UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES
Appellant

v.

Justin A. GURCZYNSKI, Private
United States Army, Appellee

No. 17-0139
Crim. App. No. 20160402

Argued March 15, 2017—Decided July 24, 2017

Military Judges: Jeffery R. Nance

For Appellant: *Captain Tara O'Brien Goble* (argued); *Colonel Mark H. Sydenham, Lieutenant Colonel A. G. Courie III,* and *Captain Samuel E. Landes* (on brief); *Captain Carling M. Dunham*.

For Appellee: *Captain Cody Cheek* (argued); *Colonel Mary J. Bradley, Lieutenant Colonel Christopher D. Carrier*, *Captain Joshua B. Fix, Captain Ryan T. Yoder,* and *Captain Scott Ashby Martin* (on brief); *Major Christopher D. Coleman.*

Amicus Brief for Appellant: *Colonel Valerie C. Danyluk*, USMC, and *Lieutenant Commander Justin C. Henderson*, JAGC, USN (on brief) for Navy-Marine Corps Appellate Government Division.

Judge RYAN delivered the opinion of the Court, in which Chief Judge ERDMANN, and Judges STUCKY, OHLSON, and SPARKS, joined.

Judge RYAN delivered the opinion of the Court.

It is unlikely that the Government would argue it is constitutionally reasonable to search a home based on a warrant previously issued for a crime the homeowner had already been convicted of, and to also direct the searchers to look for evidence of offenses not named in the warrant. In this case, however, the Government asserts the right to do just that, but for a portable hard drive (thumb drive) rather than a home. We recognize the differences between a home and a thumb drive and the unique challenges in applying

the Fourth Amendment in a digital context. *See generally* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J. Crim. L. 112 (2011); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005). But the Fourth Amendment compels us to treat them the same in this case. We hold that the military judge did not abuse his discretion in concluding that evidence of an offense not named in the warrant was outside the scope of the warrant and must be suppressed. Furthermore, based on the facts found by the military judge, we conclude, as a matter of law, that the search was not constitutionally reasonable under the particular circumstances of this case. Accordingly, we affirm the United States Army Court of Criminal Appeals (ACCA).

I. FACTS AND PROCEDURAL HISTORY

On June 19, 2014, a military judge sitting as a general court-martial convicted Appellee, consistent with his pleas, of one specification of making a false official statement, in violation of Article 107, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 907 (2012). The military judge convicted Appellee, contrary to his pleas, of two specifications of taking indecent liberties with a child and two specifications of abusive sexual contact with a child, in violation of Article 120, UCMJ, 10 U.S.C. § 920 (2006).[1] The military judge sentenced Appellee to a bad-conduct discharge, confinement for forty months, forfeiture of all pay and allowances, and a reduction to the grade of E-1. The convening authority approved the sentence as adjudged. The ACCA dismissed one specification of taking indecent liberties with a minor and affirmed the remaining findings of guilty and the sentence following a sentence reassessment. *United States v. Gurczynski*, No. ARMY 20140518, 2016 CCA LEXIS 530, 2016 WL 4547640 (A. Ct. Crim. App. Aug. 31, 2016).

Five months after Appellee's conviction for these charges, the digital forensic examiner (DFE), relying on a warrant

[1] Probable cause to search Appellee's devices for evidence of abusive sexual contact does not, without more, provide probable cause to search the devices for evidence of child pornography. *See United States v. Hoffmann*, 75 M.J. 120, 126–28 (C.A.A.F. 2016).

issued to search electronic media for these charges, searched Appellee's thumb drive with a direction to find evidence of child pornography, an offense not mentioned in either the warrant or the supporting affidavit. We adopt the facts relevant to the issues before us as set forth in the ACCA's opinion:

> The charges against [Appellee] are premised on child pornography discovered during a digital forensic examination (DFE) of a thumb drive and hard drive seized on 24 January 2014 by the Army Criminal Investigation Command (CID) from [Appellee]'s residence pursuant to a warrant. CID's investigation stemmed from allegations [Appellee] sexually abused a child. At trial, defense counsel moved under [Military Rule of Evidence (M.R.E.)] 311 to suppress the evidence on the thumb drive and a computer hard drive on the basis that CID exceeded the scope of the warrant during the DFE. The military judge granted the motion upon determining CID obtained the evidence by conducting an unlawful search and seizure in violation of the Fourth Amendment to the United States Constitution and [M.R.E.] 311.
>
> In granting the defense motion to suppress, the military judge made detailed findings of fact concerning the scope of the warrant and the search actually conducted, which we briefly summarize here.
>
> First, the military judge found the warrant obtained by CID to search [Appellee]'s residence allowed agents to search for computers and associated peripheral devices for evidence of "attempted sexual abuse of a child, abusive sexual contact with a child and other offenses related" to the allegations against [Appellee]. The warrant authorized CID to search items seized for evidence [Appellee] used the devices to communicate with the alleged victim of his abuse in order to arrange the meeting where [Appellee] ultimately engaged in indecent acts and sexual contact with the child.
>
> Second, a little over a month after the search of [Appellee]'s residence, CID Special Agent (SA) JT sent the thumb drive and other seized digital items to the Digital Forensics Lab at the Fort Lewis, Washington CID office for the DFE. The items were accompanied by a DD Form 2922, Forensic Labora-

tory Examination Request, with instructions that the DFE search the thumb drive for "child pornography or correspondence" with the alleged victim. The request specified that other digital items seized should be searched for child pornography and e-mails, online chats, online messages, and other forms of communication between [appellee] and the alleged victim.

Third, when SA CP opened the thumb drive during the DFE, he saw several file names of videos normally associated with child pornography, as well as a photo of [Appellee]. SA CP, suspecting the video files contained child pornography, and without obtaining a new or expanded search warrant, opened one of the files and concluded, based on his professional experience, that it was child pornography. After that, SA CP searched other media seized from [Appellee]'s home and found additional child pornography on a computer hard drive.

Fourth, SA CP, relied upon both the DA Form 2922 and the search warrant in determining the scope of the DFE he conducted.

Based on these facts, the military judge concluded CID exceeded the scope of the warrant in searching the thumb drive and granted [Appellee]'s motion to suppress the child pornography found on the thumb drive and computer hard drive. First, the military judge found CID had probable cause within the meaning of [M.R.E.] 315(f) and a valid warrant to search for communications. Noting that search warrants must be specific, the military judge found the same was not true for child pornography because nothing in the warrant or supporting affidavit mentioned anything "even closely approximating evidence of child pornography." *See United States v. Carey*, 172 F.3d 1268 (10th Cir, 1999). In this respect, the DA Form 2922, relied upon by SA CP, impermissibly expanded on the scope of the warrant. The military judge also noted the nature of the charges, given their plain statutory meaning, did not remotely contemplate the possession, creation or distribution of child pornography. Second, to search for child pornography upon seeing the video files, SA CP was required to obtain a new or expanded warrant. *See U.S. v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001). Third, the military judge determined that the inevitable discovery doc-

> trine set forth in [M.R.E.] 311(c)(2) did not apply since CID did not have probable cause to search for child pornography in the first instance. *See United States v. Hoffmann*, 75 M.J. 120, 127 ("Without probable cause, the inevitable discovery doctrine fails.").

United States v. Gurczynski, No. ARMY 20160402, 2016 CCA LEXIS 541, at *1–5, 2016 WL 4708565, at *1–2 (A. Ct. Crim. App. Sept. 6, 2016) (footnote omitted).

The Government appealed the ruling pursuant to Article 62, UCMJ, 10 U.S.C. § 862 (2012), and the ACCA affirmed the military judge's ruling. After affirming the military judge's conclusion that the Government exceeded the scope of the warrant by searching the thumb drive for child pornography, the ACCA declined to apply the plain view and inevitable discovery doctrines, reasoning that exceptions to the warrant requirement cannot apply in the absence of probable cause to search in the first instance. 2016 CCA LEXIS 541, at *5 n.3, 2016 WL 4708565, at *2 n.3 (citing *Hoffmann*, 75 M.J. at 127). The ACCA also denied the Government's motion for en banc reconsideration.

The Judge Advocate General of the Army then certified the following issue, pursuant to Article 67(a)(2), UCMJ, 10 U.S.C. § 867(a)(2) (2012):

> Whether the military judge erred in suppressing evidence of child pornography a digital forensic examiner discovered during a search for Appellee's communications with a child victim.

Following oral argument, we ordered that the parties file additional briefs on the following issue:

> The Fourth Amendment prohibits unreasonable searches. Was the search of [Appellee']s thumb drive unreasonable, despite being executed pursuant to a facially valid warrant, in light of the facts that: 1) [Appellee] was convicted of the offense for which the search warrant was issued five months prior to the search; and 2) over nine months had passed between the issuance of the search warrant and the digital examination of the seized devices?

II. DISCUSSION

"In an Article 62, UCMJ, appeal, this Court reviews the military judge's decision directly and reviews the evidence in the light most favorable to the party which prevailed at trial." *United States v. Henning*, 75 M.J. 187, 190–91 (C.A.A.F. 2016) (internal quotation marks omitted) (quoting *United States v. Buford*, 74 M.J. 98, 100 (C.A.A.F. 2015)). "We review a military judge's ruling on a motion to suppress for abuse of discretion." *Id.* at 191 (internal quotation marks omitted) (citations omitted). "In reviewing a military judge's ruling on a motion to suppress, we review factfinding under the clearly-erroneous standard and conclusions of law under the de novo standard." *Id.* (internal quotation marks omitted) (citation omitted). When an appeal presents a mixed question of law and fact, a military judge abuses his discretion if his findings of fact are clearly erroneous or his conclusions of law are incorrect. *See Buford*, 74 M.J. at 100.

The Government argues that the search was constitutionally reasonable because it was conducted pursuant to a facially valid warrant, regardless of the status of the offenses for which it was issued, and that the child pornography uncovered by the DFE is admissible under the plain view exception. We disagree.

At bottom, we find reliance on the warrant to justify the search for child pornography constitutionally unreasonable under the circumstances. First, Appellee had already been convicted of the offenses for which the warrant was issued. Second, the warrant and supporting affidavits did not mention child pornography. Third, SA JT nonetheless directed the DFE to search for child pornography. We focus on one of the military judge's observations in particular:

> On this point it is interesting to note that when SA [T] sent [the] 2922 to [P] he listed Child [sic] pornography first in both places where he explained to the DFE what he should be looking for. The communications between the accused and the victim that were the real object of the investigation almost appear as an afterthought in the request. The court will not speculate as to the reason for this change of course as there is no evidence to explain it. The court simply notes that this is troubling as it im-

> properly oriented DFE [P] outside the parameters of the warrant.

It is clear that it was constitutionally unreasonable to execute a search warrant oriented in such a manner to discover evidence of an offense not mentioned in the warrant nine months after the issuance of the warrant and five months after Appellee's conviction for the offenses that *were* mentioned in the warrant.

A.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "That Amendment grew out of colonial opposition to the infamous general warrants known as writs of assistance, which empowered customs officers to search at will, and to break open receptacles or packages, wherever they suspected uncustomed goods to be." *Payton v. New York*, 445 U.S. 573, 608 (1980) (citations omitted). At the epicenter of the panoply of rules intended to effectuate protection against "dragnet searches for evidence of any crime," Kerr, *supra* p. 2, at 536, are the requirements that a search warrant must: (1) be based on probable cause; (2) be supported "by Oath or affirmation"; and (3) "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. But "[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness.' " *Kentucky v. King*, 563 U.S. 452, 459 (2011) (alteration in original) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)).

"Searches conducted after obtaining a warrant or authorization based on probable cause are presumptively reasonable whereas warrantless searches are presumptively unreasonable unless they fall within a few specifically established and well-delineated exceptions." *Hoffmann*, 75 M.J. at 123–24 (internal quotation marks omitted) (quoting *United States v. Wicks*, 73 M.J. 93, 99 (C.A.A.F. 2014)). While a warrant makes a search presumptively reasonable, a warrant "does not guarantee the constitutionality" of a search "or relieve the Government of the burden of establishing that the warrant did not authorize an unreasonable

search." *United States v. Smeal*, 23 C.M.A. 347, 350, 49 C.M.R. 751, 754 (1975); *see also Camara v. Municipal Court of San Francisco,* 387 U.S. 523, 539 (1967) ("The warrant procedure is designed to guarantee that a decision to search private property is justified by a reasonable government interest. But reasonableness is still the ultimate standard."). To assess whether a search is reasonable, we must assess, "on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014) (internal quotation marks omitted) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

In the absence of some exception to the warrant requirement, to allow the seizure of objects not particularly described in the warrant would violate the "familiar principle . . . that no amount of probable cause can justify a warrantless search or seizure." *Coolidge v. New Hampshire*, 403 U.S. 443, 468 (1971); *see also Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Searches conducted pursuant to a warrant are necessarily limited in scope, thus preventing a general rummaging about. *See Ashcroft v. al-Kidd*, 563 U.S. 731, 742 (2011) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)); *see also Stanford*, 379 U.S. at 485–86 ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." (internal quotation marks omitted) (citation omitted)).

B.

Given the amount of time that passed between the issuance and execution of the warrant, the fact that Appellee had already been convicted of the offenses for which the warrant had been issued, and the Government's instruction, in fact orientation, to the DFE to venture beyond the scope of the warrant, we conclude that the Government had no legitimate interest in executing the search warrant and searching Appellee's thumb drive.

We are well aware that neither the Fourth Amendment nor the Federal Rules of Criminal Procedure impose deadlines for the digital examination of seized devices, nor did this specific warrant specify any deadline. But the constitu-

tional principle of reasonableness necessarily bears some relation to the scope of the warrant, the execution of the search warrant, and the timing of the search. *See United States v. Ramirez*, 523 U.S. 65, 71 (1998); *United States v. Jacobsen*, 466 U.S. 109, 124 (1984). Even in the absence of a time limit, the government "nevertheless remains bound by the Fourth Amendment to the extent that all seizures must be reasonable in duration." *United States v. Cote*, 72 M.J. 41, 44 n.6 (C.A.A.F. 2013). Therefore, the extraordinary length of time between the issuance of the warrant and the digital examination of the thumb drive—over nine months—has some bearing on the question whether the search was constitutionally reasonable.

More important than the mere passage of time, however, is the fact that Appellee had already been convicted of the offenses specified in the warrant. Simply put, the Government had no legitimate interest here in uncovering evidence of the offenses covered by the warrant. Our holding today is narrow: the unique facts in this case compel us to conclude that the Government no longer had a legitimate governmental interest in searching for evidence of the offenses covered by the warrant following Appellee's convictions, and so the search was constitutionally unreasonable.

Were we to conclude otherwise, we would effectively allow a digital forensic examination "for a period of unlimited duration and an examination of unlimited scope" based on a warrant issued at some time. *Cf. United States v. Kim*, 103 F. Supp. 3d 32, 59 (D.D.C. 2015). That level of discretion is incompatible with the requirements of particularity and issuance by an independent magistrate weighing probable cause for each offense individually—in other words, the requirements that "make[] general searches . . . impossible and prevents the seizure of one thing under a warrant describing another." *United States v. Leary*, 846 F.2d 592, 600 (10th Cir. 1988) (alterations in original) (internal quotation marks omitted) (citation omitted). We decline to grant the Government the unbridled discretion to conduct what is functionally a "general, exploratory rummaging in a person's belongings," *Coolidge*, 403 U.S. at 467, by relying on a warrant no longer justified by any legitimate government interest to assert that other evidence was in plain view.

C.

It is true that one exception to the warrant requirement for items not otherwise subject to a lawful search is the plain view doctrine, which allows law enforcement officials conducting a lawful search to seize items in plain view if they are acting within the scope of their authority and have probable cause to believe the item is contraband or evidence of a crime. *See United States v. Fogg*, 52 M.J. 144, 149 (C.A.A.F. 1999) (citing M.R.E. 316(d)(4)(C)). This exception applies even if "an officer is interested in an [unauthorized] item of evidence and fully expects to find it" there. *Horton v. California*, 496 U.S. 128, 138 (1990).

Courts have struggled to apply the plain view doctrine to searches of digital devices, given the vast amount of information they are capable of storing, *see* Kerr, *supra* p. 2, at 541–42; *Riley*, 134 S. Ct. at 2489–91 (explaining the significant intrusion upon privacy rights arising from the seizure of a cell phone, the seizure of which "differ[s] in both a quantitative and qualitative sense from" other types of physical seizures), and "the difficulty inherent in tailoring searches of electronic data to discover evidence of particular criminal conduct." *United States v. Lustyik*, No. 2:12-CR-645-TC, 2014 U.S. Dist. LEXIS 54819, at *37, 2014 WL 1494019, at *12 (D. Utah Apr. 16, 2014). In light of these difficulties, the application of the plain view doctrine in a digital context poses "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1005 (9th Cir. 2009), *revised and superseded by United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010)*; see also* James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809, 2830 (2011) (comparing the different approaches the federal courts of appeals have taken).

But we need not venture into this thicket today. A prerequisite for the application of the plain view doctrine is that the law enforcement officers must have been conducting a lawful search when they stumbled upon evidence in plain

view. As noted, the officers in this case were not conducting a lawful search because the execution of the warrant was constitutionally unreasonable.

III. JUDGMENT

We hold that the military judge did not abuse his discretion in suppressing the evidence obtained from the thumb drive seized from Appellee's home. We therefore answer the certified issue in the negative and the specified issue in the affirmative. Accordingly, the judgment of the United States Army Court of Criminal Appeals is affirmed.