IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES

Appellee

v.

CHRISTOPHER J. NELSON
LCpl (E-3)
U.S. Marine Corps

Appellant

REPLY BRIEF ON BEHALF OF APPELLANT

NMCCA Case No. 202000108

USCA Dkt. No. 21-0304/MC

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

Jonathan Riches
Commander, U.S. Navy Reserve
Appellate Defense Counsel
Navy-Marine Corps
Appellate Review Activity
1254 Charles Morris St., SE
Building 58, Suite 100
Washington, DC 20374
Phone: (202) 685-7290
jonathan.riches@navy.mil
Bar no. 37334

Table of Contents

Table of Cases, Statutes, and Other Authorities

Argument

I. The proper standard of review for the central legal question in this case is *de novo.*

In weighing whether Appellant knowingly waived his rights against self-incrimination and voluntarily provided his phone's passcode to law enforcement, the lower court applied an "abuse of discretion" standard to a legal question that must be reviewed *de novo*. *United States v. Nelson*, NMCCA No. 202000108, at 7 (May 4, 2021). While agreeing with Appellant that "voluntariness is a legal question reviewed *de novo*," (Ans. Br. at 12), the Government nonetheless also seeks to impose an incorrect standard of review by conflating findings of fact and conclusions of law in determining whether Appellant's statement was voluntary.

The Government contends that the legal question of voluntariness "is based on the totality of the circumstances – each of which is a factual finding." (Br. at 12.) But there are no factual findings in dispute. The question here is a legal one. *United States v. Bubonics*, 45 M.J. 93, 94 (C.A.A.F. 1996) ("Voluntariness of a confession is a question of law that an appellate court *independently* reviews *de novo.*") (emphasis added). That is, was Appellant's statement voluntary when "the 'totality of the circumstances surrounding the interrogation reveal both an uncoerced choice and the requisite level of comprehension[?]" *Moran v. Burbine*, 475 U.S. 412, 421 (1986). *Weighing* the totality of the circumstances to determine if a violation of Appellant's rights against self-incrimination has occurred is a legal

determination that this Court performs *de novo*. *United States v. Bubonics*, 45 M.J. 93, 96 (C.A.A.F. 1996) (applying "a *de novo* assessment of the totality of the circumstances…"). And without deference to how the military judge or the lower court weighed those circumstances. *United States v. Cottrill*, 45 M.J. 485, 488 (C.A.A.F. 1997) ("this Court owes no deference to the appellate court below or the military judge in deciding [whether the military judge erred on a motion to suppress as a matter of law].").

The Government also contends that whether Appellant understood his rights, and thus voluntarily provided his phone's passcode, is a factual question rather than a legal one. (Ans. Br. at 24.) In this case, Appellant asserts that his five previous refusals to allow law enforcement to search his phone is evidence that Appellant did not voluntarily provide his passcode so that a search would inevitably occur. (Opening Br. at 24-26.) According to the Government, "the finding of fact that Appellant's prior refusals indicate he understood his rights weighs in favor of the legal conclusion that Appellant's passcode entry was voluntary." (Ans. Br. at 24.)

That Appellant refused to provide his passcode five separate times *is* a *factual* observation (and one that is not disputed). But whether those refusals "indicate he understood his rights" is a *legal* determination that this Court conducts *de novo*. *United States v. Mott*, 72 M.J. 319, 332 (C.A.A.F. 2013) ("The military

judge…erred when he addressed whether Appellant's waiver was knowing and intelligent solely as a conclusory finding of fact, rather than as a conclusion of law."). By conflating the *factual* question regarding the refusals with the *legal* determination regarding Appellant's understanding of his rights, the Government seeks an improper standard of review that does not apply in this case. Instead, this Court should review the "totality of the circumstances" *de novo*, *Bubonics*, 45 M.J. at 96, to determine whether Appellant's statement was voluntary, or not.

II. Appellant did not provide his passcode to law enforcement *voluntarily* because he only did so under threat of search authorization and without an awareness of the nature of the right he was abandoning.

Appellant did not voluntarily provide his phone's passcode to law enforcement because (1) he was coerced with the threat of a search authorization, and (2) he did not comprehend his right against self-incrimination to properly waive that right. In its Answering Brief, the Government focuses—almost exclusively—on "Appellant's characteristics and the details of the interrogation [to] demonstrate Appellant voluntarily provided his passcode." (Ans. Br. at 16.) While both inquiries are essential, the Government simply misses the elements of those inquires that are central to this case. As the Supreme Court has explained, in examining the "totality of the circumstances" two criteria must be satisfied for an accused to waive his rights against self-incrimination and voluntarily provide a statement to law enforcement:

> First, the relinquishment of the right must have been voluntary in the sense that it was the product of a free and deliberate choice rather than intimidation, coercion, or deception. Second, the waiver must have been made with a full awareness of both the nature of the right being abandoned and the consequences of the decision to abandon it. Only if the "totality of the circumstances surrounding the interrogation" reveal both an uncoerced choice and the requisite level of comprehension may a court properly conclude that the *Miranda* rights have been waived. *Moran v. Burbine*, 475 U.S. 412, 421 (1986).

When Appellant provided his passcode to law enforcement, it was not "an uncoerced choice" and Appellant did not demonstrate "the requisite level of comprehension" to affect a proper waiver of his rights. And the Government has utterly failed to carry its burden under Mil. R. Evid. 304(e) to establish that Appellant's statement was voluntary.

A. Law Enforcement coerced Appellant into providing his phone's passcode by first threatening to obtain a search authorization and then presenting Appellant with a search authorization.

Both this Court and the United States Supreme Court have routinely held that consent is not voluntary when it is obtained only after law enforcement threatens to obtain a search authorization. *Bumper v. North Carolina*, 391 U.S. 543, 548 (1968); *United States v. McClain*, 31 M.J. 130, 133 (C.M.A. 1990); *United States v. White*, 27 M.J. 264, 266 (C.M.A. 1988). And in this case, Appellant provided his passcode only *after* law enforcement asserted that it had search authorization. That is because the threat of a warrant creates a "situation . . . instinct with coercion . . . ." *White*, 27 M.J. at 266. The presence of coercion is

fatal to voluntariness whether in the Fourth Amendment context, "[w]here there is coercion there cannot be consent," *id.*, or the Fifth Amendment context, where a statement is only voluntarily if it is "the product of a free and deliberate choice rather than intimidation…[or] coercion." *Moran*, 475 U.S. at 42.

The government tries to distinguish *White* and the other consent to search line of cases by observing that "Law Enforcement did not rely on Appellant's consent to search his phone." (Ans. Br. at 19.) But that is not the question. The question is whether Appellant *voluntarily* provided his phone's passcode to law enforcement so that a search would inevitably occur. In other words, the Government tries to minimize the applicability of the Fourth Amendment consent to search cases to the question of voluntariness in this self-incrimination case.

Both this Court and the Supreme Court have already rejected the argument that consent to search cases are not relevant to voluntariness of confession cases, and instead, have affirmatively held that "the same analysis would apply to either issue." *Bubonics*, 45 M.J. 93 at 94 ("Although *Schneckloth* [*v. Bustamonte*, 412 U.S. 218 (1973)] involved voluntariness of consent to a search—rather than voluntariness of a confession—the Supreme Court explained that the same analysis would apply to either issue.").

Thus, whether "Law Enforcement had proper authority to search Appellant's phone" is itself an irrelevant inquiry. What is relevant is whether law enforcement

coerced Appellant into involuntarily providing his phone's passcode so a search would occur. And what *Bumper*, *White*, and *McClain* all make abundantly clear is that where there is coercion under the threat of a search authorization, there is not voluntariness.

The Government also contends that *McClain* and other consent to search cases are irrelevant because "Appellant did not consent to a search; he assisted in the execution of a valid search authorization." (Ans. Br. at 20.) To support its argument, the Government analogizes this case to one where law enforcement has "authorization to search a suspect's padlocked locker and asking that suspect whether he is willing to remove the padlock rather than have Law Enforcement cut it off . . . ." (*Id.* at 20.) But this case is nothing like that.

In this case, the Government has failed to prove that law enforcement had the ability to unlock Appellant's phone without the passcode, as set out in Section III below. In fact, the law enforcement agent conducting the search of Appellant's case relied on Appellant to provide his passcode so that a search could occur. Thus, this case is much more like *United States v. Hubbell*, where the Supreme Court held that forcing a suspect to compile and provide incriminating documents to law enforcement violated the suspect's Fifth Amendment rights against self-incrimination. 530 U.S. 27, 43 (2000) ("The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to

surrender the key to a strongbox") (internal citations omitted). Here, Appellant did not voluntarily "assist[] in the execution of a valid search authorization." (Ans. Br. at 20.) Instead, at every turn, he resisted that search. Appellant only relented after he was threatened with a search authorization and only after he believed he had had "no choice." (J.A. at 129.) That is the opposite of "a free and deliberate choice." *Moran*, 475 U.S. at 42.

The Government also cites to *United States v. Freeman*, 65 M.J. 451 (C.A.A.F. 2008), and *United States v. Lewis*, 78 M.J. 447, 453 (C.A.A.F. 2019), to support its position that Appellant voluntarily provided his phone's passcode to law enforcement. (Ans. Br. at 15-16.) But neither of those cases involved law enforcement threatening to obtain a search authorization to compel a witness into cooperating. And neither of those cases involved a suspect who refused to provide consent to search five separate times.

In fact, the *Freeman* decision distinguishes the facts of that case by citing to *Bubonics*, 45 M.J. at 96. In *Bubonics*, this Court found that although the appellant "was advised of his pertinent rights under Article 31, UCMJ," law enforcement's threat to obtain an arrest warrant combined with a "disfavored . . . interrogation tactic, by a person in a position of authority over a sailor who has been conditioned to respond to authority" was sufficient to show that appellant's statement was not voluntary. Likewise, here, even though Appellant signed an Art. 31 rights waiver,

he was later confronted with the threat of a search authorization by a law enforcement agent in a position of authority. Although Appellant clearly did not wish to provide his passcode, and although Appellant would not have provided his passcode if making "an essentially free and unconstrained choice," *id.* at 95, he was coerced under the threat of search authorization into doing so. And where there is coercion, there cannot be voluntariness.

The government also contends that Appellant's five prior refusals to allow law enforcement to search his phone "weigh in favor of voluntariness." (Ans. Br. at 24.) But "the repeated and prolonged nature of the questioning" is not evidence of voluntariness, but instead is evidence that a defendant's "will was overborne in a particular case." *Schneckloth*, 412 U.S. at 226. Here, Investigator Hotel knew that Appellant did not want to provide his phone passcode because Appellant told him five separate times during a two-hour interview that he did not wish to provide it. (J.A. at 129). But Investigator Hotel repeated the same questioning over and over again and then under threat of search authorization, to overcome Appellant's will. That is not evidence of voluntariness; it is the opposite.

The Government's argument regarding voluntariness ultimately rests almost exclusively on the Appellant's personal characteristics; viz, that he is a "twenty-five-year-old E-3 who had served for four years . . . ." (Ans. Br. at 16.) Courts examine the personal characteristics of an accused to determine whether the tactics

used by the police are sufficiently coercive to render the accused's statement involuntary. *United States v. Preston*, 751 F.3d 1008, 1019 (9th Cir. 2014). In this case, whether the accused is a twenty-five-year-old E-3, or a more seasoned servicemember, *Bumper*, *White*, and *McClain* all stand for the proposition that consent cannot be voluntary if made under the threat of a search authorization. In that regard, Appellant's personal characteristics as a junior, enlisted sailor confronted by a law enforcement agent in a position of authority weigh in favor of the involuntariness of Appellant's statement.

What's more, in finding that an accused's consent to search was not voluntary in *United States v. Wallace*, this Court held that "it is doubtful" that "a twenty-six-year-old staff sergeant with nearly eight years of service" would know "he could withdraw consent once given." 66 M.J. 5, 9 (C.A.A.F. 2008). The same is true here. It is also "doubtful" that Appellant, a twenty-five-year-old E-3, would know that he has the right to refuse to provide his phone's passcode when confronted by law enforcement with a search authorization for his phone.

The other reason why courts examine the characteristics of an accused in determining voluntariness is to ascertain whether the statement is, in fact, "the product of a free and deliberate choice." *Moran*, 475 U.S. at 421. In this case, we don't need to guess at that question because Appellant himself could not have made it clearer that providing his passcode was not "a free and deliberate choice."

Id. Instead, Appellant stated in no uncertain terms that he would provide his passcode to law enforcement only "if I don't have a choice." (J.A. at 87.) It is, of course, axiomatic that if someone believes he or she does not have a choice about whether to do something their action is not free and deliberate. Thus, in this case, Appellant's statement to law enforcement also shows that when he provided his phone's passcode to his interrogator, it was not "a free and deliberate choice." *Moran*, 475 U.S. at 421. It was the opposite.

B. Appellant did not voluntarily provide his passcode to law enforcement because he did not know he was abandoning his rights against self-incrimination, nor did he know the consequences of abandoning those rights.

The second inquiry in determining whether Appellant voluntarily waived his rights against self-incrimination is whether such a waiver was "made with a full awareness of both the nature of the right being abandoned and the consequences of the decision to abandon it." *Moran*, 475 U.S. at 421. The Government contends that Appellant understood his rights because he signed a rights waiver[1] "yet [did] not allow[] the Agent to search his phone." (Ans. Br. at 16.)

[1] The rights advisement that Appellant signed pertained to allegations of drug use, not drug introduction or distribution; thus, his waiver with respect to statements that would pertain to other allegations was not knowing and intelligent. *Maryland v. Shatzer*, 559 U.S. 98, 109 (2010) (evidence obtained from a second interrogation about a different crime is inadmissible when defendant invoked right to counsel during first interrogation); *see also United States v. Simpson*, 54 M.J. 281, 283 (C.A.A.F. 2000). Specifically, when Appellant signed the Article 31(b) and *Miranda* rights advisement on 30 April 2019, he was informed that he was

But when Investigator Hotel threatened to obtain a search authorization for Appellant's phone, and later presented the search authorization to Appellant, it was clear Appellant did not know he could still refuse to provide the passcode. That is, Appellant did not understand that a command search authorization did not provide the government access to the *contents* of Appellant's phone. Rather, unbeknownst to Appellant, law enforcement needed Appellant to incriminate himself by providing the passcode to access the contents of the phone. Indeed, the entire reason Investigator Hotel persistently questioned Appellant about the code was so that he could conduct a search that he was otherwise unable to conduct without the passcode. In this case, it is clear that Appellant did not understand the distinction between a command authorization to seize and search the phone and his rights against self-incrimination not to provide the passcode so a search would occur.

During the first interrogation of Appellant, Investigator Hotel sought consent to search Appellant's iPhone *twice* within twenty-four minutes, and Appellant declined *twice*. (J.A. at 129.) It was only *after* the investigator told Appellant that

---

suspected of "wrongful use, possession, etc. of controlled substances" only. J.A. at 56. He was *not* advised that he was suspected of conspiracy to wrongfully distribute, wrongful distribution, or introduction of controlled substances – the far more serious charges in this case. *Id.* Appellant admitted to drug *use*, J.A. at 129, but was adamant that he did not wish to provide statements about the contents of his phone, which, contained evidence of most of the crimes for which he was ultimately charged but was never advised he was suspected of committing.

he would obtain a search authorization from Appellant's Commanding Officer to search the phone that Appellant said, "I guess at that point I'd have no choice." (*Id.*) In other words, Appellant did not know that a search authorization alone would not allow law enforcement to access the *contents* of his phone, and thus he did not understand the consequences of abandoning his rights against self-incrimination.

Additionally, approximately an hour and a half into the first interrogation, Investigator Hotel asked for Appellant's consent to search his smart phone for a *fifth* time. (*Id.*) Appellant again declined, and responded, "[N]ot *without knowing* whether I'd be incriminating myself." (*Id.* (emphasis added).) That is, Appellant plainly stated that he did not know or have a "full awareness," *Moran*, 475 U.S. at 421, of the nature of his rights against self-incrimination, or the consequences of abandoning those rights.

Nearly the same exact thing happened the next day during the second interrogation. On 1 May 2019, Appellant was informed by Investigator Hotel that he had obtained a command authorization to search Appellant's phone. The CID investigator then again solicited Appellant for his passcode. Once again, Appellant responded, "I will if I don't have a choice." (J.A. at 87.)

These statements are not evidence of a knowing, intelligent, and voluntary waiver, as the Government suggests. (Ans. Br. at 16-18.) These statements are

evidence that Appellant was unaware of his right—or his "choice"—to provide his passcode after law enforcement asserted that it had a search authorization for the phone. Like the appellant in *Wallace*, 66 M.J. at 9, Appellant here believed he "had to" provide the code in the same way Wallace believed he "had to" let law enforcement take his computer. Once presented with the search authorization, Appellant was simply unaware of his right to still refuse to provide the passcode, which is why he provided it only after concluding that he didn't have "a choice." (J.A. at 87.) Just like *Wallace*, Appellant's "acquiescence did not constitute free and voluntary consent." *Wallace*, 66 M.J. at 9.

III. The government the failed to meet its burden of proving that inevitable discovery applies.

The inevitable discovery doctrine only applies if the Government can prove "by a preponderance of the evidence," that "the evidence would have been obtained even if the statement had not been made." M.R.E. 304(b). The Government has not proven that; in fact, this record shows that evidence from Appellant's phone would very likely *not* have been discovered in the absence of Appellant's statement.

The Government cites to *United States v. Owens*, 51 M.J. 204, 208 (C.A.A.F. 1999), to contend that the incriminating text messages on Appellant's phone would have been inevitably discovered because law enforcement has probable cause to search Appellant's phone and "had already obtained a search

authorization for the phone." (Ans. Br. at 26.) But *Owens* is inapplicable because it assumes law enforcement would have been able to conduct the search whether or not Appellant provided further information. Here, the record shows that even after law enforcement obtained search authorization for the phone, it *still* needed Appellant to provide the passcode so that law enforcement could search the phone's contents.

The Government argues that "if Appellant had not entered his passcode, Law Enforcement had the means and intention to unlock it themselves." (Ans. Br. at 25.) Specifically, the Government contends that it would have inevitably discovered the incriminating text messages because the Defense Criminal Forensic Laboratory ("Laboratory") "ha[s] the capability of breaking passcode[s]." (Ans. Br. at 27; J.A. 65.) But the record here does not establish that fact regarding *this* passcode on *this* iPhone. In other words, on this record, the Government has failed to meet its burden that the inevitable discovery exception applies.

The government's *only* witness to testify about whether Appellant's phone could be forcibly unlocked without the passcode testified that he did not know whether it could be unlocked without the code. Although Investigator Hotel's testimony on this point was woefully inconsistent,[2] he ultimately concluded that he

[2] *Compare* J.A. 69 (Investigator Hotel testifies that he had experience with two phones that were the same model at Appellant's, and D.S.F.L. was only able to

did not know whether law enforcement would be able to unlock a phone of Appellant's make and model. When asked, "So you did not know at the time [the phone was seized] whether or not D.S.F.L. would be able to successfully unlock that phone?" Investigator Hotel responded, "I did not. No, sir…" (J.A. at 69-70.) Thus, the Government's only witness to testify whether law enforcement could have unlocked Appellant's phone ultimately concluded that he did not know whether or not law enforcement would have been successful in doing so.

Based on that testimony, by definition, it is not more likely than not that law enforcement could have unlocked the phone, and therefore, the preponderance of evidence *does not* establish that the government would have inevitably discovered the phone's contents in the absence of Appellant's statement. *Nix v. Williams,* 467 U.S. 431, 457 (1984) ("An inevitable discovery finding is based on objective evidence concerning the scope of the ongoing investigation which can be objectively verified or impeached.").

What's more, although it is the *Government's burden* to establish inevitable discovery, not Appellant's burden to disprove it, the record shows that law enforcement likely would not have been able to access the contents of Appellant's phone in the absence of Appellant's statement. That is because modern smart

---

unlock one of them) *with* J.A. 80 (Investigator Hotel testifies that he does not have experience with "similar type devices that were involved in this case").

phones, like Appellant's, have sophisticated encryption protections that make the phones "unbreakable" in the absence of the passcode. As the U.S. Supreme Court observed in *Riley v. California*, "Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password." 573 U.S. 373, 389 (2014) (citing Brief for United States as *Amicus Curiae* in No. 13–132, p. 11).

Here, the record shows that it is not more likely than not that law enforcement would have been able to successfully break Appellant's phone with "brute force." (J.A. at 69.) During the court-martial proceedings, trial defense counsel asked Investigator Hotel, "What is [the Laboratory's] success with unlocking updated iPhones?" (J.A. at 69.) Investigator Hotel answered, "I can say that the model *Nelson's phone* – I've had two – one and two of one recent case (*sic.*) that they were able to unlock." (*Id.*) Trial defense counsel then clarified, "[H]as there been cases with iPhones where they have not been able to unlock it?" (*Id.*) Investigator Hotel responded, "One, sir." (*Id.*) In other words, although his testimony was confused and contradictory, with respect to "Nelson's phone," the evidence in the record shows that law enforcement has been able to unlock one and has not been able to unlock one. The Government's fifty percent "success" rate in unlocking phones of Appellant's make and model by definition means it is not

more likely than not that law enforcement would have been able to inevitably unlock Appellant's phone.

Investigator Hotel's testimony regarding the "four or five" other cases (J.A. at 69) in which the Laboratory was able to unlock other phones is of little probative value because those phones were not the same make and model as Appellant's phone, and according to Investigator Hotel "[t]he model of the iPhone plays a big part in it . . . ." (J.A. at 79.) What's more, the testimony regarding whether the number of digits in the passcode makes unlocking it more difficult was inconclusive, at best. Investigator Hotel directly testified that "I don't remember if the digits or the number of digits have any play in it." (J.A. at 80.)

Because the Government's *only* witness to testify regarding inevitable discovery ultimately concluded that he did not know whether law enforcement "would be able to successfully unlock" Appellant's phone, (J.A. at 69-70), by definition, the Government has failed to meet its burden. Indeed, while the Government's evidence on this point is inconsistent and contradictory, it shows that law enforcement would have had no better than a fifty percent shot at opening a phone of the same model as Appellant's. Consequently, the Government has simply failed to meet its burden of establishing that inevitable discovery applies, and the record, in fact, establishes the opposite.

Certificate of Compliance with Rule 24

This brief complies with the type-volume limitation of Rule 24(c) because this brief contains 4,225 words.

This brief complies with the typeface and type style requirements of Rule 37.

/s/ Jonathan Riches
Jonathan Riches
CDR, JAGC, U.S. Navy Reserve
Appellate Defense Counsel
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris St., SE
Building 58, Suite 100
Washington, DC 20374
Phone: (202) 685-7290
jonathan.riches@navy.mil

Certificate of Filing and Service

I certify that the foregoing was caused to be delivered electronically to this Court, and that copies were electronically delivered to Deputy Director, Appellate Government Division, and to Director, Administrative Support Division, Navy-Marine Corps Appellate Review Activity, on January 11, 2022.

/s/ Jonathan Riches
Jonathan Riches
CDR, JAGC, U.S. Navy Reserve
Appellate Defense Counsel
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris St., SE
Building 58, Suite 100
Washington, DC 20374
Phone: (202) 685-7290
jonathan.riches@navy.mil