UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES
Appellee

v.

Luis G. NIETO, Specialist
United States Army, Appellant

No. 16-0301
Crim. App. No. 20150386

Argued October 11, 2016—Decided February 21, 2017

Military Judge: Michael J. Hargis

For Appellant: *Captain Joshua G. Grubaugh* (argued); *Lieutenant Colonel Charles D. Lozano* and *Captain Heather L. Tregle* (on brief).

For Appellee: *Captain Tara E. O'Brien Goble* (argued); *Colonel Mark H. Sydenham, Lieutenant Colonel A. G. Courie III,* and *Major Steven J. Collins* (on brief); *Major Daniel D. Derner.*

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

Judge OHLSON delivered the opinion of the Court.

Pursuant to Appellant's conditional pleas, a military judge sitting alone as a general court-martial convicted Appellant of four specifications of abusive sexual contact and one specification each of being absent without leave, violating a general order, making a false official statement, and making an indecent visual recording, in violation of Articles 86, 92, 107, 120, and 120c, Uniform Code of Military Justice, 10 U.S.C. §§ 886, 892, 907, 920, 920c (2012). The military judge sentenced Appellant to a reduction to E-1, forfeiture of all pay and allowances, confinement for five years, and a bad-conduct discharge. In accordance with the pretrial agreement, the convening authority reduced the sentence of confinement to four years, but otherwise approved the adjudged sentence.

As provided for in the pretrial agreement, Appellant challenged on appeal the military judge's denial of his motion to suppress evidence from his laptop computer. The United States Army Court of Criminal Appeals summarily affirmed the approved findings and sentence. We granted review on the following assigned issue:

> Whether the military judge erred in denying Appellant's motion to suppress the evidence seized from Appellant's laptop computer.

United States v. Nieto, 75 M.J. 292 (C.A.A.F. 2016).

Upon review of this issue, we conclude that there was an insufficient particularized nexus linking Appellant's misconduct to his laptop. Therefore, the military magistrate did not have a substantial basis for concluding that probable cause existed to seize the laptop. We further conclude that the inevitable discovery doctrine and the good-faith doctrine do not apply in this case. The military judge therefore abused his discretion in denying Appellant's motion to suppress evidence. Accordingly, we reverse the decision of the United States Army Court of Criminal Appeals.

I. Background

In May of 2013, Corporal (CPL) RAO and another soldier provided sworn statements to the Army Criminal Investigation Division (CID). They averred that Appellant had used his cell phone to record them using the latrine at Forward Operating Base (FOB) Azizullah, Afghanistan, without their consent. CPL RAO further stated that after Appellant had been identified as the person using the cell phone, two noncommissioned officers "look[ed] through the subject's cellular phone for any photographs or videos, which they did not find." His statement did not reference Appellant's laptop. Special Agent (SA) Sandefur, who had fifteen years of investigative experience, was in charge of the Kandahar Airfield CID office and initially supervised the investigation into these allegations.

In the course of the investigation, SA Sandefur was told by his agents that "somebody" had previously seen a cell phone and laptop on Appellant's bunk in his tent. SA Sandefur subsequently sought from a part-time military magistrate a search authorization to search Appellant's

bunk and to seize the cell phone and laptop. SA Sandefur testified that he did not "have any direct evidence" that images and videos were on the laptop, did not know whether the files on the cell phone were transferable to the laptop, and did not know the memory storage capacity of the cell phone. He also did not know whether Appellant took photographs in the latrine, but "the investigation suggested" that Appellant had taken photographs that would have been "in a file format." SA Sandefur supported the search authorization of the laptop with three sources of information: (1) CPL RAO's sworn statement, cited above, that Appellant had used a cell phone in the latrine; (2) SA Sandefur's own affidavit, cited below, which makes no mention of a laptop computer; and (3) SA Sandefur's in-person meeting with the military magistrate, also cited below.

SA Sandefur's affidavit in support of the search authorization stated, in relevant part:

> On 18 May 2013, this office was notified of an incident at FOB Azi Zullah [sic] that involved a male Soldier viewing other male Soldiers in bathroom stalls.
>
> Preliminary investigation revealed that [Appellant] was using his Samsung telephone to view and possibly record other male Soldiers while they were on the toilet. Victims reported that they observed someone holding a cellular telephone over the wall of the bathroom stall while they were exposed and utilizing the toilet. [Appellant] was later identified by a Soldier as he was departing the latrine.
>
> ....
>
> About 1300, 18 May 13, SA [JF], this office interviewed Cpl [RAO] … who provided a sworn statement … wherein he related on 12 May 13, he noticed a cellular telephone being held over the wall of his latrine stall. He further related [to] his fellow Soldier SPC [CS] what happened. He indicated that he and SPC [CS] … then waited outside the latrine stall as CPL [RAO] notified leadership. SPC [CS] identified [Appellant] exit the stall and reported him to leadership.

During the in-person meeting with the military magistrate to review the search authorization request, SA Sandefur informed the military magistrate about his:

> knowledge in reference to Soldiers using their cell phones to photograph things, … and that those phones are normally downloaded, the photos they take, if they're taking scene photos or photos of their friends or whatever while they're out on--on missions or on the FOB, they'll back those up to their laptops so that when they get to the--a place where they can get Internet, they can post those or send those home to family or whatever.

SA Sandefur also briefed the military magistrate about "the preliminary information that [he] received from the agents on the ground at the FOB" about Appellant "using the cell phone underneath the stall to … film or … take pictures of individuals in the stall next to him." He further informed the military magistrate about the type of cell phone Appellant owned (a "White Samsung Galaxy cellular Telephone"), but did not provide any details about any laptop that Appellant may have owned.

Relying on these three sources of information, on May 20, 2013, the military magistrate issued a search and seizure authorization to search Appellant's bunk and seize any cell phone or laptop computer that was found there. Upon seizing the two items that same day, CID agents sent them to a CID digital forensic examiner. On June 4, 2013, CID agents interviewed Appellant and he confessed to recording soldiers who were using the latrine.[1]

Before conducting a search of the laptop and the cell phone, the forensic examiner requested that CID obtain an additional search authorization tailored to that purpose. This request prompted SA Dunn, who had become the primary case agent in June of 2013, to seek a search authorization from another part-time military magistrate at Kandahar Airfield in July 2013. In support of this July search authorization, SA Dunn relied on Cpl RAO's sworn state-

[1] This was Appellant's second interview with CID. In the first, he falsely denied holding his phone over the top of a bathroom stall.

ment, as well as on an affidavit that mirrored SA Sandefur's previous affidavit, except for the following additional paragraphs:

> About 1024, 4 Jun 13, [Appellant] admitted to using his cellular telephone to view and record Soldiers utilizing the latrine while at FOB Azi Zullah [sic], Afghanistan. [Appellant] admitted to masturbating to the images on his cellular telephone of Soldiers utilizing the latrine.
>
> It is my [i.e., SA Dunn's,] experience as a CID Special Agent that persons who would use a portable digital media recorder would also transfer the media from a portable device to a computer station or storage device. Persons who view and record sexual acts often times store and catalog their images and videos on larger storage devices such as a computer or hard drive.

On July 17, 2013, the military magistrate authorized the search of the laptop and cell phone. The CID forensic examiner's search of the cell phone "revealed nothing relevant to [CID's] investigation." However, the laptop contained a number of incriminating videos and pictures, which ultimately led to additional criminal charges.

During the court-martial proceedings, Appellant moved to suppress evidence obtained from the laptop. He asserted that the facts presented to the military magistrates "were insufficient to support a finding of probable cause." The military judge denied the motion on the basis that the military magistrates "were provided with a substantial basis for determining the existence of probable cause as to images being found on the accused's laptop." The military judge cited the following points:

> The normal inference to be drawn from the accused placing a cell phone over a latrine stall … is that the accused was recording images….
>
> It is also a normal inference to be drawn—as was done in [*United States v. Clayton*, 68 M.J. 419 (C.A.A.F. 2010)]—that data is transferred from one digital device to another. Both SA Sandefur and SA Dunn told [the military magistrates] as much.

This ruling is at issue in this appeal.

II. Applicable Legal Principles

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). Accordingly, when reviewing a military magistrate's issuance of a search authorization, we "do not review [the military magistrate's] probable cause determination de novo." *Id.* at 125. Instead, we examine whether a military "magistrate had a substantial basis for concluding that probable cause existed." *United States v. Rogers*, 67 M.J. 162, 164–65 (C.A.A.F. 2009). A substantial basis exists "when, based on the totality of the circumstances, a common-sense judgment would lead to the conclusion that there is a fair probability that evidence of a crime will be found at the identified location." *Id.* at 165 (citing *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *United States v. Leedy,* 65 M.J. 208, 213 (C.A.A.F. 2007)). We give "great deference" to the magistrate's probable cause determination because of "the Fourth Amendment's strong preference for searches conducted pursuant to a warrant." *Gates*, 462 U.S. at 236 (citation omitted) (internal quotation marks omitted). However, this deference is "not boundless," and a reviewing court may conclude that "the magistrate's probable-cause determination reflected an improper analysis of the totality of the circumstances." *United States v. Leon*, 468 U.S. 897, 915 (1984). However, if a military magistrate has "a substantial basis to find probable cause, a military judge [does] not abuse his discretion in denying a motion to suppress." *Leedy*, 65 M.J. at 213.

The Fourth Amendment is predicated on "[t]he right of the people to be secure in their persons, houses, papers, and effects." U.S. Const. amend. IV. It safeguards against "unreasonable searches and seizures" and requires warrants to be supported by probable cause. *Id.* The military has implemented the Fourth Amendment through the Military Rules of Evidence (M.R.E.) 311–17. *Hoffmann*, 75 M.J. at 123. These rules reflect "the limits which military society, speaking through its Commander-in-Chief, is willing to" place upon the protections afforded under the Fourth Amendment in a military context. *See United States v. McCarthy*, 38 M.J. 398, 402 (C.M.A. 1993); *see also United States v. Taylor*, 41 M.J. 168, 171 (C.M.A. 1994). This Court is ordinarily

bound by the Military Rules of Evidence. *See Taylor*, 41 M.J. at 171.[2]

The Military Rules of Evidence provide that when a seizure is made pursuant to a search authorization, the search authorization "must be based upon probable cause." M.R.E. 315(f)(1); M.R.E. 316(c)(5)(A); *see also United States v. Hester*, 47 M.J. 461, 463 (C.A.A.F. 1998). Probable cause to seize exists if there is "a reasonable belief that the property or evidence is … evidence of crime." M.R.E. 316(c)(1); *cf.* M.R.E. 315(f)(2). "[P]robable cause determinations are inherently contextual, dependent upon the specific circumstances presented as well as on the evidence itself," and "probable cause is founded … upon the overall effect or weight of *all* factors presented to the magistrate." *Leedy*, 65 M.J. at 213; *see also Gates*, 462 US. at 232 (observing that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts"). Stated differently, in order for there to be probable cause, a sufficient nexus must be shown to exist between the alleged crime and the specific item to be seized. *See Rogers*, 67 M.J. at 166; *United States v. Gallo*, 55 M.J. 418, 421 (C.A.A.F. 2001) (stating that probable cause "definition encompasses showing a nexus"). "The question of nexus focuses on whether there was a 'fair probability' that contraband or evidence of a crime will be found in a particular place." *Clayton*, 68 M.J. at 424 (quoting *Leedy*, 65 M.J. at 213). A nexus may "be inferred from the facts and circumstances of a particular case," including the type of crime, the nature of the items sought, and reasonable inferences about where evidence is likely to be kept. *Id.*; *Gallo*, 55 M.J. at 421.

A law enforcement officer's professional experience may be useful in establishing such a nexus. *See Leedy*, 65 M.J. at 215–16; *see also United States v. Soto*, 799 F.3d 68, 85 (1st

[2] We note that in the instant case the Government has not argued that we should apply the Military Rules of Evidence in a different manner because this incident took place at a forward operating base. Therefore, we do not address whether, due to any combat exigencies, the rules governing searches and seizures might apply differently here, nor do we address whether the military magistrate's probable cause determination might be due additional deference under the attendant circumstances.

Cir. 2015). However, a law enforcement officer's generalized profile about how people normally act in certain circumstances does not, standing alone, provide a substantial basis to find probable cause to search and seize an item in a particular case; there must be some additional showing that the accused fit that profile or that the accused engaged in such conduct. *See United States v. Macomber*, 67 M.J. 214, 220 (C.A.A.F. 2009). "[W]hile courts have relied on such profiles to inform search determinations, ... a [law enforcement officer's] profile alone without specific nexus to the person concerned cannot provide the sort of articulable facts necessary to find probable cause to search" or seize. *Id.*

If a military magistrate did not have a substantial basis to find probable cause in a specific case, this Court ordinarily applies the exclusionary rule. *Hoffmann*, 75 M.J. at 124 (citing M.R.E. 311(a)). However, there are exceptions to this rule, including the inevitable discovery doctrine and the good-faith doctrine. *See* M.R.E. 311(c)(2), (3).

For the inevitable discovery doctrine to apply, the Government must establish:

> 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 and that the evidence would inevitably have been discovered in a lawful manner had not the illegality occurred."

Hoffmann, 75 M.J. at 125 (quoting *United States v. Dease*, 71 M.J. 116, 122 (C.A.A.F. 2012)); *see also* M.R.E. 311(c)(2).

For the good-faith doctrine to apply, the Government must establish that law enforcement's reliance on a defective authorization is objectively reasonable. *Hoffmann*, 75 M.J. at 127. In the military, the good-faith doctrine applies if: (1) the seizure resulted from a search and seizure authorization issued, in relevant part, by a military magistrate; (2) the military magistrate had a substantial basis for determining probable cause existed; and (3) law enforcement reasonably and in good faith relied on the authorization. M.R.E. 311(c)(3); *see also United States v. Carter*, 54 M.J. 414, 420 (C.A.A.F. 2001).

III. Discussion

We conclude that the military judge abused his discretion in denying Appellant's motion to suppress evidence from the laptop. We reach this conclusion because (1) the military magistrate had no substantial basis for finding probable cause even after according the military magistrate great deference, and (2) neither the good-faith doctrine nor the inevitable discovery doctrine applies. We discuss each conclusion below.

A. Probable Cause

Turning our attention to the military magistrate's probable cause determination, we first note the United States Supreme Court's observation that cell phones, such as the one possessed by Appellant, are "in fact minicomputers" that have "immense storage capacity" allowing them to store "thousands of pictures, or hundreds of videos." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). Indeed, Appellant's cell phone, by itself, had the ability to serve both as the instrumentality of the crime and as a storage device for the fruit of that crime. Therefore, in this age of "smart phones," SA Sandefur's generalized profile about how servicemembers "normally" store images was technologically outdated and was of little value in making a probable cause determination.

We further note that the affidavits accompanying the search authorization did not reference a laptop or data transfers from Appellant's cell phone. Accordingly, we conclude that SA Sandefur's generalized profile was not based on a firm factual foundation. As a result, the information provided by SA Sandefur to the magistrate did not independently establish a particularized nexus between (a) the crime the accused was alleged to have committed with his cell phone in the latrine and (b) the laptop that was previously seen by "somebody" on Appellant's bunk. In order to identify a substantial basis for concluding that probable cause existed to believe that Appellant's laptop was linked to the crime, we conclude that—at a minimum—there needed to be some additional showing, such as the fact that Appellant actually downloaded images (illicit or otherwise) from his cell phone to his laptop, stored images on his laptop, or

transmitted images from his laptop. And yet, there was no such showing in this case.[3] Therefore, SA Sandefur's affidavit, his generalized profile, and CPL RAO's affidavit provided no basis, substantial or otherwise, for the military magistrate to conclude that probable cause existed to seize the laptop. *See Warden v. Hayden*, 387 U.S. 294, 307 (1967) (requiring "a nexus … between the item to be seized and criminal behavior").

SA Sandefur's oral discussion with the military magistrate also failed to adequately support the search authorization. *See* M.R.E. 315(f)(2)(B) (noting that probable cause determination can be based on oral statements). Except for the generalized profile discussed and discredited above, the military magistrate was not provided with substantive oral information linking Appellant's misconduct to the laptop. This point is underscored by the fact that SA Sandefur testified that he did not have "any direct evidence" that images were on the laptop and did not know whether the files on the cell phone were transferable to the laptop, and by the fact that SA Sandefur made no proffer to the military magistrate that anyone had ever seen Appellant download material from his cell phone to a laptop. In fact, even Appellant's ownership of the laptop in question was predicated on suspect information and credited to an unknown source.[4] *Cf. Hoffmann*, 75 M.J. at 125 (noting that probable cause determination considers veracity and basis of knowledge of those supplying

---

[3] In reaching this conclusion, we are not creating a heightened standard for probable cause or requiring direct evidence to establish a nexus in cases where technology plays a key role. Rather, the traditional standard that a nexus may "be inferred from the facts and circumstances of a particular case," *Clayton*, 68 M.J. at 424, still holds in cases involving technological devices such as cell phones and laptops. We merely conclude that in the instant case there is an insufficient nexus between Appellant's cell phone and his laptop that can be inferred based on the particular facts presented to the military magistrate. We have provided some nonexhaustive examples as to how a sufficient nexus might be inferred in order to demonstrate that this burden on the Government is far from onerous.

[4] CID only knew that a laptop was on Appellant's "bunk in his tent." When pressed on this specific point, SA Sandefur could not explain how CID learned of the laptop.

hearsay information). Moreover, the military magistrate could not draw any reasonable inferences linking the crime and the laptop based on the limited information and generalized profile offered by SA Sandefur. Therefore, we hold that the military magistrate did not have a substantial basis for concluding that probable cause existed to seize Appellant's laptop.[5]

B. Good-Faith and Inevitable Discovery Doctrines

The Government argues that, even if the military magistrate did not have a substantial basis for concluding that probable cause existed to seize Appellant's laptop, the evidence from the laptop was admissible under the good-faith doctrine as well as under the inevitable discovery doctrine. In order to prevail, the Government has the burden of establishing both doctrines by a preponderance of the evidence. *See* M.R.E. 311(d)(5)(A). We conclude that the Government has not met its burden of establishing the good-faith doctrine. *See* M.R.E. 311(c)(3).[6]

The Government also has failed to establish the applicability of the inevitable discovery doctrine. In reaching this conclusion, we note that the Government has failed to iden-

---

[5] In reaching this conclusion, we are mindful that a contrary holding could be construed as providing law enforcement with broad authority to search and seize *all* of an accused's electronic devices and electronic media merely because the accused used a cell phone in furtherance of a crime. This result, based on generalized profiles created by law enforcement and on the generalized observation about "the ease with which [digital] media may be replicated on" a multitude and array of electronic devices, would run counter to the principle that law enforcement officials must provide *specific and particular* information in order for a magistrate to determine that there is "a fair probability that contraband or evidence of a crime will be found in a particular place." *See Clayton*, 68 M.J. at 424 (citation omitted) (internal quotation marks omitted)*; see also* M.R.E. 316(c)(1); *United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016).

[6] We recognize the tension between our discussion of the good-faith doctrine in *Hoffmann*, 75 M.J. at 127–28, and *Carter*, 54 M.J. at 419–22. We leave for another day resolution of this tension because we conclude that under either understanding of the good-faith doctrine the Government has not met its burden of establishing this exception to the exclusionary rule in Appellant's case.

tify any evidence that law enforcement possessed, or was actively pursuing at the time of the seizure, that would have made the lawful discovery of the laptop evidence inevitable. *See Hoffmann*, 75 M.J. at 125–26. We will not rely on "speculation and conjecture" to make this conclusion. *See United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996). Therefore, the Government has not established the applicability of the inevitable discovery doctrine.

IV. Conclusion

We hold that the military magistrate did not have a substantial basis to determine that probable cause existed to seize Appellant's laptop and that the inevitable discovery and good-faith exceptions do not apply in this case. Because the seizure of the laptop was unlawful, the subsequent search is likewise unlawful. *See Wong Sun v. United States*, 371 U.S. 471, 488 (1963); *United States v. Conklin*, 63 M.J. 333, 334 (C.A.A.F. 2006); *see also* M.R.E. 311(a). The military judge therefore abused his discretion in denying Appellant's motion to suppress evidence from the laptop.

V. Decision

The decision of the United States Army Court of Criminal Appeals is reversed. The findings and sentence are set aside. The record of trial is returned to the Judge Advocate General of the Army for proceedings consistent with this opinion.

Judge STUCKY, dissenting.

Crucial to the sensible legal treatment of modern technology is an understanding of its functioning and the commonsense application of well-established doctrine in the face of novel situations. In my view, the majority fails in both of these regards, and I therefore respectfully dissent.

Before engaging the technology at issue in this case, the majority omits mention of material precedent from this Court in its presentation of the law of probable cause.

"Probable cause exists where 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Grubbs*, 547 U.S. 90, 95 (2006) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). It "is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Gates*, 462 U.S. at 232. Pertinently, we have stated that probable cause requires

> more than bare suspicion, but something less than a preponderance of the evidence. Thus, the evidence presented … need not be sufficient to support a conviction, nor even to demonstrate that an investigator's belief is more likely true than false …; there is no specific probability required, nor must the evidence lead one to believe that it more probable than not that contraband will be present.

United States v. Leedy, 65 M.J. 208, 213 (C.A.A.F. 2007) (citations omitted). Such conclusions must also be "founded not on the determinative features of any particular piece of evidence … but rather upon the overall effect or weight of all factors," which is "dependent upon the specific circumstances presented as well as on the evidence itself." *Id.*

In addition to incompletely presenting the law of probable cause, the majority also misapplies the standard of review that we utilize with regard to these issues. When a military judge's denial of a motion to suppress comes before us, "[w]e review the legal question of sufficiency for finding probable cause de novo using a totality of the circumstances test." *Leedy*, 65 M.J. at 212. In conducting this review, we apply the standard that the military judge would use in re-

viewing the magistrate's probable cause determination. That is, we "start by examining whether the magistrate had a 'substantial basis' for determining that probable cause existed," *id*. (quoting *Gates*, 462 U.S. at 238), because "[i]t follows that where a magistrate had a substantial basis to find probable cause," a military judge would be correct in denying a motion to suppress evidence reaped from any resulting search or seizure. *Id*. The Supreme Court has held that "[t]he duty of a reviewing court is simply to ensure that the magistrate had a 'substantial basis for … conclud[ing]' that probable cause existed." *Gates*, 462 U.S. at 238–39 (alteration in original) (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)). Moreover, it has found that "[r]easonable minds frequently may differ on the question [of] whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according great deference to a magistrate's determination." *United States v. Leon*, 468 U.S. 897, 914 (1984) (internal quotation marks omitted) (citations omitted); *see also Gates*, 462 U.S. at 236 ("A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969))). Consistent with this precedent, we have held that "determinations of probable cause made by a neutral and detached magistrate are entitled to substantial deference." *United States v. Clayton*, 68 M.J. 419, 423 (C.A.A.F. 2010); *accord United States v. Hoffmann*, 75 M.J. 120, 123 (C.A.A.F. 2016) ("Searches conducted after obtaining a warrant or authorization based on probable cause are presumptively reasonable.").

Before the military magistrate who granted the initial search authorization were the following: a sworn statement from a soldier (CPL RAO) attesting to Appellant's actions and those of others; an affidavit from SA Sandefur in support of a search and seizure authorization; and information orally provided to the magistrate by SA Sandefur during an in-person meeting. The first and third sources of information are given short shrift in the majority opinion, and therefore require further elaboration.

The sworn statement from CPL RAO attested to an incident during which, while using the latrine, he looked up and

"noticed a cellular phone screen being pulled from [his] stall to the stall to [his] left." Upon returning to his tent, CPL RAO stated that he confided in his colleague (SPC S) what had happened, and that, in turn, SPC S "confided in [CPL RAO] that the same situation had happened to him a week prior." SPC S then went to the latrine in an attempt to catch the subject in the act, and returned approximately thirty minutes later, telling CPL RAO that "the cellular phone appeared over his stall as well." CPL RAO then recounted returning to the latrine with SPC S and sitting "in the stall to see if [he] could catch the subject [him]self." After waiting five minutes without glimpsing the cellular phone, CPL RAO exited the latrine stall and sought out superiors. Meanwhile, SPC S waited at the latrine to see who came out of the stall from which the cellular phone had been outstretched. CPL RAO informed four superiors of the situation and returned to the latrine with three of them. When they arrived, Appellant was standing outside of the latrine with two superiors and SPC S. The two superiors already there were looking through Appellant's cellular phone for inappropriate recordings, of which they found none. The grouping then dispersed to discuss the situation and inform others of what had transpired.

In turn, during his in-person conversation with the military magistrate, SA Sandefur informed her not just that soldiers tend to back up media files recorded using their cellular phones by uploading them to their laptops, as the majority accepts, but that they do this specifically with recordings made "on missions or on the [forward operating base]," such as that where Appellant was stationed. This insight came from a special agent with fifteen years of experience, over the course of which he was deployed multiple times. It is clear from the search authorization, and SA Sandefur's testimony, that law enforcement knew the specific type of cellular phone that Appellant possessed—a "White Samsung Galaxy cellular Telephone,"—and informed the military magistrate of this. These two sources, similarly make it apparent that law enforcement knew that Appellant possessed a laptop computer, the likely location of both the computer and cellular phone—Appellant's "Bunk," "tent 224,"—and so informed the military magistrate. The majori-

ty attempts to cast information on the laptop's location as "suspect" by criticizing its attribution to "an unknown source." *United States v. Nieto,* __ M.J. __ (10) (C.A.A.F. 2017). But an unnamed individual seeing the computer on Appellant's bunk next to his phone in the cramped living conditions of a forward operating base (FOB), and SA Sandefur being unable to recall exactly from whom his fellow agents had procured this information when questioned months after he worked on the case, do little to undermine the fact that law enforcement had a clear idea of where Appellant's laptop was and passed this insight on to the military magistrate. Finally, the majority's statement that SA Sandefur "did not know whether the files on the cell phone were transferable to the laptop" is misleading. *Id. at* __ (3). Based on a sworn statement attesting to Appellant's repeated suspicious conduct, he was suspected of making inappropriate recordings with his cellular phone. And SA Sandefur clearly stated that authorities suspected that there "would have been at least photographs on [Appellant's] phone … in a file format." It is widely understood that such files are transferable between devices, and between cellular phones and laptop computers in particular.

Applying the proper probable cause analysis to the full facts presented to the military magistrate shows that she had a substantial basis for her positive finding, notwithstanding the substantial deference she is to be accorded—deference that the majority notes must be given but fails to confer. SA Sandefur communicated to the military magistrate the specific type of cellular phone owned by Appellant and the likely location where it and Appellant's laptop would be found. He also relayed that, based on his substantial professional experience, soldiers stationed at FOBs tend to upload media files taken with their cellular phones to other devices with greater storage capacity. While the experienced counsel of law enforcement professionals is of great value to magistrates in probable cause determinations, *Leedy*, 65 M.J. at 215–16; *accord United States v. Gallo*, 55 M.J. 418, 422 (C.A.A.F. 2001) ("The courts have allowed a gap in the nexus to be filled in based on the affiant's experience."), the majority is correct in noting that this "'alone without specific nexus to the person concerned'" is not enough to form a sub-

stantial basis. *Nieto,* __ M.J. at __ (8) (quoting *United States v. Macomber*, 67 M.J. 214, 220 (C.A.A.F. 2009)). But it is incorrect in solely analyzing this source of information in assessing the magistrate's decision.

For his part, CPL RAO swore to a first-person account of actions taken by Appellant indicating that he was making inappropriate recordings with his cellular phone, others observing these actions as well, and the fact that Appellant consistently engaged in such practices over a period of time. Moreover, it was recounted that superiors conducted an impromptu search of Appellant's cellular phone for offensive material and found none, bolstering the suspicion that, given his consistent conduct, Appellant was transferring his media files to another device.

All told, the magistrate had before her a sworn statement as to Appellant's consistent suspicious behavior and an affidavit from a very experienced law enforcement officer informing her of the common practices of individuals who fit Appellant's profile. A nexus between Appellant, the crime he was suspected of, and his laptop computer is quite apparent.

But even if the nexus was not so readily discernible, military magistrates have the authority "to draw such reasonable inferences as [they] will from the material supplied to [them] by applicants for a warrant." *Gates*, 462 U.S. at 240; *accord Clayton*, 68 M.J. at 424 (holding that military magistrates have the authority to make "normal inferences as to where a criminal would likely hide the property"). "Thus, while the law requires [magistrates] to be neutral, the law does not require [them] to pretend they are babes in the woods. In evaluating search warrant applications, [magistrates] may consider what 'is or should be common knowledge.'" *United States v. Reichling*, 781 F.3d 883, 887 (7th Cir. 2015) (quoting *United States v. Seiver*, 692 F.3d 774, 778 (7th Cir. 2012)). Indeed, judicial reliance on common knowledge is a timeworn legal precept. *E.g.*, *Alberty v. United States*, 162 U.S. 499, 511 (1896) ("[I]t is a matter of *common knowledge* that men who are entirely innocent do sometimes fly from the scene of a crime through fear of being apprehended as the guilty parties, or from an unwillingness to appear as witnesses.") (emphasis added).

It is common knowledge that, despite continuing advances, cellular phones generally have less digital storage capacity than computer hard drives; that photo and video recordings are some of the most digital storage intensive items regularly created by and saved on cellular phones; that, in order to preserve storage space on cellular phones, these recordings are routinely transferred to higher capacity storage options, whether they be cloud storage services or personal hard drives, the latter including those both separate from and internal to computers; and that such transfers, whether conducted wirelessly or through a physical connection, are quite easy given modern technology. *See Reichling*, 781 F.3d at 887 (finding that it is "common knowledge to judges (like other members of the public) that images sent via cell phones or Facebook accounts may be readily transferred to other storage devices"); *Clayton*, 68 M.J. at 424 (recognizing "the ease with which computer media may be replicated on portable devices"); *Riley v. California*, 134 S. Ct. 2473, 2491 (2014) (noting that, "with increasing frequency," cellular phones are used to access data located elsewhere "at the tap of a screen"); Mark Wilson, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 Golden Gate U. L. Rev. 261, 268 (2013) ("Mobile devices, and even smaller laptop computers, have limited storage capacity due to their small size and their necessarily small internal disks."); Walter S. Mossberg, *Learning About Everything Under the 'Cloud,'* Wall. St. J. (May 6, 2010) ("Your smartphone can't run all the sophisticated programs, or store all the files, that your PC can."), *available at* http://www.wsj.com/articles/SB10001424052748703961104575226194192477512 (last visited Feb. 15, 2017). Given the commonality of these aspects of modern cellular phones, courts are increasingly confronting the specific scenario of the transfer of elicit digital material—e.g., inappropriate images and videos—from cellular phones to computers. *See, e.g.*, *United States v. Napier*, 787 F.3d 333, 338 (6th Cir. 2015); *United States v. Grzybowicz*, 747 F.3d 1296, 1310-11 (11th Cir. 2014); *United States v. Norton*, 557 F. App'x 615, 616 (8th Cir. 2014); *see also United States v. Wilson*, Magistrate No. 16-730 (DAR), 2016 U.S. Dist. LEXIS 157085, at *13, 2016 WL 6683268, at *4 (D. D.C. 2016) ("Defendant

stated that she accessed [a cloud storage service] on her cellular phone to collect, store, and share her child pornography."). The application of this common knowledge further bolsters the military magistrate's substantial basis for her finding of probable cause to search and seize Appellant's laptop computer.

The majority, however, misinterprets precedent and employs dubious logic in an attempt to avoid the commonsense conclusions noted above. First, it cites *Riley*, 134 S. Ct. at 2489, for the proposition that modern cellular phones have "'immense storage capacity'" that can hold "'thousands of pictures,'" and that this lessens the necessity of transferring data from cellular phones to other digital storage mediums. *Nieto,* __ M.J. at __ (9). But these quotations are taken out of context. The Supreme Court's statement that modern cellular phones have "immense storage capacity" was made comparing them to what individuals could previously physically carry on their person and older phone models. It in no way contradicts the common knowledge that computers generally have much larger digital storage capacities than cellular phones. In addition, the Supreme Court's comment regarding "thousands of pictures" is made in reference to a distinct storage capacity: "16 gigabytes." *Riley*, 134 S. Ct. at 2489. This storage volume could certainly hold thousands of photograph files if solely devoted to that function, but the hard drive of a cellular phone is responsible for facilitating the functioning of the entire device, not just storing photos. As such, "16 gigabytes" is generally consumed by many other files and functions besides simply photo storage, and so the storage of "thousands of pictures" is generally not practicable.

Second, the majority's argument in favor of treating modern cellular phones as digital islands contradicts itself. It notes the modern "age of 'smart phones'" as a reason why SA Sandefur's assertion that soldiers at FOBs usually transfer recording files from their phones to computers is "outdated and … of little value." *Nieto,* __ M.J. at __ (9). But this contention serves the opposite purpose. "Smart phones" are actually means of *connection* that dramatically *enhance* the ability and opportunities to collect data and disseminate it across devices. Accordingly, "[t]oday's cell phones, with their

capacity to reach the Internet, the cloud, and to store millions of documents and photographs [thereby], can no longer analogize to a run-of-the-mill wardrobe. Instead, they are also a portal." *United States v. Mayo*, No. 2:13-CR-48, 2013 U.S. Dist. LEXIS 158866, at *29, 2013 WL 5945802, at *8 (D. Vt. 2013); *see also United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) ("[A] digital device is a conduit to retrieving information from the cloud."). In fact, modern cellular phones have such "immense storage capacity" *because of* their easy connection to other storage mediums, such as cloud storage services and traditional computers. *See, e.g.*, *Riley*, 134 S. Ct. at 2491; *United States v. Saboonchi*, 990 F. Supp. 2d 536, 563 (D. Md. 2014); *In re Cellular Telephones*, No. 14-MJ-8017-DJW, 2014 U.S. Dist. LEXIS 182165, at *14–18, 2014 WL 7793690, at *5 (D. Kan. 2014); *Mayo*, 2013 U.S. Dist. LEXIS 158866, at *29, 2013 WL 5945802, at *8; *see also Wilson*, 2016 U.S. Dist. LEXIS 157085, at *13, 2016 WL 6683268, at *4. Rather than illuminating any lack of technological understanding on the part of SA Sandefur, a law enforcement officer with a great deal of experience in this area, the majority reveals its own deficient grasp of the contemporary consumer electronics environment and its networked nature.

Given the state of the law of probable cause, the evidence presented to the military magistrate, and the current state of common knowledge regarding modern cellular phones, the magistrate certainly had a substantial basis for her positive finding. The majority, however, avoids reaching this conclusion by applying a heightened requirement for probable cause than what precedent requires:

> In order to identify a substantial basis for concluding that probable cause existed to believe that Appellant's laptop was linked to the crime, we conclude that—at a minimum—there needed to be some additional showing, such as the fact that Appellant actually downloaded images (illicit or otherwise) from his cell phone to his laptop, stored images on his laptop, or transmitted images from his laptop.

Nieto, __ M.J. at __ (9–10). This appears to require direct evidence of particular conduct, and therefore a *likelihood* that

incriminating material will be found on the laptop, or that a *preponderance of the evidence* supports this supposition. But such a requirement does not comport with Supreme Court precedent requiring only a "fair probability" that incriminating material will be found, *Gates*, 462 U.S. at 238, or our own precedent stating that "the evidence presented … need not be sufficient to support a conviction, nor even to demonstrate that an investigator's belief is more likely true than false." *Leedy*, 65 M.J. at 213 (citations omitted); *see also Gates* 462 U.S. at 235 ("Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence … have no place in the [probable cause] decision."). Courts have consistently

> upheld searches although the nexus between the items to be seized and the place to be searched rested not on direct observation, … but on the type of crime, the nature of the … items, the extent of the suspect's opportunity for concealment, and normal inferences as to where a criminal would be likely to his [incriminating material].

United States v. Lucarz, 430 F.2d 1051, 1054 (9th Cir. 1970) (citations omitted); *accord United States v. Anton*, 546 F.3d 1355, 1358 (11th Cir. 2008); *United States v. Martin*, 426 F.3d 68, 74-77 (2d Cir. 2005). More specifically, they have upheld positive probable cause findings pertaining to digital devices in an accused's possession other than those used to commit the alleged offense when that offense involved inappropriate digital recordings. *See United States v. Kapordelis*, 569 F.3d 1291, 1310-12 (11th Cir. 2009); *see also United States v. Mann*, 592 F.3d 779, 786 n.2 (7th Cir. 2010).

Since the first military magistrate had a substantial basis for authorizing the search and seizure of Appellant's laptop computer, it necessarily follows that the second magistrate did as well. This is because, in addition to all of the information that was presented to the first magistrate, the second was also informed that Appellant confessed to making numerous photographic and video recordings of fellow sevicemembers in compromising positions for his own sexual gratification. Thus, the military judge's denial of the motion to suppress evidence gleaned from the searches and seizures in question should be affirmed.

Overall, a constellation of shortcomings with regard to the law of probable cause, the facts of this case, and the application of law to fact envelops the majority opinion. I therefore reiterate my respectful dissent.