SGT Mitchell, and only SGT Mitchell could access the iPhone, and that he had a good working knowledge of it and its contents.

The acts described above required SGT Mitchell to make extensive use of the contents of his own mind because access to the phone required SGT Mitchell's passcode, which existed exclusively in SGT Mitchell's mind. Similarly, SGT Mitchell's familiarity with his phone allowed him to change the security settings, as he did at the insistence of investigators, in a way that someone unfamiliar with the settings of that model of an iPhone likely could not. Further, even changing the

security settings required use of SGT Mitchell's passcode twice more. Thus, decrypting and permanently unlocking the iPhone was impossible without accessing and utilizing information only available in SGT Mitchell's mind.

2. The "foregone conclusion" exception does not apply.

The "foregone conclusion" exception to the exclusionary rule was established in the context of whether an individual's production of certain documents, created by his accountant, violated that individual's right against self-incrimination. *Fisher*, 425 U.S. at 394-95. The Supreme Court determined it did not under the facts of that case because although the act of production may have been testimonial, the government was otherwise aware of the existence, possession, control and authenticity of the documents at issue. *Id.* at 411. Later, the Supreme Court explained the same rationale is not applicable to situations where the government seeks a general class of documents without specific knowledge of individual documents. *Hubbell*, 530 U.S. at 44-45.

The "foregone conclusion" exception to the exclusionary rule for the compelled production of documents does not apply to the evidence in this case for three reasons: First, this Court should decline to extend the "foregone conclusion" exception to evidence obtained through *Edwards* violations. Second, whether government knowledge of the contents of SGT Mitchell's cell phone is a "foregone conclusion" is a factual determination and the military judge's findings to the

contrary are well-supported. Third, under any standard of review, the “foregone conclusion” exception does not apply to the evidence at issue in this case.

(a) This Court should decline to extend the “foregone conclusion” exception to evidence obtained in violation of the Edwards rule.

As discussed above, the “foregone conclusion” exception was developed in the context of grand jury subpoenas and summonses for document production. *See, e.g., Fisher, supra; Hubbell, supra; Doe [11th Cir.], supra.* Indeed, the exception is suited to the context of a judicial or quasi-judicial order of production, where there is an appropriate remedy immediately available in the form of a motion to quash. In such cases, the entire process can be carefully shepherded by the courts. This case is different. This case involves a flagrant and repeated violation of the *Edwards* rule by law enforcement in the field. Unlike those cases involving a grand jury subpoena, SGT Mitchell did not have immediate recourse to the courts when he was being held in police custody and interrogated by investigators who ignored his request for legal counsel.

The policy concerns in ensuring summonses, subpoenas, and judicial orders are appropriately tailored are different than the policy concerns in preventing police interrogation that persists in the face of a suspect’s unambiguous request for legal representation. As the Ninth Circuit has explained: “The application of privilege to a document production is different from a blanket privilege claim at an interview. An unscripted interview is undefined, so a court cannot make a

reasoned assessment of privilege before particular questions have been posed.”

United States v. Bright, 596 F.3d 683, 691 (9th Cir. 2010)(explaining why a blanket privilege was unavailable in response to an IRS summons). For this reason, this Court should decline to extend the “foregone conclusion” exception to evidence gained through *Edwards* violations.

(b) This Court should not disturb the military judge’s finding that the foregone conclusion exception does not apply unless it is clearly erroneous.

The Supreme Court has noted that whether an act of production is testimonial, to include whether the foregone conclusion exception applies, is an inherently factual issue. *See Doe [1984]*, 465 U.S. at 613-14. The Eighth and Ninth Circuit Courts of Appeals therefore hold that whether the government’s knowledge of the evidence sought is a foregone conclusion – and therefore whether the exception applies – is a question of fact to be found by the trial court. *United States v. Norwood*, 420 F.3d 888, 895 (8th Cir. 2005) (citing *Doe [1984]*), *Bright*, 596 F.3d at 690 (citing *Norwood*). Therefore, those circuits review such findings for “clear error.” *Id.*

This Court should adopt the same principle: Whether the facts conveyed in response to a Fifth Amendment violation are already known to the government is a question of fact. As such, this Court should defer to the findings of the military judge, and reverse only if her findings are clearly erroneous.

The military judge in this case correctly noted that it is the government's burden to prove prior knowledge of the facts conveyed by SGT Mitchell's otherwise testimonial acts. (App. Ex. LIV, p. 9); *Doe [1984]*, 465 U.S. at n.13. The military judge then found the Government had failed to carry that burden and it could not show that it had actual knowledge of the existence, possession, control, and authenticity of the evidence in question. (App. Ex. LIV, pp. 9-10). This finding is well-supported by the evidence, and should not be disturbed.

(c) The existence, possession, control, and authenticity of the iPhone and its contents were not a foregone conclusion.

As discussed above, the “foregone conclusion” exception may allow the government to compel the production of documents, even when such production would otherwise be testimonial, in the limited circumstance where the government is already aware of the existence, possession, control and authenticity of the documents in question. *See Fisher*, 425 U.S. at 394-95, 411. This exception does not, however, apply to the production of a general class of documents. *See, e.g., Hubbell, supra*. It is also not enough that the government has reasonable grounds to suspect that an individual will have certain records. *United States v. Ponds*, 454 F.3d 313, 325-26 (D.C. Cir. 2006)(holding that government knowledge that a car was normally parked at Ponds' apartment did not show the government knew of the existence, possession, or control of any documents relating to the car that might be in Ponds' possession).

When the government does not know of the existence, possession, control, and authenticity of specific files or documents prior to obtaining them, the foregone conclusion exception does not apply. *Hubbell*, 530 U.S. at 44-45. Mere suspicion that certain evidence exists is not sufficient to establish the “foregone conclusion” exception. *Doe [11th Cir.]*, 670 F.3d at 1346 (citing *Hubbell*).

Here, the government suspected that SGT Mitchell had been communicating with his wife in violation of a no-contact order. (App. Ex. XXXVI). Because the communications did not come from a number that SGT Mitchell was known to possess, the investigators suspected that he was using a prepaid phone. (App. Ex. XII, p. 85). Thus, the government obtained a broad warrant to search SGT Mitchell’s person, automobile, and barracks room for “cell phone devices, laptops, hard drives, any electronic devices capable of placing a phone call, SIM cards, and electronic tablets” for evidence of communication or the ability to disguise the source of communications. (App. Ex XII, p. 87). The broad scope of the search authorization, seeking to find some communications media used by SGT Mitchell but unknown to his wife, reflects the fact that the government did not have knowledge of what, if any, devices SGT Mitchell might have, and the government certainly did not have knowledge with sufficient particularity to satisfy the “foregone conclusion” exception.

The government's contention that probable cause to search for communications devices concurrently satisfies the foregone conclusion exception with regard to the possession of any particular device not previously known to the government, and indeed to the contents of that device, is a proposition that would wholly swallow the Fifth Amendment within the test for probable cause.² This would be contrary to the narrow exception as set forth by the Supreme Court, and as interpreted by the Circuit Courts of Appeals. *See, e.g. Ponds*, 454 F.3d at 325-26 (the facts describe better than probable cause to believe Ponds would have documents relating to the car normally parked outside his apartment); *Doe [11th Cir.]*, 670 F.3d at 1339 (a warrant based on probable cause was issued to search the relevant digital media for child pornography); *Bright*, 596 F.3d at 693-94 (the facts describe probable cause to believe that the Brights possessed the two additional credit cards that did not meet the foregone conclusion exception). Thus, the existence of probable cause to search for certain evidence does not mean that the government's knowledge of the existence, possession, control, and authenticity of that evidence is a foregone conclusion. The government never articulated better than a reasonable suspicion that SGT Mitchell's iPhone might contain any evidence prior to the *Edwards* violation at issue in this case. In fact, the police

² This also highlights why the foregone conclusion exception is ill-suited to *Edwards* violations, or other violations related to custodial interrogation, as discussed above.

never demonstrated that the iPhone was a prepaid phone. Sergeant Mitchell was, however, in possession of a different phone, a “Kyocera” that was prepaid. (R. at 72). Thus, there was little if any link between the evidence police suspected SGT Mitchell had somewhere in his possession, and the iPhone now at issue. For these reasons, and for the reasons discussed above, the “foregone conclusion” exception is inapplicable on the facts of this case.

C. The military judge’s remedy was appropriate.

The language of the Military Rules of Evidence is clear and unambiguous: “If a person suspected of an offense and subjected to custodial interrogation requests counsel, any statement made in the interrogation after such request, or evidence derived from the interrogation after such request, is inadmissible against the accused unless counsel was present for the interrogation.” Mil. R. Evid. 305(c)(2). The unlocked, decrypted iPhone, and all the contents thereof are evidence derived from the interrogation of SGT Mitchell, which was conducted after he requested counsel. As such, suppression of this evidence is not only appropriate, but required.

1. Suppression of the physical iPhone was appropriate.

After SGT Edwards invoked his right to counsel, and while he was in police custody, investigators asked him whether he had any cell phones. He responded by producing his iPhone. This, in itself, was a testimonial act. *See Powell*, 40 M.J. at

7-8. For this reason alone it was within the military judge's discretion to suppress the physical iPhone, but this is not the only reason. Once SGT Mitchell unlocked his iPhone, changing its settings so that its decrypted contents are accessible to investigators, it became evidence derived from his post-invocation interrogation in a manner additional to, and independent of, his production of the phone. The iPhone's interface can now be used to access all its decrypted, and potentially incriminating contents. For this reason the physical phone should not be introduced into evidence and provided to a fact-finder at trial. If the iPhone itself is introduced into evidence in its unlocked state, by necessity all its decrypted contents are also introduced into evidence. For this reason, suppression of the physical iPhone is within the discretion of the military judge, and is required by Mil. R. Evid. 305(c)(2).

2. Suppression of the iPhone's contents was appropriate.

Had the investigators not asked SGT Mitchell if he had a cell phone, or if they had not asked him repeatedly for the passcode to his cell phone, he would not have decrypted and permanently unlocked the iPhone for investigators and its contents would not be accessible. For this reason alone, a straightforward application of Mil. R. Evid. 305(c)(2) requires suppression of the contents of the iPhone. This application of Mil. R. Evid. 305(c)(2) is reinforced by the discussion

above regarding the testimonial nature of SGT Mitchell's actions in entering his passcode, changing the phone's setting, and entering his passcode twice more.

The government's argument that the contents of the iPhone can be meaningfully distinguished from SGT Mitchell's decryption and unlocking of the phone does not avail. Even if the decrypted contents of the iPhone are characterized as evidence merely derivative of SGT Mitchell's involuntary decryption and unlocking of his phone, the contents are still inadmissible under both Mil. R. Evid. 305(c)(2) and the Fifth Amendment. The Supreme Court has held that immunity for compelled testimony must include immunity from both direct and derivative use in order to be coextensive with the protections of the privilege against self-incrimination. *Kastigar v. United States*, 406 U.S. 441, 453 (1972). "Supreme Court precedent is clear: Use and derivative use immunity establishes the critical threshold to overcome an individual's invocation of the Fifth Amendment privilege against self-incrimination. No more protection is necessary; no less protection is sufficient." *Doe [11th Cir.]*, 670 F.3d at 1351 (citing *Kastigar*, 406 U.S. at 460). Put another way, the right against self-incrimination "not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." *Hoffman v. United States*, 341 U.S. 479, 486 (1951). Therefore, it is appropriate to

suppress both direct and derivative evidence stemming from SGT Mitchell's involuntary statements made after police disregarded his invocation of his Fifth Amendment rights. This is a straightforward application of *Edwards* and the Fifth Amendment, and under Mil. R. Evid 305(c)(2).

II. The investigators in this case violated the *Edwards* rule.

An accused once “having expressed his desire to deal with the police only through counsel, is not subject to further interrogation by the authorities until counsel has been made available to him, unless the accused himself initiates further communication, exchanges, or conversations with the police.” *Edwards*, 451 U.S. at 484-85. The *Edwards* rule applies to custodial interrogation. *Id.* When in custody, “all questioning must cease after an accused requests counsel.” *Smith v. Illinois*, 469 U.S. 91, 98 (1984)(emphasis original). This includes law enforcement reinitiating communication in order to ask for consent to search the belongings of the individual who requested counsel. *United States v. Hutchins* 72 M.J. 294, 299-300 (C.A.A.F. 2013).

Because the fact that SGT Mitchell unambiguously invoked his right to counsel is not in dispute, the remaining issues are whether SGT Mitchell was subsequently in custody, and if so, whether he was subjected to further interrogation while in custody. The answer to both issues is “yes.”

A. Sergeant Mitchell was in custody when the investigators asked him multiple questions about his iPhone.

The Supreme Court has explained the test for whether an individual is in custody as follows: “Two discrete inquiries are essential to the determination: first, what were the circumstances surrounding the interrogation; and second, given those circumstances, would a reasonable person have felt he or she was at liberty to terminate the interrogation and leave.” *Thompson v. Keohane*, 516 U.S. 99, 112 (1995)(internal quotations and footnotes omitted).

This Court has outlined five non-exclusive factors to consider in determining whether a reasonable person would have considered himself or herself free to leave in the context of the surrounding circumstances: (1) whether the person appeared for questioning voluntarily; (2) the location and atmosphere of the place in which questioning occurred; (3) the length of the questioning; (4) the number of law enforcement officers present at the scene; and (5) the degree of physical restraint placed upon the accused. *United States v. Chatfield*, 67 M.J. 432, 438 (C.A.A.F. 2009).

The Military Rules of Evidence define custodial interrogation as “questioning that takes place while the accused or suspect is in custody, could reasonably believe himself or herself to be in custody, or is otherwise deprived of his or her freedom of action in any significant way.” Mil. R. Evid. 305(b)(3).

The government does not appear to challenge the military judge's finding that SGT Mitchell was in police custody when military police decided to "bring in Mr. Mitchell." (R. at 202). Sergeant Mitchell was escorted to the military police station, (R. at 61), taken to an interrogation room, (R. at 61), and read his rights with a DA Form 3881. (R. at 61; App. Ex. XXXVI). Therefore it is sufficient to note that the aforementioned evidence more than adequately supports the military judge's finding that SGT Mitchell was in custody when he invoked his right to counsel. (App. Ex. LIV, pp. 2, 6).

After invoking his right to counsel while in custody at the police station, SGT Mitchell was escorted back to his unit by the same superior NCO who escorted him to the police station. (R. at 216). Shortly thereafter, however, military police contacted SGT Mitchell's commander and told him they needed to execute a search authorization on SGT Mitchell. (R. at 508). Sergeant Mitchell was ordered into the office of his commander to wait for the military police to arrive, and kept there until the police arrived. (R. at 509, 512). Sergeant Mitchell's commander then "signed him over" to the investigators. (R. at 512).

Inside his commander's office, the investigators asked SGT Mitchell if he had any cell phones. (R. at 41, 68-69). After some discussion, SGT Mitchell produced his iPhone and handed it to the investigators. (R. at 69). The lead investigator then noticed that the iPhone was locked and asked SGT Mitchell for

the passcode to unlock it. (R. at 43, 69). Sergeant Mitchell declined to produce the passcode for investigators. (R. at 43, 69). The investigators asked SGT Mitchell for his passcode, or to unlock the iPhone, “quite a few times.” (R. at 257). After repeated requests by the investigators, SGT Mitchell eventually unlocked the iPhone. (R. at 257-261).

Under the facts of this case, the military judge’s finding that SGT Mitchell was not free to leave his commander’s office is well-supported. “Under the circumstances of this case, a reasonable man in the same position would have believed his freedom of action was significantly curtailed – as if to be under arrest.” (App. Ex. LXXXV, p. 8).

Applying the non-exclusive *Chatfield* factors to this case: SGT Mitchell did not appear for questioning voluntarily, rather he was ordered to appear, first to the police station, then to his commander’s office. Sergeant Mitchell was ordered to his commander’s office for the purpose of the police asking him questions and executing a search authorization. Further, a senior NCO escort was used to ensure SGT Mitchell’s compliance with orders. Under these circumstances, the location and atmosphere of the questioning was highly coercive. Throughout the interrogation SGT Mitchell was confronted by two investigators, one of whom had apprehended him barely one and one half hours before. SGT Mitchell was also in the presence of a senior NCO escort, and at least at the beginning of the interview

by his commander who “signed him over” to the investigators. Although SGT Mitchell was not placed in handcuffs during this interrogation, the military judge observed that “he was under moral restraint in the commander’s office and not free to leave until dismissed.” (App. Ex. LXXXV, p. 8).

Finally, it is worth noting that the *Chatfield* factors are non-exclusive and such determinations are highly fact-specific. The fact that SGT Mitchell was apprehended and questioned by police barely one and a half hours before being ordered to meet the police in his commander’s office is one of the many nuances the military judge considered in reaching her findings. These findings are supported by the record, and not clearly erroneous. Sergeant Mitchell was in custody when investigators re-initiated questioning. Further, he “could reasonably believe [himself] to be in custody,” and was “otherwise deprived of [his] freedom of action in [a] significant way.” Mil. R. Evid. 305(b)(3). For these reasons, the military judge correctly found that SGT Mitchell was subjected to renewed custodial interrogation.

B. The investigators further interrogated SGT Mitchell after he invoked his right to counsel and while he was in custody.

“‘Interrogation’ means any formal or informal questioning in which an incriminating response either is sought or is a reasonable consequence of such questioning.” Mil. R. Evid. 305(b)(2). Put another way, “interrogation” “refers not only to express questioning, but also to any words or actions on the part of the

police (other than those normally attendant to arrest and custody) that the police should know are reasonably likely to elicit an incriminating response from the suspect.” *Rhode Island v. Innis*, 446 U.S. 291, 301 (U.S. 1980).

Investigators’ repeated questions regarding whether SGT Mitchell had a cell phone, what the passcode was to his cell phone, and whether he would decrypt and unlock his cell phone were likely to elicit an incriminating response, and in fact did elicit incriminating responses. The military judge explicitly found that “the investigator, a person subject to the code, was requesting the accused to divulge through his mental process, his iPhone PIN or passcode - evidence that would incriminate him.” (App. Ex. LIV, p. 8).

While the government attempts to argue the military judge used the wrong standard in reaching her conclusion of law that SGT Mitchell was subjected to an interrogation when the investigators asked for his phone and then repeatedly asked for his passcode or for him to unlock his phone, the military judge cites directly to M.R.E. 305(b)(3) and the Supreme Court standard in *Innis* immediately before concluding that SGT Mitchell was subjected to renewed custodial interrogation. (App. Ex. LXXXV, pp. 8-9). These are the correct standards to apply and the military judge applied them correctly.

Further, as discussed above, the military judge considered evidence that the investigators were indeed “badgering” SGT Mitchell about his phone, and that

SGT Mitchell was told that unlocking the phone was “required” by the warrant. (R. at 279-80, 87; App. Ex. LXXXIII, p. 7). Thus, there was a sound basis in the evidence before the court for the military judge to conclude that SGT Mitchell was “required” to disable the security on the iPhone, and such action was not voluntary under the circumstances. (App. Ex. LXXXV, p. 5).

III. The military judge did not abuse her discretion by suppressing the iPhone and its decrypted contents.

The military judge did not abuse her discretion by suppressing the iPhone and its decrypted contents because the plain language of Mil. R. Evid. 305(c)(2) is clear and does not yield an absurd result. Further, the government’s reliance on *United States v. Patane*, 542 U.S. 630 (2004), is misplaced. Finally, the doctrine of inevitable discovery is inapplicable to the facts of this case.

A. The exclusionary rule is appropriately applied to derivative evidence of an involuntary statement.

It is a basic tenant of interpreting statutes and rules that the “plain language will control, unless use of the plain language would lead to an absurd result.” *United States v. Lewis*, 65 M.J. 85, 88 (C.A.A.F. 2007). This principle is equally applicable to the Military Rules of Evidence. *See United States v. McNutt*, 62 M.J. 16, 20 (C.A.A.F. 2005).

The Military Rules of Evidence are clear and unambiguous: “If a person suspected of an offense and subjected to custodial interrogation requests counsel,

any statement made in the interrogation after such request, or evidence derived from the interrogation after such request, is inadmissible against the accused unless counsel was present for the interrogation.” Mil. R. Evid. 305(c)(2).

The Military Rules of Evidence explicitly state: “An individual may claim the most favorable privilege provided by the Fifth Amendment to the United States Constitution, Article 31, *or these rules*.” Mil. R. Evid. 301(a)(emphasis added).

The government argues that the plain language of the Rule is not controlling, and urges this Court to look instead to the Military Rules of Evidence prior to the 2013 restyling by Exec. Order 13643 of May 15, 2013, 78 Fed. Reg. 29559 (May 21, 2013). (Appellant’s Br. pp. 50-51). The prior Rules do not, however, yield a substantially different result. The prior Mil. R. Evid. 305(e) prohibited continued custodial interrogation of a suspect after he invoked his right to counsel. *Manual for Courts Martial*, p. III-7 (2008 Ed.) [hereinafter *MCM 2008*]. Prior Mil. R. Evid. 305(a), states: “A statement obtained in violation of this rule is involuntary and shall be treated under Mil. R. Evid. 304.” *MCM 2008*, p. III-6. Prior Mil. R. Evid. 304(a) states, “an involuntary statement or any derivative evidence therefrom may not be received in evidence against an accused who made the statement. . . .” *MCM 2008*, p. III-4. While there are exceptions to this general rule, they do not apply under the facts of this case. The prior Mil R. Evid. 304(b)(3) permitted the introduction of evidence if the military judge finds that the statement was made

voluntarily, that the evidence was not obtained by use of the involuntary statement, or that the evidence would have been obtained even if the involuntary statement had not been made. *MCM 2008*, p. III-4-5. The first of these exceptions does not apply because the statements and testimonial acts in this case were indeed involuntary. The second exception does not apply because the only way to access the content of the iPhone was through the involuntary testimonial acts of SGT Mitchell. Similarly, the third exception does not apply because, but for the involuntary testimonial acts of SGT Mitchell, the contents of the iPhone would remain an enigma.

Nevertheless, while the prior version of Mil. R. Evid. 304 and 305 would yield the same result, it is a fruitless exercise to contest the outcome of this case based on the Rule the government wants and not the Rule this Court has before it when the language of the Rule is clear and the result is not absurd.

Moreover, the government argument depends on a misapprehension on the authority of the Military Rules of Evidence, which in Section III are indeed a codification of the law of search and seizure, but which also carry independent authority as Executive Orders. *See, e.g.*, Exec. Order 13643 of May 15, 2013, 78 Fed. Reg. 29559 (May 21, 2013) (implementing the Military Rules of Evidence now before this Court). Further reinforcing this point, the Rules explicitly direct

that in individual may claim the “most favorable privilege” as between the Fifth Amendment, Article 31, and the Military Rules of Evidence. Mil. R. Evid. 301(a).

Similarly, the government’s reliance on *Patane* is misplaced. *Patane* is a plurality decision that deals with a nominal failure to read a suspect his *Miranda* rights where the suspect interrupted the reading to assert he already knew his rights. *Id.* at 635. The leading opinion, in which three justices join, states that the statements at issue in the case were voluntary, and therefore the fruit of the poisonous tree doctrine did not apply. *Id.* at 636. Unlike the situation in *Patane*, however, this case involves a violation of the *Edwards* rule, and not merely the warning requirement of *Miranda*. Unlike the suspect in *Patane*, SGT Mitchell explicitly invoked his Fifth Amendment rights, and that invocation was ultimately disregarded by police. Thus, SGT Mitchell’s subsequent statements are presumed to be involuntary. *Shatzer*, 559 U.S. at 100, 105. The government failed to rebut that presumption, and the military judge correctly found that SGT Mitchell’s statements and act were, in fact, involuntary. (App. Ex. LXXXV, pp. 5).³ Thus, *Patane* is inapplicable insofar as it relates to *Miranda* warnings and not to statements made involuntary due to police conduct.

³ Finding 25 finds that SGT Mitchell was *required* to disable the iPhone’s security. In a footnote, the military judge explains how this was not a voluntary act.

While *Patane* may be a red herring insofar as it is focused on voluntary statements taken in nominal violation of *Miranda*, it is still relevant to this case in that it reaffirms the longstanding rule that the Fifth Amendment protects individuals from “the use of their involuntary statements (or evidence derived from their statements)” at trial. *Patane*, 542 U.S. at 640 (quoting *Chavez v. Martinez*, 538 U.S. 760, 769 (2003)(plurality opinion)). As discussed previously, the military judge found that SGT Mitchel did not voluntarily disable the security on the iPhone, but rather was “required” to do so. (App. Ex. LXXXV, p. 5, n. 5).

B. The doctrine of inevitable discovery is inapplicable to this case.

The inevitable discovery exception applies only if: “when the illegality occurred, the government agents possessed, or were actively pursuing, evidence or leads that would have inevitably led to the discovery of the evidence and that the evidence would inevitably have been discovered in a lawful manner had not the illegality occurred.” *United States v. Kozak*, 12 M.J. 389, 394 (C.M.A. 1982). The government bears the burden of proof to establish, by a preponderance of the evidence, that the inevitable discovery exception applies. *United States v. Wicks*, 73 M.J. 93, 103 (C.A.A.F. 2014). The military judge correctly stated and applied this standard in her ruling. (App. Ex. LIV, p. 9).

Here, the government simply did not meet its burden, nor could it. As the military judge found, the government was unaware that the iPhone in question

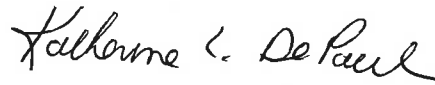
could be accessed through fingerprints until April 20, 2015. (App. Ex. LXXXV, p. 4). The illegal custodial interrogation of SGT Mitchell took place on January 8, 2015. Further, law enforcement had to access the settings of the iPhone in order to verify whether fingerprint access was enabled, and did not do so until April 20. (App. Ex. LXXIX, pp. 9-10). Therefore, the government could not have verified that accessing the iPhone through legal means was possible had it not already obtained illegal access. This, coupled with the fact the government did not even check for fingerprint accessibility until over three months after it violated SGT Mitchell's rights, explains the military judge's statement: "This court is not going to engage in 'mere speculation and conjecture' as to the inevitable discovery of the evidence and the government did not provide more than that." (App. Ex. LIV, p. 9)(quoting *United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996)).

Conclusion

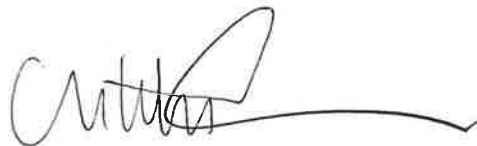
WHEREFORE, the appellant respectfully requests that this Honorable Court affirm the ruling below.



JOSHUA B. FIX
Captain, Judge Advocate
Appellate Defense Counsel
9275 Gunston Road
Fort Belvoir, Virginia 22060-5546
(703) 693-0658
USCAAF No. 36775



KATHERINE L. DEPAUL
Captain, Judge Advocate
Acting Branch Chief,
Defense Appellate Division
USCAAF Bar No. 36536



CHRISTOPHER D. CARRIER
Lieutenant Colonel, Judge Advocate
Chief, Capital and
Complex Litigation Branch
USCAAF Bar Number 32172

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

1. This brief complies with the type-volume limitation of Rules 24(c) because it contains 9,399 words.
2. This brief complies with the typeface and type style requirements of Rule 37 because it has been prepared in Times New Roman font, using 14-point type with one-inch margins.

A handwritten signature in black ink, appearing to read 'J B Fix', with a stylized, cursive script.

JOSHUA B. FIX
Captain, Judge Advocate
Appellate Defense Counsel
9275 Gunston Road
Fort Belvoir, Virginia 22060-5546
(703) 693-0658
USCAAF No. 36775

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing in the case of *United States v. Mitchell*, Army. Dkt. No. 20150776, USCA Dkt. No. 17-0153/AR, was electronically filed with the Court and Government Appellate Division on January 18, 2017.

A handwritten signature in black ink, appearing to read 'J B Fix', with a stylized flourish at the end.

JOSHUA B. FIX
Captain, Judge Advocate
Appellate Defense Counsel
9275 Gunston Road
Fort Belvoir, Virginia 22060-5546
(703) 693-0658
USCAAF No. 36775

APPENDIX

SEC Civil Action v. Huang

United States District Court for the Eastern District of Pennsylvania

September 23, 2015, Decided; September 23, 2015, Filed

NO. 15-269

Reporter

2015 U.S. Dist. LEXIS 127853 *

SECURITIES AND EXCHANGE COMMISSION CIVIL ACTION v. BONAN HUANG, et al.

Subsequent History: Judgment entered by SEC v. Nan Huang, 2016 U.S. Dist. LEXIS 22903 (E.D. Pa., Feb. 25, 2016)

Motion denied by SEC v. Huang, 2016 U.S. Dist. LEXIS 60832 (E.D. Pa., May 9, 2016)

Counsel: [*1] For SECURITIES AND EXCHANGE COMMISSION, Plaintiff: DAVID L. AXELROD, LEAD ATTORNEY, SECURITIES AND EXCHANGE COMMISSION, PHILADELPHIA, PA; CHRISTOPHER REYNOLDS KELLY, G. JEFFREY BOUJOUKOS, U.S. SECURITIES & EXCHANGE COMMISSION, PHILA REGIONAL OFFICE, PHILADELPHIA, PA.

For BONAN HUANG, NAN HUANG, Defendant: GREGORY MORVILLO, LEAD ATTORNEY, PRO HAC VICE, MORVILLO LLP, NEW YORK, NY; EUGENE INGOGLIA, JASON SOMENSATTO, PRO HAC VICE, MORVILLO LLP, NEW YORK, NY; MARK BILLION, LEAD ATTORNEY, BILLION LAW, PHILADELPHIA, PA.

Judges: KEARNEY, J.

Opinion by: KEARNEY

Opinion

OPINION

KEARNEY, J.

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 [*2] ("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. 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

¹ To date, the SEC has not answered Defendants' request as to whether there is any ongoing criminal investigation. Defendants, [*3] presently residing in the Far East, are evaluating possible criminal prosecution for the same conduct.

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, 94 S. Ct. 2179, 40 L. Ed. 2d 678 (1974); *Braswell v. United States*, 487 U.S. 99, 108 S. Ct. 2284, 101 L. Ed. 2d 98 (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. [*4] 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 [*5] Supreme Court. In *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 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, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000)). Accordingly, the [*6] 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

²Unlike 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.

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 phone rather than what they have requested, which are [*7] 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 1345-46. Thus, "where the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available." *Id.* at 1344.

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 [*8] purloined corporate documents is obviously not within the scope of the *Braswell* rule."), with *In re Grand Jury Subpoena 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).

The SEC argues any incriminating testimonial aspect to Defendants' production of the 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 [*9] 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, [*10] 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 U.S. Dist. LEXIS 13006, 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 U.S. Dist. LEXIS 13006, 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" [*11] the existence or location of the documents it seeks. Accordingly, the SEC's motion to compel the passcodes is denied.

ORDER

AND NOW, this 23rd day of September 2015, upon consideration of Plaintiff's Motion to Compel (ECF Doc. No. 36), Defendants' Response (ECF Doc. No. 43), Plaintiff's Reply (ECF Doc. No. 45), after a telephone conference with all counsel, in accord with our September 2, 2015 Order (ECF Doc, No. 40), and for the reasons in the accompanying Opinion, it is **ORDERED** Plaintiff's Motion to Compel Defendants to disclose the passcodes for their personal smartphones (ECF Doc. No. 36) is **DENIED**.

/s/ Kearney

KEARNEY, J.

End of Document

State v. Trant

Superior Court of Maine, Cumberland County
October 22, 2015, Decided; October 27, 2015, Filed
Docket No. 15-2389

Reporter

2015 Me. Super. LEXIS 272 *

STATE OF MAINE v. MARQUISE TRANT

Counsel: [*1] VERNE PARADIE, PARADIE SHERMAN
WALKER & WORDEN, LEWISTON, ME.

DEVENS HAMLIN, HEMINWAY HAMLIN LAW
CENTER PA, PORTLAND, ME.

For State of Maine: STEPHANIE ANDERSON.

Judges: E. Mary Kelly, Maine District Court Judge.

Opinion by: Kelly

Opinion

ORDER ON STATE'S MOTION TO COMPEL PRODUCTION OF CELLPHONE PASSCODES

The Grand Jury has indicted Marquise Trant with two counts of Aggravated Trafficking in Scheduled Drugs. (Class A). The State has also filed a request for Criminal Forfeiture of U.S. currency. On April 9, 2015 and again on April 14, 2015 the State orchestrated two controlled buys through a confidential informant. On both occasions the State alleges that Mr. Trant sold crack cocaine to the confidential informant. Based on these two buys, the Maine Drug Enforcement Agency arrested Mr. Trant on April 27, 2015. When he was arrested, the police seized two cell phones, an iPhone 4 and iPhone 6. The State obtained a search warrant authorizing a search of the seized cellphones for "[e]lectronically stored information including phone numbers, names, text messages, voice recordings, photographs, video clips, date and time stamps, and other electronic information; all of which may be contraband and evidence of the offenses of possession, furnishing, [*2] and/or trafficking scheduled drugs which are seizable pursuant to Maine Rule of Criminal Procedure 41 and/or Maine Rule of Civil Procedure 80I."

The State's Drug Enforcement Agency reported on April

30, 2015 that it has been unable to execute the search on the seized phones because they are locked. See Report of Eric Pfeffer at P1 ("In order to complete the part of the investigation I would need the pin/passcode/pattern to unlock the above items. I'm requesting the owners of each device be compelled to release their pin/passcode/pattern to complete this portion of the investigation"). Accordingly, by motion filed June 11, 2015, the State "asks that this Court compel the Defendant to produce the passcodes for each phone." Subsequent to filing its motion, the State revised its position to indicate that it does not need a court order requiring Defendant to release his passcode, but rather seeks only that the Court compel the Defendant to himself insert the passcodes so that the State may gain access to the phones' contents.

The court held a non-testimonial hearing on the State's Motion to Compel on June 26, 2015. Following a conference call with counsel, the Court scheduled an evidentiary [*3] hearing on the State's motion to compel on September 29, 2015.¹ Attorney Devens Hamlin appeared on behalf of Defendant. Assistant Attorney General Lea-Anne Sutton appeared on behalf of the State. The court heard testimony from the arresting officer, Detective Bradley Rogers, and from Eric Pfeffer, as well as extensive oral argument.

At hearing the State's witness testified that the State of Maine does not have the technology required to access the information on either phone without Defendant's cooperation. The State indicated that there is a federal facility in Boston that can access encrypted information on cellphones, but only by destroying the phones, adding that in any event that facility is designated for homeland security purposes, not drug investigations. The State had initially thought that one of the phones was accessible by fingerprint, but has since determined

¹ The court initially scheduled the hearing on August 11, 2015, but continued the matter at Defendant's request to allow him to have new counsel appointed.

that both phones are password, not fingerprint, protected. The State also acknowledges that when it first seized the phones there may have been a window of time when [*4] it could have accessed the information stored on the phones, but decided to shut the phones down immediately after they were seized to avoid any possibility that Defendant might remotely delete or edit their contents.

Having considered the facts adduced at hearing, counsel's oral argument, Defendant's Objection to State's Motion to Compel, filed September 29, 2015, and the State's Response to Defendant's Objection, filed October 5, 2015, the court concludes as follows.

The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend V. See also Me. Const. art. I, § 6 ("the accused ... shall not be compelled to furnish or give evidence against himself"). It is well established that the constitutional right against self-incrimination is implicated only where there is compulsion of an incriminating testimonial communication. See, e.g., *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335, 1341 (11th Cir. 2012) ("An individual must show three things to fall within the ambit of the Fifth Amendment: 1) compulsion, 2) a testimonial communication or act, and 3) incrimination"); *United States v. Authement*, 607 F.2d 1129, 1131 (5th Cir. 1979) (same). The State argues that its pending motion does not implicate Defendant's Fifth Amendment rights on the ground that "production of the passcode is not testimonial." See Motion to Compel Passcode. The [*5] court is not persuaded by the State's argument on this point.²

It follows from U.S. Supreme Court precedent that an "act of production itself qualifies as testimonial if conceding the existence, possession and control, and authenticity of the documents tend[s] to incriminate." *United States v. Doe, supra*, 670 F.3d at 1343 (citing *Fisher v. United States*, 425 U.S. 391, 410 (1976)). While a defendant may be compelled to submit to

fingerprinting, photography, or the taking of measurements, and may be compelled to provide a blood sample or a handwriting or voice exemplar, forcing a defendant to produce a passcode is distinguishable, as a passcode is not akin to physical characteristic evidence, but rather is the product of mental processes. See, e.g., *id.* at 1345 ("The Fifth Amendment privilege is not triggered where the Government merely compels some physical act, *ie.*, where the individual is not called upon to make use of the contents of his or her [*6] mind"); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 ("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'").

The State attempts to avoid the testimonial hurdle by suggesting that it is not interested in having Defendant disclose the passcode to them, but rather simply seeks a court order directing Defendant to open the phones so that the State may gain access to his stored information, an act that the State asserts is essentially physical. The court does not agree that in this case the Fifth Amendment issue may be avoided by requiring Defendant to himself open the phones. At its core, the privilege against self-incrimination "reflects our fierce unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt." *Pennsylvania v. Muniz*, 496 U.S. 582, 596 (1990). "It is evident that a suspect is 'compelled to be a witness against himself at least whenever he must face the modern-day analog of the historic trilemma -- either during a criminal trial where the a sworn witness faces the identical three choices, or during custodial interrogation, where . . . the choices are analogous and hence raise similar concerns." *Id.* The State [*7] is asking the court to compel Defendant to give the State access to his phones, and thus Defendant is presented with the choice of acknowledging either that he indeed can access them (thus potentially incriminating himself), or lying about his inability to do so. If the court were to issue the order sought by the State, and Defendant were to fail (or were unable) to cooperate, Defendant would be subject to contempt proceedings. Accordingly, the Court does not agree that the information sought by the State is non-testimonial.³

² The State's motion presents an issue of first impression in Maine. Moreover, despite the ubiquitous presence of cellphones today, only a few reported cases address Fifth Amendment concerns with respect to cellphone passwords. See generally Marjorie A. Shields, Annotation, *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 (2015).

³ The Court recognizes that the line between testimonial and non-testimonial is very fine, and that application of Fifth Amendment jurisprudence produces what may appear to many to be an absurd result, whereby suspects who use a four-digit password to protect information on their electronic

Even though a passcode is a product of one's mind, and thus testimonial in nature, compelling production of a passcode does not offend the Fifth Amendment provided that the elements of the "foregone conclusion" doctrine are met. "The '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 are" already known to the government, such that the individual 'add little or nothing to the sum total of the Government's information.'" *Commonwealth v. Gelfgatt*, 11 N.E.2d 605, 614 (Mass. 2014) (citing *Fisher v. United States*, 425 U.S. 391, 411 (1976)).

In order for the foregone conclusion to apply, the State must establish that it already has 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.* Applying this analysis to the facts of this matter, the court finds that the State has failed to establish that production of the passcode would "add little or nothing to the sum total of the [State]'s information." The State knows that the iPhones exist and that they are passcode-protected. The State knows that the iPhones were found on Defendant's person, and that one [*9] of the phones belongs to Defendant's mother, who resides in Florida. The State knows that Defendant contacted the State's confidential informants by text message two weeks before his arrest, but does not know that the phones seized were the devices used by Defendant to send the text messages. The State knows that when Defendant was asked to give the State his passcodes he did not indicate that he did not know them; rather, Defendant asked that he be allowed to talk to his lawyer before responding to the State's request. Thus, while it is highly likely that Defendant knows the passcodes, the State does not know that Defendant has or had control over the iPhones. Furthermore, the State acknowledges that it does not know what information is stored on the phones. Accordingly, compelling either production of the passcodes or Defendant's unlocking of the phones for the State's purposes would incriminate Defendant and authenticate whatever evidence is ultimately recovered.

devices are given full sanctuary, and suspects who use their fingerprint to protect information are given no sanctuary. Given the daunting task of reconciling Fifth Amendment case-law (and the values underlying that jurisprudence) with the enormous challenges posed for law enforcement by modern encryption technology, resolution of the issues posed by password-protected cellphones may need to await consideration [*8] by the U.S. Supreme Court.

The State's relative lack of preexisting knowledge distinguishes this matter from those cases in which courts have found the foregone conclusion exception applicable. See, e.g., *Commonwealth v. Gelfgatt*, *supra*, 11 N.E.3d at 608 (holding that defendant could be compelled [*10] to provide his password to seized encrypted digital evidence "where the defendant's compelled decryption would not communicate facts of a testimonial nature to the Commonwealth *beyond what the defendant already had admitted to investigators*") (emphasis added); *Baust*, *supra*, 89 Va. Cir. At 271 ("the passcode 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 the 11th Circuit noted in *Doe*, *supra*, 670 F.3d at 1347-49, the foregone conclusion does not apply where the State "has failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the [iPhones], that [Defendant] had access to those files, or that he is capable of decrypting the files."

As stated by the U.S. Supreme Court, whether the production of evidence in response to a governmental demand is testimonial for Fifth Amendment purposes "depend[s] on the facts and circumstances of [each] particular case." *Fisher v. United States*, 425 U.S. 757 (1966); *Doe v. United States*, 487 U.S., 201, 214-15 (1988). Based on the facts and circumstances of this particular [*11] case, given the dearth of preexisting knowledge possessed by the State, the court finds that the foregone conclusion exception does not apply in these circumstances, and accordingly finds that compelling Defendant to divulge the contents of his mind -- either by compelling him to surrender the passcodes or compelling him to himself open the phones -- would violate his privilege against self-incrimination protected by the Federal and Maine Constitutions.

Accordingly, it is hereby ORDERED that the State's Motion to Compel Passcodes is DENIED.

DATED: 10/22/2015

/s/ E. Mary Kelly

E. Mary Kelly

Maine District Court Judge

MOTION TO COMPEL PASSCODE

NOW COMES the Attorney for the State and moves this Court to compel the Defendant in this case to produce the passcodes to the telephone seized from him when he was arrested for the charges of Aggravated Trafficking in Sched. W Drugs. SA Brad Rogers of the Maine Drug Enforcement Agency has obtained a search warrant from a judge, who authorized such search because there is probable cause to search said phones. However, the State is unable to execute this search warrant because the phones are protected by passcodes that cannot be unlocked. Please see attached [*12] affidavit. Wherefore, in order to execute this search warrant, the State asks that this Court compel the Defendant to produce the passcodes for each phone. The State does not need to know what the passcode is. The State asserts that production of the passcode is not testimonial. The Defendant objects to producing the passcode. The State asks that this matter be set for a hearing on this issue.

Dated: June 8, 2015

/s/ Lea-Anne Sutton

Assistant Attorney General

Maine Bar Number 8186

ORDER

Upon the State's Motion, it is hereby ORDERED that the Defendant be compelled to produce the passcode for each phone seized from him, so that law enforcement can execute a judicially authorized search warrant in this case.

Maine Drug Enforcement Agency

Continuation Report

Case #

DE-2015-0945

Author

ICSO Pfeffer, Eric R

Date of Report

04/30/2015

DETAILS OF INVESTIGATION:

1. Currently conducting a search warrant on phones seized as evidence by Special Agent Rogers for MDEA case DE-2015-0945, warrant sign by the Honorable Judge Powers. I am unable to unlock the following phones for examination. Each phone listed below has its owners name listed.

a. iPhone 6 cellular phone, model A1549, gold and white in color, IMEI# 356991067963108, [*13] found on MARQUISE TRANT's person (DOB 11/09/1988)

b. iPhone 4 cellular phone, model A1387, white in color, IC# 579C-E2430A, found on MARQUISE TRANT's person (DOB 11/09/1988)

In order to complete the part of the investigation I would need the pin/passcode/pattern to unlock the above items. I'm requesting the owners of each device be compelled to release their pin/passcode/pattern to complete this portion of the investigation.

2. I am using the UFED Touch made by Cellebrite to perform a Physical Extraction of the above Cellular devices; which requires the devices to be unlocked. I am certified Cellebrite Operator.

ATTACHMENTS:

DISTRIBUTION:

CASE STATUS:

/s/ Eric R Pfeffer

AUTHOR'S SIGNATURE

DATE

REVIEWER'S SIGNATURE

DATE

End of Document