

UNITED STATES ARMY COURT OF CRIMINAL APPEALS

Before
CAMPANELLA, SALUSSOLIA, and CELTNIIEKS
Appellate Military Judges

UNITED STATES, Appellee
v.
Warrant Officer One GRAHAM H. SMITH
United States Army, Appellant

ARMY 20160150

Headquarters, Fort Rucker
Deidra J. Fleming, Military Judge
Lieutenant Colonel Andras M. Marton, Staff Judge Advocate

For Appellant: Bryan D. DePowell, Esquire (argued); Captain Daniel C. Kim, JA;
Bryan D. DePowell, Esquire (on brief).

For Appellee: Captain Meredith M. Picard, JA (argued); Major Michael E. Korte,
JA; Captain Meredith M. Picard, JA (on brief); Colonel Tania M. Martin, JA; Major
Michael E. Korte, JA; Captain Meredith M. Picard, JA (on brief in response to
specified issues).

28 February 2018

OPINION OF THE COURT

SALUSSOLIA, Judge:

In this case, appellant asserts for the first time that the military judge abused her discretion by not granting his suppression motion. We hold the asserted error was waived, and that even if not waived, the good faith exception to the exclusionary rule would apply because the law enforcement officers who seized and conducted the digital forensic examination of appellant's computer and Apple iPhone (iPhone) reasonably relied on a military magistrate's authorizations.

A military judge sitting as a general court-martial convicted appellant, contrary to his plea, of indecent recording in violation of Article 120c, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 920c (2012 & Supp. I 2014). The convening authority approved the adjudged sentence of a dishonorable discharge and confinement for two months.

We review this case under Article 66, UCMJ. Appellant raises four assignments of error, one of which requires discussion, none of which merit relief. Upon consideration of the assignment of error “the military judge abused her discretion by denying the defense motion to suppress evidence obtained from [appellant’s] cellular telephone because [the] evidence was obtained in violation of the Fourth Amendment of the United States Constitution and Military Rule of Evidence 311,” this court specified additional issues pertaining to the lawfulness of the government’s search and seizure.

BACKGROUND

A. Report to Law Enforcement

On 15 July 2014, while shopping at the post commissary, Ms. JW noticed appellant walking closely alongside her. Ms. JW then observed appellant crouch down next to her and take a photograph aimed underneath her dress, using his iPhone. Quickly reacting, Ms. JW attempted to confront appellant and yelled for assistance. Appellant ran towards the exit of the commissary, but was blocked by a senior noncommissioned officer (NCO). Having observed some of the interaction between Ms. JW and appellant and seeing appellant fumbling with his iPhone, the senior NCO took the iPhone from appellant—to prevent appellant from further accessing it—and turned appellant’s iPhone over to military police upon their arrival to the commissary.

B. The Search and Seizure

Based on the report from Ms. JW, Military Police Investigator (Investigator) Kessler contacted the part-time military magistrate, Major (MAJ) Farmer, from whom he sought and obtained verbal authorization to search appellant’s iPhone for photographs.

After appellant was released from custody, Investigator Kessler sought authorization to search appellant’s residence for Apple brand digital devices containing the nonconsensual pictures of a person’s private area. Investigator Kessler’s affidavit in support of the authorization stated, in relevant part:

based on technology and capability built in to Apple [p]roducts, known as the iCloud we have reason to believe any pictures taken with [appellant’s] iPhone have been synchronized wirelessly with the iCloud allowing them to be synchronized with all Apple products linked to Smith’s Apple account. In addition those items can be accessed by the internet to be viewed and/or distributed to other parties electronically.

During a telephonic briefing with the military magistrate, Investigator Kessler discussed the basis for the follow-on search request for other digital devices. He stated based on his investigative experience and knowledge of Apple technology, appellant's iPhone had the capability to be automatically linked with the iCloud. He opined that photographs or videos taken of Ms. JW could be accessed by other Apple devices and maintained or further distributed. The military magistrate asked if only Apple devices could access the iCloud. Investigator Kessler said no, other devices could access the iCloud as well. Based on this information, the military magistrate provided authorization to search for any electronic devices that could access the iCloud and obtain the sought images taken by appellant's iPhone. Investigator Kessler searched appellant's residence and seized several digital devices to include three computers, an iPad, and a digital camera.¹

A few weeks later, the Fort Rucker office of U.S. Army Criminal Investigation Command (CID) assumed investigative responsibility for the case and took possession of appellant's iPhone and the digital devices seized from his residence. In reviewing the first authorization, Special Agent (SA) Howell believed it provided authority to seize, but not search, the devices. As a result, he obtained a second authorization from the same military magistrate so the devices could be sent to Fort Benning's CID office for a digital forensic examination (DFE). In obtaining the second authorization, SA Howell relied on the same information Investigator Kessler had provided for the first authorization.

Pursuant to the military magistrate's search authorizations, SA Pugliese, Fort Benning CID office, conducted a DFE of all digital devices. Special Agent Pugliese found no evidence of criminal activity on the digital devices obtained from appellant's residence. Because appellant's iPhone was password-protected and locked, SA Pugliese used a computer seized from appellant's residence to unlock it.²

Once he unlocked the iPhone, SA Pugliese used forensic software to extract data on the phone and search portions of the data that were within the search parameters to which he believed he had authorization to search in light of the authorizations and the lab request. Special Agent Pugliese's subsequent examination of appellant's iPhone identified eight "up-skirt" videos involving Ms. JW and an unknown female while they shopped at the commissary.

¹ The military magistrate later reduced her oral search authorization provided to Investigator Kessler to writing in December 2014.

² When the iPhone was connected to the computer, the devices were set to trust each other and allow communication back and forth. Special Agent Pugliese used the link between the laptop and iPhone to unlock the iPhone.

C. The Suppression Motion

At trial, appellant moved the court to suppress the eight videos found on his iPhone. In appellant's written motion, he asserted two distinct grounds for suppression. First, the senior NCO's actions in relieving appellant of his iPhone constituted an unlawful seizure under both the Fourth Amendment and Military Rule of Evidence (Mil. R. Evid.) 311. Second, the search of the digital devices seized from appellant's residence was not based on probable cause and thus any evidence obtained from these devices should be suppressed.

At the suppression hearing, in response to the military judge's inquiry, appellant clarified the specific grounds for his motion to suppress focusing only on the iPhone. He challenged the seizure of the iPhone by MSG Clark as unlawful and the subsequent authorization to search the iPhone as too broad—requiring the eight videos obtained from the phone be suppressed. At no time during the initial suppression hearing, did appellant challenge the search of the iPhone because it was opened by a computer illegally seized from appellant's residence.

The military judge initially granted appellant's motion to suppress videos obtained from appellant's iPhone, finding the government did not meet its burden by a preponderance of the evidence under Mil. R. Evid. 311. The government then sought reconsideration of the military judge's motion, which was granted. The government called additional witnesses and introduced evidence of the search.

During reconsideration, appellant appeared to concede the lawfulness of the seizure of the iPhone, but again challenged the search of the phone arguing it was overbroad and lacking in particularity. Although appellant knew the digital forensic examiner used one of appellant's computers to open the phone, he again never challenged the search of the iPhone based on this fact.

After receiving additional evidence, the military judge denied appellant's motion to suppress concluding even if the authorizations were "deemed deficient," and the scope of the search on the iPhone too broad, the government met its burden by a preponderance of the evidence that the seized videos were obtained by officials who reasonably, and with good faith, relied on the issuance of an authorization to search and seize. In the alternative, she found the seized evidence would have been obtained under the inevitable discovery doctrine.

D. New Ground for Suppression Raised for the First Time on Appeal

On appeal, appellant concedes the seizure of the iPhone and the scope of the actual search of it was proper. Appellant, however, now asserts the military judge abused her discretion by denying his motion to suppress, relying on a new theory raised for the first time on appeal. Appellant now argues that since his iPhone was

locked and not otherwise accessible, but for a computer illegally seized from his home, the eight videos obtained from the iPhone represent fruit of an illegal search and therefore should have been suppressed.³ We disagree.

LAW AND DISCUSSION

A. *Standard of Review*

We review a military judge’s denial of a motion to suppress for an abuse of discretion. *United States v. Hoffmann*, 75 M.J. 120, 124 (C.A.A.F. 2016).

B. *Waiver*

Before confronting the merits of the asserted error, we first look to whether appellant waived this new ground for suppression by failing to raise it at trial.

If an appellant makes a timely motion to suppress, evidence deemed inadmissible as a result of an unlawful search and seizure may not be received in evidence. Mil. R. Evid. 311(a). If the defense moves to suppress evidence, the prosecution has the burden of establishing that the evidence is admissible by a preponderance of the evidence. Mil. R. Evid. 311(d)(5)(A). A military judge may require the defense to state specifically the grounds upon which the defense moves to suppress evidence. Mil. R. Evid. 311(d)(3). In that circumstance, the burden upon the prosecution extends only to the grounds upon which the defense moved to suppress the evidence. Mil. R. Evid. 311(d)(5)(C). Failure to object or to move to suppress constitutes waiver. *See* Mil. R. Evid. 311(d)(2); Rule for Courts-Martial (R.C.M.) 905(e).⁴

In this case, the appellant did more than merely object or generally move to suppress the evidence. Rather, he specifically stated the grounds for his motion in

³ At oral argument, when asked “How can we now review the judge’s non-decision for an abuse of discretion when she never made a decision because you never raised the ground?” appellant’s counsel responded, “our case was prior to [*United States v. Nieto* [76 M.J. 103, 108 (C.A.A.F. 2017)]], so obviously looking at *Nieto* and looking at CAAF’s position on this it helped clarify my position.”

⁴ As a general rule, federal appellate courts do not review issues not decided in the trial court. *Singleton v. Wulff*, 428 U.S. 106, 120 (1976); *Hormel v. Helvering*, 312 U.S. 552, 556 (1941). The logic behind the rule is obvious—an appellate court can only properly review matters that have been adequately developed in the record of trial.

both a detailed written motion and a response to the government’s request for reconsideration. At the suppression hearing, in response to the military judge’s inquiry, appellant narrowed the grounds upon which he sought to suppress the evidence at issue—the eight videos. Appellant did not at any time during the trial assert the ground he now asserts on appeal.

There are two ways to view appellant’s failure, both arriving at the same result. First, appellant’s failure to raise this theory of suppression to the military judge waived the issue. *United States v. Ahern*, 76 M.J. 194, 197 (C.A.A.F. 2017); Mil. R. Evid 311 (d)(2)(A); R.C.M. 905(e). Alternatively, by failing to articulate this specific ground for relief, the burden never shifted to the government. As such, the military judge did not err as a matter of law because the defense failed to meet its burden when the matter was never brought to the attention of the military judge.

While this court may notice an issue not raised at trial, we decline appellant’s invitation to address his new ground for suppression. Even if we were to address this new ground for suppression, we find the government would still prevail based on the good faith exception.

C. Good Faith Exception

If a military magistrate did not have a substantial basis to find probable cause in a specific case, military courts ordinarily apply the exclusionary rule unless an exception to the rule applies. *See* Mil. R. Evid. 311(a).⁵ In this case, while the government concedes no substantial basis for probable cause existed to seize appellant’s laptop, the government argues that law enforcement acted in good faith in seizing the device.⁶ We agree.

⁵ The exclusionary rule is “‘a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.’” *United States v. Leon*, 468 U.S. 897, 906 (1984) (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). The Supreme Court has recognized that the exclusionary rule “cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity.” *Id.* at 918-19. This has become known as the good faith exception to the exclusionary rule.

⁶ Appellant argues that the magistrate did not have a substantial basis to conclude that probable cause existed when she issued the search authorization of appellant’s residence for the digital devices, to include computers, that possibly contained evidence of the offense of photographing or videoing Ms. JW, therefore, the search authorization was invalid. The government concedes the magistrate did not have a

(continued . . .)

The good faith exception to the exclusionary rule is applicable when investigators “act with an objectively ‘reasonable good faith belief’ that their conduct is lawful.” *Davis v. United States*, 564 U.S. 229, 238 (2011) (citing *Leon*, 468 U.S. at 909). The test is “whether a reasonably well-trained officer would have known that the search was illegal” in light of “all of the circumstances.” *Herring v. United States*, 555 U.S. 135, 145 (2009) (citing *Leon*, 468 U.S. at 922, n. 23). This standard takes into account the officer’s training and experience, but not his or her subjective intent. *Id.* at 145-46. The good faith exception applies to conduct involving only “simple, isolated negligence,” but not to conduct amounting to a deliberate, reckless, or grossly negligent disregard of Fourth Amendment rights.” *Davis*, 564 U.S. at 238. The good faith exception recognizes that the exclusionary rule “cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity.” *Leon*, 468 U.S. at 918-19. The exclusionary rule “is designed to deter police misconduct rather than to punish the errors of judges and magistrates” who “as neutral judicial officers . . . have no stake in the outcome of particular criminal prosecutions,” so “[t]he threat of exclusion thus cannot be expected significantly to deter them.” *Id.* at 916-17.

The President, exercising his authority under Article 36, UCMJ, promulgated a military good faith exception rule. Evidence obtained as a result of an unlawful search or seizure may be used if:

- (A) The search or seizure resulted from an authorization to search, seize or apprehend issued by an individual competent to issue the authorization under Mil. R. Evid. 315(d) or from a search warrant or arrest warrant issued by competent civilian authority;
- (B) The individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause; and
- (C) The officials seeking and executing the authorization or warrant reasonably and with good faith relied on the issuance of the authorization or warrant. Good faith is to be determined using an objective standard.

Mil. R. Evid. 311(c)(3).

(. . . continued)

substantial basis for concluding that probable cause existed to search appellant’s residence for such digital devices. We accept this concession.

Military Rule of Evidence 311(c)(3) embodies the good faith exception as articulated in *Leon* and *Massachusetts v. Sheppard*, 468 U.S. 981 (1984), which specifically address the scenario when law enforcement officers rely on a subsequently invalidated search warrant. *United States v. Carter*, 54 M.J. 414, 421 (C.A.A.F. 2001).

The government has the burden of proving, by a preponderance of the evidence, the requirements of the good faith exception have been met. Mil. R. Evid. 311(d)(5). Here, the military magistrate possessed authority to issue a search authorization. We now turn to the second and third requirements.

In finding the government met prong (B) of Mil. R. Evid. 311(c)(3), we look to *Carter*, where our superior court determined that with respect to prong (B) of Mil. R. Evid. 311(c)(3), the phrase “substantial basis” does not have the same meaning as the term “substantial basis” in *Illinois v. Gates*, 462 U.S. 213, 238 (1983).⁷ 54 M.J. at 421. Rather, “substantial basis” as an element of good faith “is satisfied if the law enforcement official has an objectively reasonable belief that the magistrate had a ‘substantial basis’ for determining the existence of probable cause.” *Id.* at 422.

Here, Investigator Kessler provided a detailed affidavit to support his request to search appellant’s residence for other digital devices that could have accessed the iCloud and retrieved evidence of the videos. We do not find the military magistrate abdicated her role. She discussed the request at length with Investigator Kessler and questioned the basis for his conclusions and limited the scope of his search. Moreover, we find no evidence that Investigator Kessler provided or omitted information in an attempt to mislead the magistrate. Based on this exchange, an objectively reasonable law enforcement official executing the authorized search would have believed the military magistrate had a substantial basis for determining

⁷ In *United States v. Nieto*, 76 M.J. 103, 108 (C.A.A.F. 2017), our superior court noted a tension in their analysis of prong (B) of the good faith doctrine in *Carter* and *Hoffmann*. 76 M.J. at 108 n.6. The tension arises because in *Carter*, the court’s determination of whether this prong was met focused on whether law enforcement officials had a reasonable belief that the magistrate had a substantial basis for determining the existence of probable cause. *Carter*’s approach to the good faith exception is consistent with the Supreme Court’s application of the exception in *Leon* and *Herring*. Although not overruling *Carter*, the court in a subsequent decision, *Hoffmann*, focused on the issuer (i.e., the magistrate) having a substantial basis for concluding the existence of probable cause. 75 M.J. at 125. Because *Carter* has not been overruled, is consistent with the Supreme Court’s application of the good faith exception, and gives purpose to Mil. R. Evid 311(c)(3), we follow its approach in analyzing prong (B).

probable cause with respect to a search for digital devices capable of linking to the iCloud.

With respect to prong (C) of Mil. R. Evid. 311(c)(3), we also find the government has met its burden because the official seeking and executing the authorization that resulted in the seizure of the computer acted reasonably. Investigator Kessler not only sought the search authorization, but also limited his search of appellant's residence to the parameters of the magistrate's verbal authorization. Thus, we hold the computer used to open the iPhone was seized in good faith.

We also find that SA Pugliese acted in good faith when he conducted a search of the computer although it revealed no evidence at issue in this case. Lastly, we find nothing unlawful in SA Pugliese's reliance on his technological acumen to use the laptop as a "key" to open the locked iPhone. We, therefore, conclude the eight videos obtained from appellant's iPhone were not tainted as a result of an unlawful search and were otherwise admissible.

CONCLUSION

The findings and sentence are AFFIRMED.

Senior Judge CAMPANELLA and Judge CELTNIKS concur.



FOR THE COURT:

A handwritten signature in black ink, appearing to read "Malcolm H. Squires, Jr.", written in a cursive style.

MALCOLM H. SQUIRES, JR.
Clerk of Court