UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES
Appellee

v.

James W. RICHARDS IV, Lieutenant Colonel
United States Air Force, Appellant

No. 16-0727
Crim. App. No. 38346

Argued March 15, 2017—Decided July 13, 2017

Military Judge: Mark L. Allred

For Appellant: *William E. Cassara,* Esq. (argued); *Major Johnathan D. Legg, Major Thomas A. Smith*, and *Captain Patrick A. Clary*.

For Appellee: *Major Mary Ellen Payne* (argued); *Colonel Katherine E. Oler* and *Gerald R. Bruce,* Esq. (on brief).

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

Judge SPARKS delivered the opinion of the Court.

This case arises out of the conviction of Lieutenant Colonel James W. Richards IV (Appellant), contrary to his pleas, of one specification of possession of child pornography and five specifications of indecent acts with a male under sixteen years of age, both in violation of Article 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 934 (2012); and four specifications of failing to obey a lawful order in violation of Article 92, UCMJ, 10 U.S.C. § 892 (2012). A military judge, sitting alone, sentenced Appellant to a dismissal, seventeen years confinement, and forfeiture of all pay and allowances. The convening authority approved the adjudged sentence.

Appellant raised numerous issues before the United States Air Force Court of Criminal Appeals and, on May 2, 2016, the lower court affirmed the findings and sentence. Appellant then filed a petition for review with this Court. We granted review on the issue of whether the November 9,

2011, search authorization was overly broad in failing to limit the dates of communications being searched.[1]

Upon review of this issue, we agree with the lower court that the November 9, 2011, search authorization was sufficiently particularized and that investigators did not exceed the scope of that authorization in searching the electronic devices in question.[2]

Facts

In April 2011, the Air Force Office of Special Investigations (AFOSI) at Tyndall Air Force Base in Florida initiated an investigation into Appellant based on notification from the National Center for Missing and Exploited Children that one of Appellant's former "little brothers"[3] from the Big Brothers Big Sisters program had alleged Appellant sexually abused him between 1993 and 1997, prior to Appellant joining the Air Force. Several months into their investigation, agents received permission to place a GPS tracking device on Appellant's car, through which they learned that on a number of occasions he had signed a seventeen-year-old boy onto Tyndall Air Force Base. Agents interviewed the boy, AP, who told them he and Appellant had met online, developed a sexual relationship, and continued to communicate

---

[1] **Without briefs, the Court granted review of an issue addressing the constitution of the lower court. That issue is moot per our holding in *United States v. Dalmazzi*, 76 M.J. 1, 3 (C.A.A.F. 2016).** The exact issue granted was:

> Whether the 9 November 2011 search authorization was overbroad in failing to limit the dates of the communications being searched, and if so, whether the error was harmless.

[2] On May 11, 2017, Appellant filed two additional motions requesting that the Court consider whether Appellant's counsel was ineffective in failing to file in a timely manner Appellant's additional issues pursuant to *United States v. Grostefon,* 12 M.J. 431 (C.M.A. 1982). These motions are denied. On May 24, 2017, Appellant filed a motion for leave to correct errata in a previous motion. This motion is granted. On May 24, 2017, and May 25, 2017, Appellant filed two separate motions for leave to supplement the record. These motions are denied.

[3] Children in the Big Brothers Big Sisters program are commonly referred to as "little brothers" and "little sisters."

online as their relationship evolved. Several weeks later AP recanted the portion of his statement about himself and Appellant having a sexual relationship.

AFOSI coordinated with the local sheriff's office who assumed the primary investigative role in Appellant's relationship with AP. However, AFOSI agents did utilize information from AP's statement to obtain a search authorization for Appellant's residence and person for items used to electronically communicate with AP, requesting the seizure of "[a]ll electronic media and power cords for devices capable of transmitting or storing online communications." The affidavit accompanying the search request stated that AFOSI, in tandem with the Bay County Sherriff's Office, was investigating Appellant's violation of a Florida statute "Computer Pornography; Traveling to meet a minor."[4] The affidavit detailed the investigation into Appellant's relationship with AP, including the fact that the sexual relationship had been ongoing since approximately April 2011 with sexually explicit online communications starting about a year earlier. The affidavit did not mention Appellant's history or any potential allegations connected with the Big Brothers Big Sisters program.[5] On November 9, 2011, agents seized a number of electronic devices from Appellant's home. The following day, the Bay County Sherriff's Office arrested Appellant and seized all electronic devices on his person. Among the items seized from Appellant himself was a personal laptop, which was handed over to AFOSI on November 24, 2011.

AFOSI agents sent the electronic devices they had collected to the Defense Computer Forensic Laboratory (DCFL) so that DCFL could extract data to be searched. The DCFL

---

[4] The lower court summarized the relevant section of the Florida statute as follows:

> The Florida state statute defines "traveling to meet a minor" as, inter alia, a person who travels within the state in order to engage in an illegal sexual act with a child under the age of 18 years after using a computer online or Internet service to seduce, solicit, lure or entice the child to do so.

[5] At one point, Special Agent Nishioka testified that he was searching for communication between Appellant and AP or the "little brothers." However, there was no mention of communication with "little brothers" in the warrant or affidavit.

application form required submission of both case background information and a copy of the search authority documentation. The case background information provided by AFOSI agent Sara Winchester included the accusations of the former "little brother" which formed the genesis of the investigation and detailed how this led to the identification of an investigation into Appellant's relationship to AP and the subsequent seizure of the electronic materials. Agent Winchester requested that DCFL:

> Search SUBJECT's Cell Phones, laptop computers, digital cameras and memory cards for all videos, images and possible online communication. To include, but not limited to the following: any and all information saved or maintained on SUBJECT's cellular telephones, laptop computers or hard drives; all associated SIM cards, components, peripherals or other data, relating to the matter being investigated.

Unfortunately, SA Winchester's request did not clarify that the "matter being investigated" was Appellant's communication with AP between 2010 and 2011, not the earlier accusation by the "little brother." DCFL created a mirror image of the data on the devices and placed that data on a forensic data extraction (FDE). As Mr. Kleeh, the forensics examiner, described the extraction process, "it goes through the image – the mirrored copy of the drive, it looks for those files, pictures, chat logs, Word documents, Internet history, and it pulls them all out and throws them into a directory on a new drive."

The first batch of extracted data (FDE #1) was returned to AFOSI on December 23, 2011, and around January 4, 2012, Special Agent Nishioka conducted a search of the data. FDE #1 contained materials found on Appellant's personal laptop as well as from two seized loose hard drives. Agent Nishioka described in his statement that "DCFL simply dumped all pictures and on-line chats from these drives onto one big drive for review." Agent Nishioka plugged the FDE into a stand-alone laptop and, utilizing a graphic user interface or GUI, opened the FDE in which all the materials extracted were arranged in folders and subfolders. He testified that he worked through the FDE folders in the order they were listed, beginning with the "pictures" folder. Agent Nishioka stated that he started by going through the "at-

tributable" folder. He then moved on to the folders of "unattributable" material. It appears that by using the term "unattributable" Agent Nishioka was referring to what Mr. Kleeh testified to as unallocated or deleted material. Mr. Kleeh testified that unallocated materials are deleted files that remain in the system but potentially without dates and times attached.

While searching the unallocated pictures, Agent Nishioka encountered an image that appeared to be child pornography. He stopped his search and sought an additional authorization to search for child pornography. A search of the remainder of FDE #1, pursuant to the additional authorization, turned up thousands of suspected child pornography images. The discovery of child pornography on these devices formed the basis for additional search authorizations, turning up more images which led to the charges of possessing child pornography and indecent acts of which Appellant was ultimately convicted.

At trial, Appellant moved to suppress the evidence derived from the November 9, 2011, search authorization because it was overbroad. The military judge denied Appellant's motion. The scope and propriety of that initial search authorization is now at issue in this appeal.

Discussion

"A military judge's decision to admit evidence is reviewed for an abuse of discretion." *United States v. Hills*, 75 M.J. 350, 354 (C.A.A.F. 2016). "An abuse of discretion occurs when we determine that the military judge's findings of fact are clearly erroneous or that he misapprehended the law." *United States v. Clayton*, 68 M.J. 419, 423 (C.A.A.F. 2010). When we review a decision on a motion to suppress, 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). We review de novo questions regarding whether a search authorization is overly broad. *United States v. Maxwell*, 45 M.J. 406, 420 (C.A.A.F. 1996). "Evidence derivative of an unlawful search, seizure, or interrogation is commonly referred to as the 'fruit of the poisonous tree' and is generally not admissible at trial." *United States v. Conklin*, 63 M.J. 333, 334 (C.A.A.F. 2006) (citing *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)).

A search authorization, whether for a physical location or for an electronic device, must adhere to the standards of the Fourth Amendment of the Constitution. The Fourth Amendment states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. This insistence on particularity is a defining aspect of search and seizure law.

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Maryland v. Garrison, 480 U.S. 79, 84 (1987). "The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings." *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999).

Despite the importance of preserving this particularity requirement, considerable support can be found in federal law for the notion of achieving a balance by not overly restricting the ability to search electronic devices.

> The prohibition of general searches is not to be confused with a demand for precise ex ante knowledge of the location and content of evidence .... The proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation.

United States v. Richards, 659 F.3d 527, 541 (6th Cir. 2011) (alteration in original) (quoting *United States v. Meek,* 366 F. 3d 705, 716 (9th Cir. 2004)); *see id.* at 540–42 (court allowing the search of an entire server known to contain websites harboring child pornography). "[I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives." *United States v. Burgess*, 576 F.3d 1078, 1094–95 (10th Cir. 2009) (court upholding a warrant to search "all computer records" for evidence of drug

trafficking). Instead of attempting to set out bright line rules for limiting searches of electronic devices, the courts have looked to what is reasonable under the circumstances. "As always under the Fourth Amendment, the standard is reasonableness." *United States v. Hill*, 459 F.3d 966, 974–77 (9th Cir. 2006) (court upholding an off-site search of all of the defendant's computer storage media for evidence of child pornography).[6]

Searches of electronic devices present distinct issues surrounding where and how incriminating evidence may be located. While we support the notion that "warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material," *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005), we also recognize the dangers of too narrowly limiting where investigators can go. As stated by the United States Court of Appeals for the Seventh Circuit, "[u]nlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents." *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010). "[I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files. It is particularly true with image files." *Burgess*, 576 F.3d at 1094; *see also United States v. Williams*, 592 F.3d 511, 521–22 (4th Cir. 2010) (positing an implied authorization for officers to open each file on the computer and view its contents, at least cursorily, to determine whether it falls within the scope of the warrant's authorization. "To be effective, such a search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance"). Of course our reluctance to prescribe ex ante limitations or require particular search methods and protocols does not render them immune from an ex post reasonableness analysis. *See, e.g., United States v. Christie*, 717 F.3d 1156, 1167 (10th Cir. 2013) ("[E]ven if courts do not specify particular search protocols up front in the warrant application process, they retain the flexibility to assess the reasonableness of the

[6] Obviously, what is reasonable in one instance may not be so in another.

search protocols the government actually employed in its search after the fact, when the case comes to court, and in light of the totality of the circumstances.").

In charting how to apply the Fourth Amendment to searches of electronic devices, we glean from our reading of the case law a zone in which such searches are expansive enough to allow investigators access to places where incriminating materials may be hidden, yet not so broad that they become the sort of free-for-all general searches the Fourth Amendment was designed to prevent.

> On one hand, it is clear that because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required.... On the other hand, ... granting the Government a *carte blanche* to search *every* file on the hard drive impermissibly transforms a "limited search into a general one."

United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011) (citations omitted).

Appellant argues that the November 9, 2011, authorization was overbroad because it did not contain a temporal limitation when that information was available and known to investigators. Applying the above Fourth Amendment law, we conclude that the authorization did not require a date restriction because it was already sufficiently particularized to prevent a general search. Though a temporal limitation is one possible method of tailoring a search authorization, it is by no means a requirement. Here, the authorization and accompanying affidavit did not give authorities carte blanche to search in areas clearly outside the scope of the crime being investigated. They were entitled to search Appellant's electronic media for any communication that related to his possible violation of the Florida statute in his relationship with AP.

We also conclude that the authorization allowed for a search of the unallocated space and through potential communications materials that did not have an immediately clear date associated with them. The precise extraction process utilized by Agent Kleeh and the accessibility of metadata on unallocated materials was not fleshed out in trial or anywhere on the record. However, we deduce from

Mr. Kleeh's testimony that metadata for unallocated materials often does not exist or is difficult to extract. We conclude that the possibility that relevant communications could have existed among the unallocated materials provided sufficient basis to subject those materials to an authorized and particularized search.

The record also does not disclose the origin of the first image of child pornography encountered by Agent Nishioka. Though he indicates he saw it in the folder of unallocated or unattributable materials, we do not know whether the specific image was drawn from the laptop or one of the two external hard drives. A list of images compiled by the Government as potential Rule for Courts-Martial 404(b) evidence indicates that child pornography from both the laptop and one of the external hard drives appeared in the unallocated folder viewed around January 4, 2012. This is supported by testimony from Mr. Kleeh. Neither Agent Nishioka nor trial counsel indicated any obvious delineation between materials found on individual devices in their description of what was contained on FDE #1. The issue of the shutdown dates of the two loose hard drives was raised during oral argument and addressed by both parties in subsequent motions. The FDE lists the shutdown dates for the hard drives as 2006 and 2008, years before Appellant initiated his relationship with AP. Assuming the shutdown dates were indicative of the timing of their last use, these materials were outside the scope of the search authorization, which described criminal activity dating no earlier than approximately April 2010. However, because images of child pornography from the laptop, with a last shutdown date in 2011, appeared in the unallocated materials Agent Nishioka searched, we conclude that he either did discover or inevitably would have discovered child pornography that validly lay within the scope of the search regardless of the significance of the shutdown dates on the two loose hard drives.

Agent Nishioka's discovery of the child pornography images within the folder of unallocated materials was consistent with *Horton v. California* and the plain view exception to the Fourth Amendment. 496 U.S. 128 (1990). Under *Horton*, in order for the plain view exception to apply: (1) the officer must not violate the Fourth Amendment in arriving at the spot from which the incriminating materials can be plainly viewed; (2) the incriminating character of the mate-

rials must be immediately apparent; and (3) the officer must have lawful access to the object itself. *Id.* at 136–37. Here, Agent Nishioka was lawfully searching through the extracted files based on what we have determined to be a valid authorization when he encountered what appeared to be child pornography among the unallocated materials. Upon spotting the child pornography, he properly stopped his search and obtained a new authorization that allowed him to search specifically for child pornography.

We hold that the November 9, 2011, search authorization was sufficiently particularized to avoid any violation of Appellant's Fourth Amendment rights and uphold the military judge's decision not to suppress evidence derived from the fruits of that authorization.

Decision

The decision of the United States Air Force Court of Criminal Appeals is affirmed.