UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES
Appellant

v.

Edward J. MITCHELL II, Sergeant
United States Army, Appellee

No. 17-0153
Crim. App. No. 20150776

Argued April 4, 2017—Decided August 30, 2017

Military Judge: Rebecca K. Connally

For Appellant: *Captain Samuel E. Landes* (argued); *Colonel Mark H. Sydenham* and *Lieutenant Colonel A. G. Courie III* (on brief); *Major Anne C. Hsieh.*

For Appellee: *Captain Joshua B. Fix* (argued); *Lieutenant Colonel Christopher D. Carrier* and *Captain Katherine L. DePaul* (on brief); *Major Andres Vazquez Jr.*

Amici Curiae for Appellant: *Colonel Katherine E. Oler, Major Mary Ellen Payne*, and *Gerald R. Bruce*, Esq. (on brief)—for Air Force Appellate Government Division. *Sean Patrick Flynn* (law student) (argued); *Alyssa Hughes* (law student), *Jimmy Gurulé*, Esq. (supervising attorney), and *Marah McLeod*, Esq. (supervising attorney) (on brief)—Notre Dame Law School.

Amici Curiae for Appellee: *Jamie Williams*, Esq., and *Mark Rumold,* Esq. (Electronic Frontier Foundation); *Brett Max Kaufman*, Esq., and *Patrick Toomey*, Esq. (American Civil Liberties Union); and *Arthur B. Spitzer*, Esq, and *Scott Michelman*, Esq. (ACLU of the District of Columbia) (on brief)—for Electronic Frontier Foundation, American Civil Liberties Union, and ACLU of the District of Columbia. *Dominic X. Barceleau* (law student) (argued); *Stephen F. Smith*, Esq. (supervising attorney) (on brief)—Notre Dame Law School.

Chief Judge STUCKY delivered the opinion of the Court, in which Judges OHLSON and SPARKS, and Senior Judge ERDMANN, joined. Judge RYAN filed a separate dissenting opinion.

Chief Judge STUCKY delivered the opinion of the Court.

We address today the Fifth Amendment limits on asking a suspect to unlock his phone when the device has been seized pursuant to a valid search and seizure authorization.[1] Because Appellee had previously invoked his right to counsel, we hold that the Government violated his Fifth Amendment rights as protected by *Edwards v. Arizona*, 451 U.S. 477 (1981), when agents asked him in the absence of counsel to enter the phone's passcode. Pursuant to the plain language of Military Rule of Evidence (M.R.E.) 305(c)(2), the contents of the phone must therefore be suppressed.

I. Background

Sergeant Edward J. Mitchell II (Appellee) is charged with many offenses, including using calls, text messages, and lewd online postings to harass his wife, in violation of a no-contact order issued after she made an allegation of sexual assault.[2] The facts relevant to this appeal occurred after Appellee's wife told military police that Appellee was calling and texting her with numbers artificially created by applications on his phone or computer (spoofing), and had posted nude photographs of her online and in cell phone communication applications, Whisper and Kik.

Staff Sergeant (SSG) Knight, a member of Appellee's unit, escorted him to a military police station in Fort Hood, Texas, to discuss the allegations, where Investigator Tsai informed Appellee of his rights. Appellee invoked his right to counsel at approximately 10:50 a.m. Appellee's platoon leader signed a "Receipt for Pre-Trial/Post Trial Prisoner or Detained Person," and SSG Knight escorted Appellee back to

---

[1] We heard oral argument in this case at the University of Notre Dame Law School, Notre Dame, Indiana, as part of the Court's Project Outreach. This practice was developed as a public awareness program to demonstrate the operation of a federal court of appeals, and the military justice system.

[2] The facts stated in the text are drawn from the military judge's findings of fact. Both parties ask the Court to rely upon additional facts taken from the record rather than official findings, but we need not address these putative facts.

his unit, where he remained in the company area and accessed both his Kyocera phone and iPhone.

Meanwhile, Investigator Tsai obtained a verbal authorization to seize and search various electronic media belonging to Appellee, including cell phones, for "evidence of spoofing calls, text messages or other similar communications … and other similar software capable of allowing communications in a spoofing … fashion." Appellee's commander learned that investigators were on their way, and a member of Appellee's company was directed to find and bring Appellee to the commander's office. When Investigators Tsai and Carlton arrived between 1:00 and 1:30 p.m., little more than two hours after the original request for counsel, Appellee was waiting in the office with his commander.

In the office, Investigator Tsai informed Appellee of the verbal search and seizure authorization, and Appellee questioned the validity of verbal authorizations, asking to see a written one. Around this time, the commander left the office. Investigator Tsai told Appellee that verbal authorizations are valid and asked if Appellee had any cell phones on his person. Appellee then handed an iPhone to the investigators. Investigator Tsai saw that the iPhone was protected by a numeric passcode, and asked Appellee to provide it. Appellee refused.

Investigator Tsai then handed the phone back to Appellee and asked him to unlock it, saying: "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." Neither investigator knew at the time that Appellee's iPhone had two finger/thumb prints stored, and could have potentially been opened using "Touch ID capabilities." Appellee then entered his passcode and unlocked the phone: "[Appellee] was also required to permanently disable the cell phone's passcode protection. In order to do so, [he] was required to access the phone's settings and enter his numeric passcode (PIN) two more times to fully disable the phone's protections." (Footnote omitted.)

After Appellee permanently unlocked and surrendered his iPhone, investigators directed Appellee to his vehicle and barracks room to execute the rest of the search and seizure

authorization. In Appellee's room, investigators seized Appellee's computer, and asked him to provide the password. He refused, and the investigators did not press him further.

Following a defense motion to suppress, the military judge held that the Government had violated Appellee's Fifth Amendment right against self-incrimination and his *Edwards* right to counsel, and suppressed "[t]he iPhone at issue and any evidence derived therefrom."[3] The Government appealed pursuant to Article 62, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 862 (2012). The United States Army Court of Criminal Appeals (CCA) held that the military judge's findings of fact were ambiguous, set aside the ruling suppressing the evidence, and remanded, ordering the military judge to make detailed findings. *United States v. Mitchell*, No. ARMY MISC 20150776, 2016 CCA LEXIS 179, 2016 WL 1128111 (A. Ct. Crim. App. Mar. 18, 2016). In her second order, the military judge clarified, inter alia, that Appellee was in custody at the police station and in his commander's office, although not during the intervening time, and again suppressed the iPhone and its contents. After the Government again appealed, the CCA upheld the order. *United States v. Mitchell*, No. ARMY MISC 20150776, 2016 WL 4529149 (A. Ct. Crim. App. Aug. 29, 2016) (per curiam). The CCA later denied a motion for reconsideration and suggestion for consideration en banc. *United States v. Mitchell*, No. ARMY MISC 20150776 (A. Ct. Crim. App. Oct. 24, 2016) (order). The Government then certified the case for our review.

II. Analysis

The Fifth Amendment provides that "[n]o person … shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. Because "[t]he circumstances surrounding in-custody interrogation can operate very quickly to overbear the will of one merely made aware of his privilege by his interrogators.… the right to have counsel present at the interrogation is indispensable to the protec-

[3] The order also discussed various Fourth Amendment claims, and suppressed a book found in Appellee's car on those grounds. That ruling is not before the Court.

tion of the Fifth Amendment privilege." *Miranda v. Arizona*, 384 U.S. 436, 469 (1966).

Once a suspect in custody has "expressed his desire to deal with the police only through counsel, [he] is not subject to further interrogation by the authorities until counsel has been made available to him, unless the accused himself initiates further communication." *Edwards*, 451 U.S. at 484–85; *see* M.R.E. 305(e)(3). "In every case involving *Edwards,* the courts must determine whether the suspect was in custody when he requested counsel and when he later made the statements he seeks to suppress." *Maryland v. Shatzer*, 559 U.S. 98, 111 (2010). We have previously recognized that "*Edwards* clearly applies to the military." *United States v. Dock*, 40 M.J. 112, 115 (C.M.A. 1994).

We review a military judge's ruling on a motion to suppress for an abuse of discretion and consider the evidence in the light most favorable to the party that prevailed at trial. *United States v. Rodriguez*, 60 M.J. 239, 246–47 (C.A.A.F. 2004). "A military judge abuses [her] discretion if [her] findings of fact are clearly erroneous or [her] conclusions of law are incorrect." *United States v. Olson*, 74 M.J. 132, 134 (C.A.A.F. 2015) (internal quotation marks omitted) (citation omitted). These standards also apply to interlocutory appeals under Article 62, UCMJ. *United States v. Michael*, 66 M.J. 78, 80 (C.A.A.F. 2008).

Under the circumstances presented, we conclude that the Government violated Appellee's Fifth Amendment right to counsel as protected by *Miranda* and *Edwards*. The Government does not contest that Appellee was in custody when he invoked his right to counsel while detained at the military police station. It is almost equally clear that Appellee was in custody in his commander's office when investigators asked him to unlock his iPhone. "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 not at liberty to terminate the interrogation and leave." *Thompson v. Keohane*, 516 U.S. 99, 112 (1995). "[T]he ultimate inquiry is simply whether there is a formal arrest or restraint on freedom of movement of the degree associated with a formal arrest." *California v. Beheler*, 463 U.S.

1121, 1125 (1983) (internal quotation marks omitted) (citation omitted). Courts evaluate:

> (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 suspect.

United States v. Chatfield, 67 M.J. 432, 438 (C.A.A.F. 2009) (internal quotation marks omitted) (citing *Oregon v. Mathiason*, 429 U.S. 492, 495 (1977); *United States v. Mittel-Carey*, 493 F.3d 36, 39 (1st Cir. 2007)).

When investigators confronted Appellee to execute the search and seizure authorization, he had been in custody less than two hours earlier at a military police station, where he originally invoked his right to counsel.[4] Pursuant to his commander's orders, Appellee was taken to his commander's office for the express purpose of allowing the agents to again speak with him and execute the authorization. Thus, (1) Appellee did not appear voluntarily and (2) the "location and atmosphere of the place" suggested that Appellee was again in custody. Although (3) the length of the questioning itself was not particularly remarkable, (4) the Government had two law enforcement officers on the scene, backed by the authority of Appellee's commander. Finally, (5) although Appellee was not handcuffed, he was restrained just as completely by an environment in which both his command and the Government investigators required him to remain in place. Under these circumstances, Appellee was subject to "'restraint on freedom of movement' of the degree associated with a formal arrest," and was therefore in custody. *Beheler*, 463 U.S. at 1125 (citation omitted).

In addition to being in custody, Appellee was also subject to interrogation. Interrogation of a suspect includes "not on-

[4] This break in custody was obviously less than the fourteen days required to terminate *Edwards* protection. *Shatzer,* 559 U.S. at 109–10.

ly … express questioning, but also … 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 (1980) (footnote omitted); *Edwards*, 451 U.S. at 486–87 (applying the *Innis* standard).

After investigators seized Appellee's iPhone and saw that it was passcode protected, they immediately "asked [him] if he could provide the PIN to unlock the phone." When Appellee refused, the agents handed his phone back to him and asked him to "help [them] out" by entering the passcode himself. Appellee "eventually complied with the nature of their request" and permanently unlocked his phone for the agents.

This line of questioning qualifies as interrogation. The agents' initial request—"can you give us your PIN?"—is an express question, reasonably likely to elicit an incriminating response. The Government contends that a request for consent to search is not an interrogation, citing this Court's reasoning in *United States v. Frazier* that "such requests are not interrogations and the consent given is ordinarily not a statement." 34 M.J. 135, 137 (C.M.A. 1992). But asking Appellee to *state* his passcode involves more than a mere consent to search; it asks Appellee to provide the Government with the passcode itself, which is incriminating information in the Fifth Amendment sense, and thus privileged. "The privilege … not only extends to answers that would in themselves support a conviction … but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute ...." *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *see also United States v. Hubbell*, 530 U.S. 27, 37–38 (2000).

When the agents switched tactics and succeeded in getting Appellee to enter his passcode rather than verbally provide it, that request was part of the same basic effort to convince Appellee to provide the information necessary for the Government to access and search the contents of his phone, and to help prove that he himself had the same ability

(which also extends beyond a mere consent to search).[5] By asking Appellee to enter his passcode, the Government was seeking an "answer[] … which would furnish a link in the chain of evidence needed to prosecute" in the same way that *Hoffman* and *Hubbell* used the phrase. Not only did the response give the Government access to direct evidence as in *Hubbell*, it also constituted direct evidence as in *Hoffman*. *See Hubbell*, 530 U.S. at 39–40 ("The documents were produced before a grand jury …. The use of those sources of information eventually led to the return of an indictment …."); *Hoffman*, 341 U.S. at 488 ("[T]ruthful answers … to these questions might have disclosed that he was engaged in such proscribed activity."). As even the dissent concedes, Appellee's response constitutes an implicit statement "that [he] owned the phone and knew the passcode for it." *Mitchell,* __ M.J. at __ (8) (Ryan, J., dissenting). And the fact that Investigators Tsai and Carlton could have testified to this act confounds any contention that "entering the passcode—was not incriminating." *Id.* at __ (7).

Viewed as a whole, the Government's inquiries constituted "not only … express questioning, but also … words or actions … that the police should know are reasonably likely to elicit an incriminating response from the suspect." *Innis*, 446 U.S. at 301 (footnote omitted). Without the benefit of counsel that he had requested, subjecting Appellee to a custodial interrogation endangered his Fifth Amendment privilege against self-incrimination and violated the protective rule created in *Edwards*. 451 U.S. at 484–85. In light of this holding, we need not reach the question of whether the Government directly violated Appellee's Fifth Amendment privilege against compelled self-incrimination. We thus do not address whether Appellee's delivery of his passcode was "testimonial" or "compelled," as each represents a distinct inquiry. *Hiibel v. Sixth Judicial Dist. Court of Nev.*, 542 U.S. 177, 189 (2004).

---

[5] Accordingly, we need not consider the applicability of this Court's holding in *United States v. Hutchins* that a request for consent to search may in certain circumstances violate *Edwards*. 72 M.J. 294, 298–99 (C.A.A.F. 2013).

The dissent contends that the Fifth Amendment only protects testimonial communications, *Mitchell*, __ M.J. at __ (4–6) (Ryan, J., dissenting), but we are enforcing the "prophylactic" *Miranda* right to counsel, and the "second layer of prophylaxis" established in *Edwards*, both of which are constitutionally grounded measures taken to protect the core Fifth Amendment privilege. *McNeil v. Wisconsin*, 501 U.S. 171, 176–77 (1991); *accord Dickerson v. United States*, 530 U.S. 428, 442–43 (2000) (upholding *Miranda* against legislative challenge, but declining to hold that nothing besides *Miranda* will ever "suffice to satisfy constitutional requirements").

Because *Edwards* forbids interrogation following the invocation of the *Miranda* right to counsel, not just interrogation that succeeds, 451 U.S. at 484–85, it follows that those who seek *Edwards* protection do not need to establish that the interrogation produced or sought a testimonial statement in order to establish a violation. Rather, only interrogation itself must be established, and Appellee has demonstrated that entry of his passcode was an "incriminating response" that the Government should have known they were "reasonably likely to elicit." *Innis*, 446 U.S. at 301. Once an *Edwards* violation has been established, whether the incriminating response or derivative evidence will be suppressed is a question of remedy, not wrong. This interpretation of *Edwards* makes intuitive sense, because badgering an unrepresented suspect into granting access to incriminating information threatens the core Fifth Amendment privilege, even if the government already knows that the suspect knows his own password.

At the moment when interrogation occurred, the violation of Appellee's rights under *Edwards* was complete. The only question that remains is the proper remedy. Under the plain language of the Military Rules of Evidence, any evidence derived from a violation of *Edwards* must be suppressed. "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." M.R.E. 305(c)(2) (emphasis added).

The Government argues that the suppression of derivative evidence does not extend to violations of the *Edwards* rule, citing *United States v. Patane*, 542 U.S. 630 (2004). In *Patane*, a three-justice plurality of the Supreme Court held that physical evidence discovered as a result of a suspect's voluntary statements was admissible at trial, despite the failure to administer a *Miranda* warning. *Id.* at 634. The Government reasons that if derivative evidence is not suppressed when *Miranda*'s prophylactic protections are violated,[6] certainly the same rule applies when the *Edwards* "second layer of prophylaxis," *McNeil*, 501 U.S. at 176, is violated. But whatever the merits of the Government's *Patane* argument, the Military Rules of Evidence expressly provide that "[a]n individual may claim the most favorable privilege provided by the Fifth Amendment to the United States Constitution, Article 31, *or these rules*." M.R.E. 301(a) (emphasis added). And though the Government argues that the derivative evidence language in M.R.E. 305(c)(2) is the result of a scrivener's error, those arguments are not persuasive.[7]

---

[6] Although originally referred to as a prophylactic rule, we recognize that *Miranda* actually announced a constitutional rule. *Dickerson*, 530 U.S. at 444.

[7] The Government argues that the 2013 amendment resulting in the modern language "was not intended to have any substantive effect at all." It is true that the Drafters' Analysis does not mention *Patane*, and explains that M.R.E. 305(c)(2) was retitled "Fifth Amendment Right to Counsel" in order to "allow practitioners to quickly find the desired rule," and that changes which "ensure that [the rule] addressed admissibility rather than conduct" were "not intend[ed] to change any result in any ruling on evidence admissibility." *Manual for Courts-Martial, United States*, Analysis of the Military Rules of Evidence app. 22 at A22-19 (Supp. 2012 ed.). But the analysis indicates in several places that changes were intended to be substantive, including explicit acknowledgment that "subsection (c)(3) provides more protection than the Supreme Court requires," and that "[t]he words 'after such request' were added to subsection (c)(2)" for a substantive purpose. *Id.* In the absence of a more convincing argument that an entire phrase was accidentally inserted, this Court will thus apply the plain language of M.R.E. 305(c)(2).

Furthermore, the Government has not established that the contents of Appellee's phone are admissible because they would have inevitably been discovered. For the exception to apply, the Government must "demonstrate by a preponderance of the evidence that 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 in a lawful manner." *United States v. Wicks*, 73 M.J. 93, 103 (C.A.A.F. 2014) (internal quotation marks omitted) (citations omitted). The Government's sole argument[8] is that it could have legally compelled Appellee to "press his finger to the phone and thereby unlock it" under *United States v. Fagan,* 28 M.J. 64, 69 (C.M.A. 1989) ("A servicemember simply has no basis to withhold fingerprints from military authorities [on Fourth Amendment grounds], provided that the manner of collecting them is reasonable."); *see also Doe v. United States*, 487 U.S. 201, 210–11 (1988) (the compulsion of physical, nontestimonial acts is not prohibited by the Fifth Amendment). But the record discloses no guarantee that this procedure would have succeeded, and the Government therefore cannot demonstrate inevitability.

Although the iPhone "had Touch ID capabilities" and "the accused had two finger/thumbprints saved," we cannot know whether Appellee had in fact turned fingerprint access "on" (as opposed to simply saving his fingerprints), because the phone's entire security system is now permanently turned off. Moreover, the Government did not even learn about the possibility of fingerprint access until April 20, 2016, over fifteen months after the offending interrogation. We conclude that the Government's eventual access to the phone's contents was not inevitable, but rather "a matter of mere speculation and conjecture, in which [the Court] will not engage." *United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996).

Although the contents of Appellee's phone are therefore inadmissible, Appellee's physical iPhone should not have been suppressed, since it was seized pursuant to lawful au-

[8] Notably, the Government does not argue that a digital forensic examiner could have bypassed Appellee's security, as Investigator Tsai claimed.

thorization prior to the *Edwards* violation, or any other alleged Fifth Amendment violation. The phone itself does not constitute evidence derived from the illicit interrogation, and the possibility that a court-martial panel could impermissibly review the phone's contents—since it is now permanently unlocked—could be overcome with an instruction forbidding such use. The military judge therefore abused her discretion in suppressing the phone itself.

III. Judgment

The decision of the United States Army Court of Criminal Appeals, to the extent that it affirmed the suppression of the contents of the iPhone, is hereby affirmed. To the extent that it affirmed the suppression of the physical phone, it is reversed. The record is returned to the Judge Advocate General of the Army for transmission to the convening authority for further proceedings.

Judge RYAN, dissenting.

I disagree that the Government violated Appellee's legal rights by asking him to enter the passcode to unlock his iPhone, a device the Government had the legal right to seize and search pursuant to a valid search authorization. It is abundantly clear that such a request does not constitute an "interrogation," *see Edwards v. Arizo*na, 451 U.S. 477, 485 (1981); Military Rule of Evidence (M.R.E.) 305(c)(2), in derogation of the Fifth Amendment's protection against "being compelled in any criminal case to be a witness against himself." U.S. Const. amend. V [hereinafter Fifth Amendment]; *cf. United States v. Seay*, 60 M.J. 73, 78 (C.A.A.F. 2004) ("*Edwards* [was] adopted in M.R.E. 305[(f) (version in force in 2002, now M.R.E. 305(c)(2), (4))]."). And, even assuming it could constitute a *testimonial* statement, the entry of a passcode into a phone known to belong to Appellee does not constitute an *incriminating* statement.[1] Therefore, I respectfully dissent.

I.

We review a military judge's ruling on a motion to suppress for an abuse of discretion. *United States v. Keefauver*, 74 M.J. 230, 233 (C.A.A.F. 2015). In doing so, "we consider the evidence in the light most favorable to the prevailing party." *United States v. Cowgill*, 68 M.J. 388, 390 (C.A.A.F. 2010) (quotation marks omitted). This Court reviews findings of fact for clear error and conclusions of law de novo. *United States v. Leedy*, 65 M.J. 208, 213 (C.A.A.F. 2007). "Whether an interrogation occurred is a question of law, reviewable *de novo* by . . . this Court." *United States v. Kosek*, 41 M.J. 60, 63 (C.M.A. 1994); *cf. United States v. Davis*, 773 F.3d 334, 338 (1st Cir. 2014); *Endress v. Dugger*, 880 F.2d 1244, 1249 (11th Cir. 1989).

---

[1] The fact that investigators initially asked Appellee to speak his passcode is irrelevant for purposes of the Fifth Amendment or *Edwards* inquiry as he declined to tell them his passcode—there was no statement. *See United States v. Patane,* 542 U.S. 630, 634 (2004) (plurality opinion); *McNeil v. Wisconsin*, 501 U.S. 171, 176 (1991).

I agree that Appellee properly invoked his right to counsel and was in custody at the time of the request. But even reviewing the facts in the light most favorable to Appellee, the military judge erred as a matter of law in concluding that the below request constitutes interrogation:

> If you could unlock it, great, if you could help us out. But if you don't, we'll wait on a—for a digital forensic expert to unlock it.[2]

An "interrogation" does not occur unless law enforcement officers ask questions "reasonably likely to elicit an *incriminating* response from the suspect." *Rhode Island v. Innis*, 446 U.S. 291, 301 (1980) (emphasis added).

First, it seems dubious at best to assume that Appellee's act of unlocking his iPhone by physically entering his passcode constituted a "testimonial" event. *See United States v. Venega*s, 594 F. App'x 822, 827 (5th Cir. 2014) (per curiam) (concluding that defendant's consent to search his cellular telephone and provision of his passcode were "neither testimonial nor communicative in the Fifth Amendment sense" (quotation marks omitted)).

Indeed, the majority opinion has no clear testimonial statement to work with—despite it being a fundamental prerequisite for triggering the Fifth Amendment inquiry to which *Edwards* is tied. *See United States v. Roa*, 24 M.J. 297, 299 (C.M.A. 1987) (concluding that the prophylactic *Edwards* rule does not prohibit consent requests, because the Fifth Amendment privilege, and hence *Edwards*, "protects only *testimonial* evidence" (emphasis added)). *Edwards*—like *Miranda v. Arizona*, 384 U.S. 436 (1966)—merely established a procedural safeguard to protect against the admission into evidence of self-incriminating testimony in response to interrogation. Accordingly, *Edwards* established a presumption that such statements, made after a suspect had invoked his right against self-incrimination,

---

[2] The law enforcement officer involved in the exchange with Appellee indicated at trial that to the best of his knowledge, he had no reason to believe that the digital forensic examiner could not unlock Appellee's iPhone.

are compelled, i.e., involuntary. *See Maryland v. Shatzer*, 559 U.S. 98, 106 (2010) ("*Edwards*' presumption of involuntariness has the incidental effect of 'conserving judicial resources which would otherwise be expended in making difficult determinations of voluntariness." (internal brackets omitted) (citation omitted)). The majority starts by arguing that "asking Appellee to *state* his passcode involves more than a mere consent to search; it asks Appellee to provide the Government with the passcode itself, which is incriminating information." *United States v. Mitchell*, __ M.J. __ (7) (C.A.A.F. 2017). However, Appellee declined to state or otherwise speak his passcode to the Government. He declined. There is nothing to suppress there.

The majority goes on to conflate Appellee's non-answer to a question with the later request that he physically unlock his iPhone, and (perhaps) identifies *that* as the Fifth Amendment violation. But there was no testimonial statement or testimonial act to which the Fifth Amendment privilege or *Edwards* could attach. Accordingly, there was no interrogation, no *Edwards* violation, and nothing to suppress as "derived" therefrom pursuant to M.R.E. 305(c)(2). Neither the right against self-incrimination nor *Edwards* is in play in the absence of *testimony* that is "a witness against [oneself]."

II.

Contrary to its understanding of the law[3] the majority does in fact need to show that the entry of the password itself was both testimonial and incriminating to trigger the protections of the Fifth Amendment. *See United States v. Castillo*, 74 M.J. 160, 165 (C.A.A.F. 2015) (" 'To qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating, and compelled.' " (quoting *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 189 (2004))); *Schmerber v. California*, 384 U.S. 757, 761 (1966) ("[T]he privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with

[3] *Mitchell*, __ M.J. at __, __ (8, 9).

evidence of a *testimonial or communicative* nature." (emphasis added)); *see also Doe v. United States*, 487 U.S. 201, 210–11 (1988) (concluding that "certain *acts*, though incriminating, are not within the privilege," because "the suspect was not required to disclose any knowledge he might have, or to speak his guilt" (emphasis added) (citations omitted) (internal quotation marks omitted)). The Fifth Amendment's protections against self-incrimination, and hence *Edwards*, apply only to testimonial communications that are the result of interrogation. *See Fisher v. United States*, 425 U.S. 391, 408 (1976); *Everett v. Sec., Fla. Dept. of Corrections*, 779 F.3d 1212, 1244 (11th Cir. 2015) (concluding, with respect to a DNA request in a post-invocation custodial context, that "[t]he privilege against self-incrimination extends only to compelled *testimonial* communications" (emphasis added)); *see also Roa*, 24 M.J. at 301 (Everett, C.J., concurring in the result) (recognizing that "*Edwards* provides protection only as to interrogation").

Granted, "the distinction between real or physical evidence, on the one hand, and communications or testimony, on the other, is not readily drawn in many cases." *South Dakota v. Neville*, 459 U.S. 553, 561 (1983) (citing *Schmerber*, 384 U.S. at 764). For instance, the Fifth Amendment's protections apply in some instances to an accused who is compelled to produce papers and documents, but never applies to an accused who is compelled to produce a writing sample, undergo fingerprinting, or the withdrawal of blood samples. *See Schmerber*, 384 U.S. at 763–65; *see also Fisher*, 425 U.S. at 408. In this context, the question whether the act of *entering* a passcode into a phone can be testimonial is fairly novel. Some courts have concluded that the fact that a passcode emanates from "mental processes" is enough to deem it testimonial, at least when it is spoken, or the passcode subpoenaed. *See United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); *see also Sec. and Exch. Comm'n v. Huang*, No. 15-269, 2015 U.S. Dist. LEXIS 127853, at *6, 2015 WL 5611644, at *2 (E.D. Pa. Sept. 23, 2015). Other courts have concluded that a telephone passcode is "neither testimonial nor communicative in the Fifth Amendment sense," *Venega*s, 594 F. App'x at 827, or that post-invocation password requests do not violate the

Fifth Amendment, *United States v. Gavegnano*, 305 F. App'x 954, 956 (4th Cir. 2009), or that there is no meaningful distinction between a numeric passcode and a fingerprint passcode in the context of mobile phones—and that neither is testimonial in any event, *see State v. Stahl*, 206 So. 3d 124, 135–36 (Fl. Dist. Ct. App. 2016).

Rather than grapple with a critical point of law, the majority chooses to baldly assert—without citation to any authority—that "those who seek *Edwards* protection *do not need to establish that the interrogation produced or sought a testimonial statement* in order to establish a violation." *Mitchell*, __ M.J. __ (9) (emphasis added). It is simply bizarre to conclude that the Fifth Amendment right against self-incrimination could possibly be implicated where no testimony was forthcoming, i.e., produced. Equally foreign to reason is the ipse dixit notion that *Edwards*, which assumes self-incrimination was compelled—i.e., involuntary, under certain circumstances—has some independent substantive identity absent an incriminating testimonial statement.

The majority's wrongheaded application of *Edwards* appears to transform a prudential prophylactic into a freestanding constitutional right untethered from "bearing witness" against oneself at all. The majority's view that *Edwards* provides a right against "badgering,"[4] whether it results in an incriminating *statement* or not, *see id.*, is a policy judgment divorced from the relevant clause of the Fifth Amendment. That clause plainly states that its purpose is to protect a suspect from being "compelled in any criminal case to be *a witness* against himself." U.S. Const. amend. V; *see also Schmerber*, 384 U.S. at 765; *Doe*, 487 U.S. at 210–11 (recognizing that "certain acts, though

[4] The majority defends their conclusion that an *Edwards* violation exists in the absence of a testimonial statement by stating that the "core [of] the Fifth Amendment" protects against "badgering an unrepresented suspect into granting access to incriminating information." __ M.J. at __ (9). The brevity of the encounter between Appellee and Investigator Tsai, and the former's voluntary act of unlocking his iPhone, cannot seriously be said to support the majority's weighty charge of "badgering."

incriminating, are not within the privilege" and noting that an accused incriminates himself when he "speak[s] his *guilt*" (emphasis added)); *cf. Solem v. Stumes*, 465 U.S. 638, 646 (1984) ("*Edwards* established a bright-line rule to safeguard *pre-existing rights* . . . ." (emphasis added)).

III.

But while the majority must explain how the act of entering an iPhone passcode is in fact testimonial, in response to interrogation, and incriminating, it is sufficient for my purposes to illustrate that the request that Appellee enter his passcode was not "reasonably likely to elicit an *incriminating* response," *Innis*, 446 U.S. at 301 (emphasis added), and therefore not an "interrogation" for the purposes of *Edwards* and the Fifth Amendment. This is not a novel inquiry.

A.

It is well established that an accused is subject to interrogation when law enforcement officers ask questions "reasonably likely to elicit an *incriminating* response from the suspect." *Id.* (emphasis added). An accused incriminates himself—that is, gives an incriminating response—when he makes statements that "support a conviction under a federal criminal statute" or "furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." *United States v. Hubbell*, 530 U.S. 27, 38 (2000) (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951) (quotation marks omitted)). Not all statements are incriminating, and courts have recognized that just as "not all statements made while in custody are the product of interrogation," *Holman v. Kemna*, 212 F.3d 413, 418 (8th Cir. 2000), "not all questioning of in-custody suspects constitutes interrogation." *United States v. Ventura*, 85 F.3d 708, 712 n.5 (1st Cir. 1996).

" 'A request for consent to search does not infringe upon Article 31 or Fifth Amendment safeguards against self-incrimination because such requests are not interrogations and the consent given is ordinarily not a statement.' " *United States v. Hutchins*, 72 M.J. 294, 297 (C.A.A.F. 2013)

(quoting *United States v. Frazier*, 34 M.J. 135, 137 (C.M.A. 1992)). This is true even where the person has invoked and *Edwards* applies. *Cf. United States v. Gonzalez*, Nos. 95-5004, 95-5026, 1995 U.S. App. LEXIS 34730, at *9–10, 1995 WL 729483, at *3 (4th Cir. 1995) (per curiam) (unpublished) (acknowledging *Edwards* but noting that a post-invocation "request to search [defendant's] hotel room does not in and of itself elicit testimonial evidence of guilt"). In this case, the Government had authority to search and seize Appellee's iPhone pursuant to a valid search authorization. While the request that Appellee unlock his iPhone was not a request for consent to search, in this case it resembles "the common-law principle of announcement," which has been recognized as an element of the reasonableness inquiry under the Fourth Amendment. *Wilson v. Arkansas*, 514 U.S. 927, 934–36 (1995). Requesting that Appellee unlock his phone before the Government seeks to unlock it by force is the functional equivalent of "knock and announce," a request that the owner open the door, as opposed to an agent kicking it in. *See generally United States v. Ramirez*, 523 U.S. 65, 73 (1998) (discussing the relationship between property damage during no-knock entries and reasonableness under the Fourth Amendment). A request for access into a phone seized pursuant to a search authorization is plainly not an interrogation, just as a request to open the door to a home prior to executing a search warrant is not an interrogation.

B.

Even without this well-settled law, the request to unlock the iPhone is also not an interrogation because the answer one could reasonably expect—entering the passcode—was not incriminating. It would not itself have served as a directly inculpatory statement expressing Appellee's guilt or supported a conviction under a criminal statute. The passcode would not have been admitted at trial and did not itself "communicate any information about the investigated crime." *Roa*, 24 M.J. at 301 (Everett, C.J., concurring in the result).

Likewise, the act of entering the code conveyed no incriminating facts in the way that providing documents sometimes does. Unlike statements that "authenticat[e] or

identif[y] . . . documents," *see id.*, neither Appellee's passcode nor the fact that he entered it was likely to—or actually did—reveal any incriminating information. At most, the entry of a passcode would reveal, (1) an undisclosed specific number combination with no contextual meaning or weight and (2) an implicit admission that Appellee owned the phone and knew the passcode for it. *Cf. United States v. Apple Mac Pro Computer*, 851 F.3d 238, 248 (3d Cir. 2017); *Gavegnano*, 305 F. App'x at 956.

Here such revelations would have been a foregone conclusion that "add[ed] little or nothing to the sum total of the Government's information." *Hubbell*, 530 U.S. at 44 (quoting *Fisher*, 425 U.S. at 411). Based on the facts of record, it was apparent to all parties that Appellee owned the iPhone: ownership was not in dispute. And it is common sense that a person who owns a phone also knows the passcode and has the capability to use it. "[I]n common experience, the first would be a near truism, and the latter self-evident." *Fisher*, 425 U.S. at 411. The fact that Appellee could unlock his own phone was simply neither testimonial nor incriminating. *See* Brief of Notre Dame Law Students as Amicus Curiae in Support of Appellant, at 14–15, *United States v. Mitchell*, No. 17-0153 (C.A.A.F. Mar. 21, 2017); *Roa*, 24 M.J. at 301 (Everett, C.J., concurring in the result) ("A distinction must be made . . . between granting consent to search property which has already been identified by law-enforcement agents and identifying property for those agents.").[5]

[5] If ownership of the iPhone was in question before the agents asked Appellee to enter his passcode, perhaps this would be a different case. *See* Orin Kerr, *The Fifth Amendment and Touch ID*, Wash. Post: The Volokoh Conspiracy, Oct. 21, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/21/the-fifth-amendment-and-touch-id/?utm_term=.f8926f1eb712 (last visited Aug. 25, 2017) (distinguishing that situation from provision of a passcode to a phone whose ownership is known, a foregone conclusion "that should defeat the [Fifth Amendment] privilege").

Like the Fourth and Fifth Circuits, *cf. Gavegnano*, 305 F. App'x at 956; *Venegas*, 594 F. App'x at 827; the Air Force Court of Criminal Appeals has similarly concluded that a request for a passcode to a phone—whether spoken or physically entered—does not violate the Fifth Amendment. *See, e.g.*, *United States v. Robinson*, No. ACM 38942, 2017 CCA LEXIS 378, at *17–18, 2017 WL 2417746, at *6 (A.F. Ct. Crim. App. May 15, 2017) (holding that a post-invocation passcode request made in conjunction with a request for consent to search was not an interrogation because the passcode was not itself incriminating); *United States v. Blatney*, Misc. Dkt. No. 2016–16, 2017 CCA LEXIS 354, at *10, 2017 WL 2422807, at *4 (A.F. Ct. Crim. App. May 22, 2017) (concluding that because the identity, location, ownership, dominion, and control of a cell phone were not in dispute, the military judge abused her discretion in holding that the request for the phone's passcode constituted an interrogation); *see also United States v. Fricosu*, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (holding the Fifth Amendment did not prohibit a government-compelled production of unencrypted contents of a computer when their existence and location were known); *cf. In re Grand Jury Subpoena (Boucher)*, No. 2:06–mj–91, 2009 U.S. Dist. LEXIS 13006, at *6–10, 2009 WL 424718, at *3–4 (D. Vt. Feb. 19, 2009) (concluding that compelling the production of an unencrypted version of a laptop's hard drive would not "communicate incriminating facts"). *But see Kirschner*, 823 F. Supp. 2d at 669 (quashing subpoena for the password to a computer as a testimonial communication).

IV.

The majority concludes, to the contrary, that an interrogation, and therefore an *Edwards* violation, occurred because Appellee "demonstrated that entry of his passcode was an 'incriminating response,'" i.e., a response that "furnish[ed] a link in the chain of evidence needed to prosecute" Appellee. *Mitchell*, __ M.J. at __, __ (7, 9). The majority's conclusion rests entirely on a naïve misunderstanding of what the phrase "link in the chain," *Hoffman*, 341 U.S. at 486, actually means. The majority interprets the phrase to mean something that it clearly did

not mean in *Hoffman* and has never been read to mean in any legal authority I have found. "Link in the chain" for purposes of the Fifth Amendment simply does not mean "but for."

In *Hoffman*, the government sought a bench warrant for William Weisberg, a witness who failed to appear before a grand jury. *Hoffman*, 341 U.S. at 481, 487. The prosecutor asked Hoffman several questions about Weisberg's whereabouts and Hoffman's communications with Weisberg. *Id.* at 481. For example, the prosecutor asked Hoffman, "When did you last see [Weisberg]?" and "Have you seen [Weisberg] this week?" *Id.* Hoffman invoked his Fifth Amendment privilege and refused to answer. *Id.* The Supreme Court held that Hoffman's answers, though facially neutral, could incriminate Hoffman because they could "establish contacts between [Hoffman] and Weisberg during the crucial period when the latter was eluding the grand jury," thereby "forg[ing] links in a chain of facts imperiling [him] with conviction" for hiding Weisberg. *Id.* at 488. Phrased differently, Hoffman's testimony could have shown that he helped Weisberg hide on his property or shown that he was communicating with, and helping, Weisberg.

The majority uses this language to conclude that Appellee's act of entering his iPhone passcode is a "link in a chain" because it allowed entry to the iPhone, which in turn contained evidence. But *Hoffman* did not purport to expand the scope of the Fifth Amendment to include all non-incriminating statements or acts that might lead investigators to, or provide access to, evidence; it merely recognized that some statements, which are not incriminating on their face, might *themselves* become incriminating when placed in context with other evidence. As the Court in *Hoffman* explained:

> The privilege afforded not only extends to *answers* that would *in themselves* support a conviction . . . but likewise embraces *those* which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime . . . . [I]f the witness, upon interposing his claim, were required to prove the hazard in the sense in which a claim is usually required to be established in court,

> he would be compelled to surrender the very protection which the privilege is designed to guarantee. To sustain the privilege, it need only be evident from the implications of the question, in the setting in which it is asked, that a responsive answer to the question or an explanation of why it cannot be answered might be dangerous because injurious disclosure could result.

Id. at 486–87 (emphasis added). *Hoffman* merely extended the protections of the Fifth Amendment to those statements that were not facially inculpatory, but could be read, in context, to incriminate the accused. Likewise, in the case that *Hoffman* cited for the "link in the chain" language, *Blau v. United States*, the Court observed:

> [Petitioner] was asked several questions concerning the Communist Party of Colorado and her employment by it. . . .
>
> [S]he reasonably could fear that criminal charges might be brought against her if she admitted employment by the Communist Party or intimate knowledge of its workings. *Whether such admissions by themselves would support a conviction under a criminal statute is immaterial.* Answers to the questions asked by the grand jury would have furnished a link in the chain of evidence needed in a prosecution of petitioner for violation of (or conspiracy to violate) the Smith Act.

340 U.S. 159–61 (1950) (emphasis added) (footnote omitted). In both *Blau* and *Hoffman*, the Court contrasted facially incriminating answers with answers that were not facially inculpatory, but could have been used as "evidence . . . to prosecute." *Hoffman*, 341 U.S. at 486. As noted previously, the passcode itself is clearly not "evidence" in this case, and neither is Appellee's act of unlocking his iPhone. Rather, it is the contents stored on the iPhone itself that revealed facts related to the criminal investigation and the Government had a lawful authorization to search and seize those contents.[6]

[6] In executing the search authorization, law enforcement did not ask Appellee anything about the contents of his iPhone, let

Appellee's act of entering his password into his iPhone gave law enforcement immediate access to its contents; but the Supreme Court has clearly held that provision of access to evidence is not necessarily "incriminating" under the Fifth Amendment. In *Doe*, for example, the accused invoked his Fifth Amendment privilege "[w]hen questioned about the existence or location of additional records" of his overseas bank records. 487 U.S. at 202–03. The government sought a court order requiring the accused to sign twelve forms consenting to the disclosure of records relating to overseas bank accounts that the government "knew or suspected that Doe had control" over. *Id.* at 203. The *Doe* Court concluded that these forms did not implicate the Fifth Amendment privilege, because, although the answers gave the government "*access* to a potential source of evidence," they did not themselves "point the Government toward hidden accounts" or "provide information that w[ould] assist the prosecution in uncovering evidence." *Id.* at 215 (emphasis added). Similarly here, Appellee's entry of his passcode merely provided access to a device already known to—indeed in the possession of—law enforcement.

V.

In this case the majority has inexplicably, and without a textually principled explanation, wandered far from the core principles the Fifth Amendment and *Edwards* were intended to protect. This gratuitous expansion of the scope of the Fifth Amendment privilege will necessarily tear at the logical contours of the Fourth Amendment.[7] How can we

---

alone the files, photos, or applications he stored on his iPhone. Nor did they ask Appellee to pinpoint where particular files or photos were located. *See United States v. Green*, 272 F.3d 748, 752 (5th Cir. 2001) (law enforcement violated suspect's rights under *Edward* and *Miranda* when they asked suspect to disclose the location of his firearms and open cases that he had identified as containing firearms because this amounted to custodial interrogation).

[7] The majority's purported discovery of an *Edwards* violation absent either a "statement" or an "interrogation" undeniably leads us down a lawless and reckless path, the effects of which will be felt immediately in this Court's review of *United States v. Blatney*,

reasonably explain that the government may lawfully obtain authorization to seize and search a phone, lawfully "break into" that phone independent of Appellee's cooperation after it is seized, but cannot first request that Appellee furnish access?

It is difficult to say how the majority's expansive ruling will work in practice. If we were dealing with a house rather than an iPhone, and had Appellee unlocked the door to his home following a request from law enforcement executing a warrant, would the majority similarly conclude that the request to open the door was an interrogation and the affirmative action an incriminating statement because it provided the government with quicker access to that home than if they had attempted to break down the door?

At bottom, this was a reasonable search and seizure conducted pursuant to a valid search authorization. The Government did not violate Appellee's legal rights either when it asked Appellee for his iPhone passcode (which he declined to provide) or when it asked him to enter his iPhone passcode. Even assuming the majority can explain how this latter act of inputting a passcode was itself testimonial, the request was not "reasonably likely to elicit an incriminating response from the suspect," *Innis*, 446 U.S. at 301, nor did it in fact do so. Therefore, Appellee was not subjected to interrogation in violation of *Edwards* or M.R.E. 305(c)(2).[8] I respectfully dissent.

No. 17-0485 (C.A.A.F. Aug. 10, 2017) (order granting review), and *United States v. Robinson*, No. 17-0504 (C.A.A.F. Aug. 18, 2017) (order granting review).

[8] I also note that the majority oddly suggests that the facts of this case somehow "extend[] beyond a mere consent to search" and that therefore our decision in *United States v. Hutchins* is inapplicable. *Mitchell*, __ M.J. at __ (8). On the contrary, the facts of *Hutchins* are instructive. There, the accused was kept in solitary confinement for a week, deprived of a lawyer despite a request for one, and the investigator admitted that he reinitiated contact to further the investigation. *See Hutchins*, 72 M.J. at 296–98. This contact, unlike the instant case, *resulted in an incriminating statement*. Clearly, under some circumstances, a request for con-

sent to search may conceal an unlawful attempt to coax incriminating information out of an accused, as in *Hutchins*. Those circumstances are not present here.