UNITED STATES AIR FORCE COURT OF CRIMINAL APPEALS

U N I T E D S T A T E S,	**)**	**Misc. Dkt. No. 2009-15**
Appellant	**)**	
	)	
v.	**)**	
	)	**ORDER**
Airman First Class (E-3)	**)**	
ADAM G. COTE,	**)**	
USAF,	**)**	
Appellee	**)**	**Special Panel**

GREGORY, Judge

On 22 December 2009, counsel for the United States filed an Appeal Under Article 62, UCMJ, 10 U.S.C. § 862, in accordance with this Court's Rules of Practice and Procedure, asserting that the military judge erred as a matter of law in suppressing the evidence discovered through forensic review of the appellee's computer devices occurring after the 90-day search warrant "deadline" because the delay in completing forensic review was reasonable under the Fourth Amendment.[1]

Background

While conducting an internet peer-to-peer child pornography investigation in May 2008, Special Agent (SA) SH of the North Dakota Bureau of Criminal Investigation (NDBCI) discovered nine files of suspected child pornography on a computer with a specific internet protocol (IP) address. He contacted SA BN of Immigrations and Customs Enforcement (ICE) to subpoena the name and address of the subscriber. The internet service provider identified the subscriber as the appellee and his location as Minot Air Force Base, North Dakota.

SA BN received search authorization for the appellee's Minot Air Force Base dormitory room in a written warrant issued by the Federal Magistrate, United States District Court for the District of North Dakota, on 1 July 2008. The warrant commanded that the search of the dormitory room be completed by 10 July 2008, and authorized the seizure of any items listed in an attachment to the warrant to include electronic devices and storage media. SA SH and SA BN executed the warrant on 2 July 2008 and seized, among other items, a Sony laptop computer, a Hewlett-Packard (HP) laptop computer, and a Western Digital (WD) external hard drive. During an on-site forensic preview of

[1] U.S. CONST. amend. IV.

the devices, SA SH found "one or two" files believed to be child pornography on the Sony but was unable to preview the HP or WD drives.

The addendum to the warrant directed that the search of any electronic device or storage media seized during the search be completed within 90 days. Notably, this clause does not apply to electronic data or documents – only the electronic devices and storage media themselves. On 18 August 2008, within the 90-day time limit specified in the warrant, SA SH made forensic copies of the data on the Sony and HP laptop hard drives and stored the copies on clean NDBCI hard drives. He found two suspected child pornography videos on the copy of the Sony drive but the data on the copy of the HP drive was scrambled. SA SH was unable to copy or analyze the data on the WD drive.

In July 2009, almost a year later, government counsel requested that SA SH conduct additional analysis of the Sony and HP drives. He conducted all such subsequent analysis of the data found on these two drives using the forensic copies he had made the previous year. On the copy of the HP drive he found three suspected child pornography videos that appeared to match three of the nine he had initially observed in May 2008. On the Sony he found internet search histories relevant to the charged possession offense.

In September 2009 the Air Force Office of Special Investigations sent the WD drive, which had been in their custody for the past year, to the Defense Computer Forensics Laboratory (DCFL) for possible repair. DCFL repaired the drive, made a forensic copy of the data, and sent both to SA SH. In October 2009, SA SH analyzed the forensic copy of the WD drive and found 22 video files of suspected child pornography.

Charged with three specifications of possessing child pornography and one specification of distributing child pornography, in violation of Article 134, UCMJ, 10 U.S.C. § 934, the appellee moved to suppress all evidence obtained from the searches of the three computer drives and the forensic copies of those drives that occurred after 28 September 2008, the 90-day deadline imposed by the search warrant for searches of devices or media seized pursuant to the warrant. The military judge granted the motion, essentially finding that any analysis of the drives, data in drives, or copies of data in drives after the warrant's 90-day limit violated the warrant and was, therefore, unlawful. Although she expressly found "good cause" for getting an extension of time from the magistrate if the government had requested it, she nevertheless held that the evidence must be suppressed.

On 6 November 2009, the trial counsel filed a notice of government appeal of the ruling by the military judge with this Court. On 22 December 2009, the government submitted its appeal pursuant to Article 62, UCMJ. We find jurisdiction to hear the appeal since the ruling excluded substantial evidence material to the proceedings: specifically 25 child pornography video files (three on the HP and 22 on the WD) and the internet search history. We review rulings on the admission or exclusion of evidence for an abuse of discretion. *United States v. Rodriguez*, 60 M.J. 239, 246 (C.A.A.F. 2004).

We are bound by the military judge's factual findings unless they are clearly erroneous, and we consider conclusions of law de novo. *United States v. Terry*, 66 M.J. 514, 517 (A.F. Ct. Crim. App. 2008).

The Sony and HP Drives

We find the military judge erred in excluding data from the Sony and HP drives because (1) the 90-day time limit in the warrant only applies to devices and media, not data and (2) no reasonable expectation of privacy exists in government copies of lawfully seized data. For his July 2009 analysis, SA SH used forensic copies lawfully in possession of the government rather than the original devices or media seized from the appellee. In finding this search of the forensic copies a violation the warrant's 90-day time limit to search devices or media, the military judge apparently equated data contained in the government's forensic copies with the original devices and media.[2] The facts do not support this conclusion.

The warrant clearly distinguishes three types of material: electronic devices, storage media, and electronic data. As stated in the addendum to the warrant, the 90-day time limit for searches clearly applies only to seized devices and media, not the data on such devices and media: "The search of any *Electronic Device* or *Storage Media* authorized by this warrant shall be completed within 90 days from the date of the warrant unless, for good cause demonstrated, such date is extended by an order of the Court." Emphasis added. Highlighting this distinction between devices, media, and data, the warrant later authorizes *retention of devices and media* that contain contraband but directs the return of *copies of data* on such devices and media that do not contain contraband.

This construction of the warrant is consistent with the view that computer searches are a "two-step process" of first seizing devices and media and then later searching the data. 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE, § 4.7 (4th ed. supp. 2009-10) (citing Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 86 (2005)). Indeed, in her ruling the military judge recognized the routine practice of law enforcement to make forensic copies of computer data for later analysis, but then mistakenly applied the 90-day restriction to that copied data. Consistent with routine practice, SA SH lawfully copied and stored the electronic data from the Sony and HP storage media onto government servers within the time specified in the warrant. His later analysis of that data in the forensic copies did not violate the warrant's 90-day time limit for searches of electronic devices or media seized from the appellee.

[2] In ruling on a motion for reconsideration, the military judge rejected any distinction between data, copies of data, and the devices themselves and appears to confuse the terms in discussing the 90-day search time limit: "The warrant . . . doesn't state that the government can continue to search that *data* after the 90 days has expired." Emphasis added. The 90-day limit expressly applies only to electronic devices and storage media, not data.

This construction is also consistent with the settled view that, contrary to the military judge's conclusion, no reasonable expectation of privacy exists in copies made of lawfully seized data. The Fourth Amendment requires a warrant to search only those areas in which a reasonable expectation of privacy exists. *Rakas v. Illinois*, 439 U.S. 128 (1978). In *Vaughn v. Baldwin*, 950 F.2d 331 (6th Cir. 1991), a case involving the analogous situation of paper copies of seized documents, the court recognized the government's right to copy records lawfully in its possession and "to keep the copies after the plaintiff regained possession of the originals." *Vaughn*, 950 F.2d at 333. Extending this rationale to computer data, the court in *United States v. Megahed*, 2009 WL 722481, slip op. at 3 (M.D. Fla. Mar. 18, 2009), found no reasonable expectation of privacy in a mirror image copy of a hard drive that FBI agents obtained by consent despite later revocation of consent.

Here, the warrant itself excludes data from the 90-day time limit for searches and thereby implicitly recognizes both the standard two-step practice of searching computer data after seizure of computer devices as well as the lack of any reasonable expectation of privacy in copies of such data that is lawfully seized. The appellee correctly argues a privacy interest in personal computer files, devices, and data, citing *United States v. Conklin*, 63 M.J. 333, 338 (C.A.A.F. 2006). However, his privacy interest was lawfully breached by a warrant based on probable cause, and later examination of the data seized pursuant to that warrant violates neither the Fourth Amendment nor the warrant. *See United States v. Habershaw*, 2002 WL 33003434 (D. Mass. May 13, 2002) (forensic analysis of imaged hard drive seized pursuant to warrant does not constitute a second execution of the warrant "any more than would a review of a file cabinet's worth of seized documents.") The appellee had no reasonable expectation of privacy in lawfully seized copies of data, and the subsequent search of that data did not violate the Fourth Amendment. Therefore, the military judge abused her discretion in suppressing the data from the Sony and HP devices contained on forensic copies of lawfully seized material made within the 90-day time limit for searching the devices.

The WD Drive

Unlike the forensic copies of the data on the Sony and HP devices, the data on the WD device was not copied within the 90-day time limit specified for searches of electronic devices. DCFL made the WD forensic copy after repairing the device over a year after the 90 days expired, and SA SH searched the data on this forensic copy shortly thereafter. We agree with the military judge's finding that the DCFL search of the WD device and the derivative search of the data violated the 90-day time limit in the warrant for searches of devices and media, but we find the military judge erred in concluding that the violation in this case required suppression of the evidence.

"The Fourth Amendment by its terms prohibits 'unreasonable' searches and seizures." *New York v. Class*, 475 U.S. 106, 116 (1986). "The relevant test is not the reasonableness of the opportunity to procure a warrant, but the reasonableness of the

seizure under all the circumstances. The test of reasonableness cannot be fixed by per se rules; each case must be decided on its own facts." *Coolidge v. New Hampshire*, 403 U.S. 443, 509-10 (1971) (Black, J., concurring and dissenting). "[T]he Court has insisted upon probable cause as a minimum requirement for a reasonable search permitted by the Constitution." *Chambers v. Maroney*, 399 U.S. 42, 51 (1970).

The Fourth Amendment requires specificity as to the property to be searched, and searches that exceed the scope permitted by the warrant are invalid absent some exception. *United States v. Osario*, 66 M.J. 632 (A.F. Ct. Crim. App. 2008) (law enforcement agents went beyond the scope of the subject matter described in the warrant). However, unlike the specificity required for the place to be searched, the Fourth Amendment does not require expiration dates in search warrants and, in fact, "contains no requirements about *when* the search or seizure is to occur or the *duration*." *United States v. Gerber*, 994 F.2d 1556, 1559 (11th Cir. 1993). Consequently, violations of time requirements in a warrant do not per se equate to a constitutional violation. When a warrant or procedural rule imposes a time requirement on execution, admissibility of evidence obtained depends on whether the failure to search within the specified time violates the fundamental requirements of the Fourth Amendment. *Id*. at 1560; *see* Mil. R. Evid. 315(h)(4) (errors in execution of warrant affect admissibility only where constitutionally required).

Several considerations impact the constitutional analysis necessary to determine admissibility of evidence obtained after expiration of time requirements imposed by rule or warrant. First, and most obvious, violation of time requirements imposed by rule or warrant results in a constitutional violation when probable cause lapses during the delay. *United States v. Brewer*, 588 F.3d 1165, 1173 (8th Cir. 2009). Analyzing a violation of a federal rule requirement that search warrants be executed within a specified number of days,[3] the court in *Brewer* upheld the search of a computer several months after it was seized pursuant to a warrant since probable cause continued to exist: "[O]ur analysis of the delay in executing the warrants considers only whether the delay rendered the warrants stale." *Id*. In the present case, the military judge expressly found "good cause" for extending the time permitted in the warrant and the evidence supports that finding. The delay had absolutely no impact on probable cause since, as in *Brewer*, the computer device had been in the continuous custody of law enforcement since it was seized. Also, probable cause to believe that contraband images existed on the WD device was even greater since only a couple of the images originally observed had been located on the Sony and HP devices. Thus, violation of the time requirement in the warrant did not result in a constitutional violation based on the lapse of probable cause.

Second, the policy underlying the time requirement assists in determining whether a violation rises to a constitutional level. Where the policy is intended to implement the

[3] At the time of *United States v. Brewer*, 588 F.3d 1165 (8th Cir. 2009), Fed. R. Crim. P. 41(e)(2)(A) required that warrants direct execution "within a specified time no longer than 10 days;" however, the 2009 amendments to the Rules revised this to 14 days.

Fourth Amendment's probable cause requirement, the appropriate constitutional analysis is whether violation of the policy actually resulted in a lapse of probable cause. *Id*. In the present case, the language in the warrant clearly shows that the policy behind the warrant's time requirement is the return of seized property or data that does not contain contraband rather than implementation of some Fourth Amendment requirement. The warrant directs return of seized devices and media only if contraband is not found on them and directs return of *copies* of data files that have either (1) been already searched and not seized or (2) not searched because they are beyond the scope of the warrant. Because the WD drive was inoperable the government could not comply with the warrant's requirement to return non-contraband items until it could be repaired and searched.[4] The warrant's recognition of the personal utility of computer devices, media, and data files by requiring the search to be completed within 90 days so that non-contraband items could be returned to the owner does not implement any constitutional requirement such that violation requires suppression of the evidence.

By focusing on constitutional requirements, the court in *Brewer* rejects a mechanistic approach to the exclusion of evidence based on violation of time requirements in a rule or warrant. Relying on *United States v. Brunette*, 76 F. Supp. 2d 30 (D. Me. 1999), the appellee argues for such an approach. In *Brunette*, the court suppressed the results of a search that occurred only a few days after the expiration of a time requirement in the warrant. Though the court did not discuss whether this equated to a Fourth Amendment violation, the discussion of precedent in the opinion appears to focus on the Fourth Amendment's probable cause requirement by highlighting that the "element of time can admittedly affect the validity of a search warrant" and that "a search pursuant to a stale warrant is invalid." *Brunette*, 76 F. Supp. 2d at 42 (internal citations omitted). To the extent that *Brunette* stands for de facto exclusion of evidence based on violation of time requirements in a rule or warrant, the *Brewer* court implicitly rejects that view in favor of a constitutional analysis to determine the admissibility of evidence. *Brewer*, 588 F.3d at 1172 (citing *United States v. Syphers*, 426 F.3d 461 (1st Cir. 2005)).

Like *Brewer*, the court in *Syphers* looks to the policy underlying a particular time requirement to determine whether a constitutional violation occurred such that the evidence seized must be suppressed: where the policy is intended to ensure probable cause, violations of time requirements will result in suppression of evidence where probable cause lapses as a result of the violation. Analyzing a warrant's one-year time

[4] We find error in the military judge's conclusion that the evidence would not have been inevitably discovered. Assuming, arguendo, that the delayed search of the WD drive rose to the level of a constitutional violation, we find that the evidence would have been inevitably discovered in the normal course of processing seized evidence. Mil. R. Evid. 311(b)(2). As discussed above, the warrant directed the return of only those devices and media that did not contain contraband. Although agents could not access the inoperable WD drive, probable cause to believe that child pornography would be found on it continued to exist. Therefore, the drive could not be returned to the owner without analyzing it for contraband. To ultimately dispose of the property as directed by the warrant, agents would have had to either repair it and analyze it for contraband or destroy it. A demand for the return of the property by the appellee would trigger further efforts to analyze the device for contraband, but the record contains no evidence that such a demand had been made at the time of trial.

limit to conduct a computer search that violated a federal requirement to execute search warrants within ten days, the court in *Syphers* found the delayed search constitutional because (1) probable cause had not lapsed, (2) the delay did not prejudice the defendant, and (3) law enforcement officers did not act in bad faith. *Syphers*, 426 F.3d at 469.

Application of the *Sypher's* constitutional analysis to the facts of the present case shows that the evidence obtained from the delayed search should not have been suppressed. First, as already discussed, probable cause did not lapse as a result of the delay since the data on the WD drive remained as it was on the date it was seized. Second, for reasons similar to those supporting continued probable cause, the evidence shows no prejudice in the sense that either (1) evidence was discovered after the delay that would not have been discovered had the search taken place before the delay or (2) the appellee's property rights were adversely affected. As with the continuing probable cause, the data remained unchanged and the appellee's property interest did not change from when the item was first seized. Third, the record shows no evidence of bad faith. The military judge's summary finding of "good cause" to get an extension not only recognizes the continued existence of probable cause but also implicitly finds no prejudice or bad faith, and we agree with that finding. Where we find error is in the military judge's conclusion that a violation of a time requirement in a rule or warrant requires suppression of the evidence where the delay did not rise to the level of a constitutional violation. Therefore, the military judge abused her discretion in suppressing the evidence obtained from the WD drive.

On consideration of the United States Appeal Under Article 62, UCMJ, it is by the Court on this 6th day of April, 2010,

ORDERED:

That the United States Appeal Under Article 62, UCMJ is hereby **GRANTED.**

The ruling of the military judge is vacated and the record is remanded for further proceedings consistent with this opinion.

(BRAND, Chief Judge and THOMPSON, Judge participating)

FOR THE COURT

OFFICIAL

STEVEN LUCAS, YA-02, DAF
Clerk of the Court