5 September 2012

IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES, *Appellee,* v. Airman First Class (E-3) ADAM G. COTE, USAF, *Appellant.*	)))))))))	FINAL BRIEF ON BEHALF OF THE UNITED STATES Crim. App. Dkt. ACM 37745 USCA Dkt. No. 12-0522/AF

FINAL BRIEF ON BEHALF OF THE UNITED STATES

BRIAN C. MASON, Capt, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
Court Bar No. 33634

C. Taylor Smith, Lt Col, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
Court Bar No. 31485

GERALD R. BRUCE
Senior Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
Court Bar No. 27428

DON M. CHRISTENSEN, Col, USAF
Chief, Government Trial and Appellate Counsel Division
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd. Ste. 1190
Joint Base Andrews, MD 20762
(240) 612-4800
Court Bar No. 35093

INDEX

TABLE OF AUTHORITIES

SUPREME COURT CASES

COURT OF APPEALS FOR THE ARMED FORCES

SERVICE COURTS OF CRIMINAL APPEALS

FEDERAL CASES

DISTRICT COURTS

MISCELLANEOUS

5 September 2012

IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES, *Appellee,* v. Airman First Class (E-3) ADAM G. COTE, USAF, *Appellant.*	)))))))))	FINAL BRIEF ON BEHALF OF THE UNITED STATES Crim. App. Dkt. ACM 37745 USCA Dkt. No. 12-0522/AF

TO THE HONORABLE, THE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES:

ISSUE PRESENTED

WHETHER EVIDENCE FOUND ON APPELLANT'S COMPUTER SHOULD BE SUPPRESSED BECAUSE IT WAS FOUND PURSUANT TO A SEARCH THAT VIOLATED THE TERMS OF THE WARRANT.

STATEMENT OF STATUTORY JURISDICTION

The Air Force Court of Criminal Appeals (AFCCA) reviewed this case under Article 66(c), UCMJ, 10 U.S.C. § 866(c) (2006). This Court has jurisdiction to review this case under Article 67(a)(3), UCMJ, 10 U.S.C. §867(a)(3) (2006).

STATEMENT OF THE CASE

Appellant's statement of the case is accepted.

STATEMENT OF THE FACTS

The pertinent facts of this case concern the government's securing a lawful search warrant against Appellant in July 2008, the government's execution of that warrant, and the government's subsequent attempts to conduct forensic analysis of the material lawfully searched and seized from Appellant's computer devices.

Appellant came under formal investigation by civilian law enforcement authorities on 30 May 2008 when Special Agent (SA) Steve Harstad of the North Dakota Bureau of Criminal Investigation (NDBCI) accessed the Gnutella file-sharing network and downloaded nine videos with hash values corresponding to suspected child pornography from IP address 24.111.205.252. (J.A. at 127.) On 2 June 2008, SA Brian Novlesky of Immigrations and Customs Enforcement (ICE) subpoenaed the name and address of the subscriber using the aforementioned IP address from service provider Midcontinent Communications. (J.A. at 128.) On 3 June 2008, Midcontinent Communications identified the subscriber as Adam Cote: BK211, Room 216, Minot Air Force Base, ND. (J.A. at 128.) That same day, SA Novlesky contacted the Air Force Office of Special Investigations (AFOSI) at Minot AFB and confirmed Appellant's name, address, and active duty status. (J.A. at 128.)

Having confirmed Appellant's military status and address, SA Novlesky then prepared an affidavit for a federal search warrant that was issued on 1 July 2008 by Federal Magistrate Judge Charles S. Miller, United States District Court for the District of North Dakota. (J.A. at 138-42.) The warrant commanded the search of Appellant's dorm room and the seizure of items listed in attachment "A" of the warrant, including computers, computer storage media and digital content, including

but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks, flash drives or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography. (J.A. at 138-42.) The warrant directed that the execution of the search take place on or before 10 July 2008 and contained the following addendum regarding electronic devices, storage media, and electronic data:

> The following requirements shall apply to any computer, printer, plotter, scanner, cell phone, camera, or other like electronic device capable of storing creating, displaying, transmitting or storing electronic data ("Electronic Device"), to any electronic storage media ("Storage Media"), and to any electronic data and documents that are seized and searched pursuant to the warrant:
>
> 1. 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.

(J.A. at 138-42.)

SA Novlesky and SA Harstad executed the warrant the following day, 2 July 2008, and seized the following relevant items from Appellant's dormitory room: one silver and black Canon Power Shot SD 630 camera; one blue ScanDisk 1.0 GB memory card; one silver Sony VAIO laptop; one black Western Digital

(WD) hard drive; and one HP Pavilion Entertainment PC laptop. (J.A. at 50.) On the same day while conducting an initial on-site forensic "preview" of the Sony files using "Encase" software, SA Harstad found two videos which he believed to be child pornography. (J.A. at 55.)

On 18 August 2008, SA Harstad searched the aforementioned items using Encase Software. To complete his search for evidence of child pornography, SA Harstad endeavored to "image" (*i.e.*, make an exact forensic copy on which to conduct evidentiary review and analysis) the hard drives for the Sony and HP laptops, as well as the WD external hard drive. (J.A. at 53-54.) However, SA Harstad was unable to get the computer to recognize the WD external hard drive. SA Harstad then attempted to use several other computers at NDBCI. However, he was unable to get any of the computers to recognize the WD external hard drive. (J.A. at 56-57, 149.) SA Harstad is not trained to repair broken hard drives. The NDBCI does not repair hard drives which are not operable. (J.A. at 56-58.)

On 18 August 2008, SA Harstad searched the WD external hard drive to the extent possible at NDBCI. (J.A. at 91-92.) Presuming that the WD external hard drive was inoperable, but also likely contained contraband (J.A. at 89-90.), SA Harstad transferred the WD to Minot AFB's AFOSI detachment where it was maintained in their evidence locker after 18 August 2008. (J.A.

at 144.) At no time prior to trial on 3 November 2009 did Appellant ever demand return of his WD, Sony or HP. (J.A. at 91.)

On or about 17 July 2009, at the request of trial counsel, SA Harstad continued his forensic analysis on the Sony and as a result was able to reconstruct Appellant's internet activity from 15 June-19 June 2008 and 1 July 2008 using the imaged hard drive. (J.A. at 60-83; 151-51.) In September 2009, after a discussion with the Defense Computer Forensic Laboratory (DCFL), Minot AFOSI submitted a request to have DCFL repair the WD in order to complete the search of its contents. (J.A. at 152-53.) AFOSI formally submitted the request on 8 September 2009. (Id.) Resources within the Department of Defense (DoD) to expertly repair computer hard drives with forensic precision are exceedingly scarce. The DCFL is the only laboratory within the DoD which is capable of hard drive repair. (J.A. at 102.) Within the DCFL, Mr. Lallis is one of only three people trained in hard drive repair. (Id.) Moreover, as Mr. Lallis testified, only approximately 40 percent of hard drive repair attempts are successful. (Id.)

Nonetheless, on 15 September 2009, Mr. Lallis received the inoperable WD and began undertaking its repair. Upon beginning his repair, Mr. Lallis noted that the external hard drive showed signs of a previous attempt to open the hard drive. (J.A. at

94-95.) Mr. Lallis attempted to attach the external hard drive to a Forensic Recovery Evidence Device; however, the drive was not detected. (J.A. at 95-96.) Mr. Lallis then removed the drive from its casing and removed the face cover from the drive itself. (J.A. at 97.) Mr. Lallis determined the head stack, which is used to read data from the platters in the drive, was in the wrong location. (J.A. at 98.) He used his training to place the headstack back in the correct location and inspected the drive for further damage. (J.A. at 98-99.) Subsequently he put the hard drive back into its casing and turned on the drive. (J.A. at 99.) After he repaired the drive, he created a digital image of the external hard drive. (J.A. at 99-101.) Mr. Lallis verified that the hash values were correct and verified the readability of the image created. (J.A. at 100-01.) He determined that the drive was readable and completed his work on the repair on 2 October 2009. (J.A. at 154-59.)

Search of the WD began on 18 August 2008 and was interrupted only due to technical difficulties with repairing the then-inoperable WD. (J.A. at 56-57.) After discovering that the WD could in fact be repaired, the government moved to repair, image, and analyze the data from the WD within approximately one month's time (8 September 2009 – 8 October 2009). (J.A. at 58-59, 94-99, 152-67.) The WD was at all times the property of the NDBCI.

Additional facts necessary to the disposition of these issues are set forth in argument below.

SUMMARY OF THE ARGUMENT

Appellant's request for relief should be denied in that the repair and subsequent analysis of Appellant's media seized pursuant to a federal warrant was reasonable because probable cause never lapsed, Appellant suffered no prejudice by the delay, and there was no bad faith on the part of the government. The fact that the repair and analysis was conducted after the timeframe articulated in the warrant does not render either the search unreasonable or the results inadmissible.

ARGUMENT

THE FORENSIC REVIEW OF APPELLANT'S EXTERNAL HARD DRIVE WAS REASONABLE UNDER THE FOURTH AMENDMENT.

Standard of Review

The standard of review is whether the military judge abused his discretion in denying a motion to suppress evidence. United States v. Rodriguez, 60 M.J. 239 (C.A.A.F. 2004); United States v. Ayala, 43 M.J. 296 (C.A.A.F. 1995). In reviewing a military judge's ruling on a motion to suppress, appellate courts review fact finding under the clearly erroneous standard and conclusions of law under the de novo standard. Ayala, 43 M.J. at 298. In addition, the evidence is considered in the light most favorable to the prevailing party. Rodriguez, 60 M.J. at

245 (citing United States v. Reister, 44 M.J. 409, 413 (C.A.A.F. 1996)).

Law and Analysis

As Mil. R. Evid. 315(h)(4) makes clear, technical violations in the execution of a warrant only result in suppression of the evidence concerned if suppression is "required by the Constitution of the United States or an applicable act of Congress." Even if this Court finds that continued forensic analysis of the hard drive beyond prophylactic 90-day deadline constituted a violation of the warrant, the search was not unreasonable under the Fourth Amendment. In granting the government's appeal of the military judge's ruling, the AFCCA correctly applied the three factor "reasonableness" analysis set forth in United States v. Syphers, 426 F.3d 461 (1st Cir. 2005), and concluded that the search was reasonable under the circumstances of this case. United States v. Cote, Misc. Dkt. 2009-15, unpub. op. at 5-7 (A.F. Ct. Crim. App. 6 April 2010) (citing United States v. Brewer, 588 F.3d 1165 (8th Cir. 2009)).

Appellant attempts to assert that upon finding a search was conducted outside of the time stated in a warrant, the search is, by definition, unlawful and "any evidence seized during the search [is] inadmissible." (App. Br. at 8.) This argument fails because the Fourth Amendment "contains no requirements

about when the search or seizure is to occur or the duration." United States v. Gerber, 994 F.2d 1556, 1559-60 (11th Cir. 1993). Moreover, a significant and growing number of federal jurisdictions confronting these "timeliness of execution" issues in the realm of computer forensic searches are analyzing this issue similarly to the way the Military Rules of Evidence do, by applying a constitutional "reasonableness" analysis to the length of delay. Specifically, the First Circuit Court of Appeals in Syphers created a helpful three-factor analytical framework to analyze the "reasonableness" of the delay by examining whether: (1) it resulted in a lapse of probable cause; (2) it created unfair prejudice to the defendant; and (3) it was caused by police bad faith. Syphers, 426 F.3d at 469.

While the government readily acknowledges that "unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant," delayed execution of a warrant does not necessarily render the seized evidence inadmissible. United States v. Marin-Buitrago, 734 F.2d 889, 894 (2d Cir. 1984); Syphers, 426 F.3d at 469 (citing United States v. Cafero, 473 F.2d 489, 499 (3rd Cir. 1973)). In Syphers, the Court examined the mandate of Federal Rule of Criminal Procedure 41 that all search warrants, once

issued, be executed within 10 days.[1] In fact, a string of federal courts have taken pains to emphasize that the policy behind the 10-day "execution requirement" is not expeditious processing alone, but rather, the prevention of "staleness" of probable cause. Syphers, 426 F.3d at 469 (citations omitted). Indeed, as courts confronting these issues post-Syphers have noted, "[a] delay must be reasonable, but there is no constitutional upper limit on reasonableness." United States v. Burns, 2008 U.S. Dist. LEXIS 4542990, *9, *26 (N.D.Ill. 2008).

While the Syphers factors provide a helpful analytical framework, Syphers, its antecedent, and subsequent case law make abundantly clear that the pivotal inquiry in adjudicating timeliness issues is whether probable cause has "dissipated" as a result of the delay.[2] Moreover, as courts have been apt to observe, ordinary Fourth Amendment concerns with "staleness" are essentially unnecessary where computer evidence is concerned, particularly when the computer has been seized by law

[1] It is important to note that the analysis in Syphers does not turn on the source of the time restriction, but rather any impact a delay may have had on the probable cause giving rise to the warrant.

[2] *See* Syphers, 426 F.3d at 469 (holding that a five-month delay did not invalidate the search of the appellant's computer because there was no showing that delay caused a lapse in probable cause); Burns, 2008 U.S. Dist. LEXIS at *26 (due to nature of computer evidence, ten-month delay had no effect on probable cause); United States v. Gorrell, 360 F.Supp.2d 48, 55 n.5 (D. D.C. 2004) (ten-month delay in conducting forensic search of computer and camera did not impact probable cause, referring to any proposed restraints on off-site forensic analysis as "prophylactic constraints" only); United States v. Hernandez, 183 F.Supp.2d 468, 480 (D.P.R. 2002) (upholding the forensic examination of several computer discs after the 10-day warrant execution period because when "[t]he documents are seized within the time frame established with warrant but examination of those documents may take a longer time, and extensions or additional warrants are not required.")

enforcement. "Once the officers obtained the computers and the discs, 'any danger that probable cause would cease to exist passed.'" United States v. Cameron, 652 F.Supp.2d 74, 81 (D.Me. 2009)(quoting United States v. Sturm, 2007 U.S. Dist. LEXIS 12261, *19 (D.Co. 2007).

Turning to the "prejudice" prong of the Syphers factors, "prejudice" in this context includes instances where, as a result of the delay, evidence is discovered that would otherwise have been undiscoverable had the search taken place prior to the delay (United States v. Burgess, 576 F.3d 1078, 1097 (10th Cir. 2009); or, where there was a marked affect on Appellant's property or possessory rights. (United States v. Johns, 469 U.S. 478, 487 (1985) (holding that to prove prejudice the owner of the property must prove delay in the completion of a search was unreasonable because it adversely affected a privacy or possessory interest).

The "bad faith" prong of the Syphers factors appears to deal with intentional and calculated delays by law enforcement for the purpose of delay. However, this type of "gamesmanship" is largely inapplicable to the computer forensic search arena for two reasons. First, no tactical advantage is gained by delay for delay's sake because the status of the evidence is "static and unchanging." Secondly, at the same time, courts have recognized that the demands of computer forensic searches

are considerably greater than other areas of evidence, calling for a more flexible approach to accommodate proper analysis: "it is no easy task to search a well-laden hard drive by going through all of the information it contains, let alone search through it and the disks for information that may have been 'deleted.'" United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).

Applying the Syphers factors to the case *sub judice*, Appellant fails on each prong. First, it is undisputed by all parties below, including the military judge in her ruling, that probable cause persisted as to Appellant's WD at all times pertinent to this case. (J.A. at 106-07.) Second, Appellant suffered no prejudice here insofar as the delay did not enable the government to discover anything that they would not have already discovered had they been able to image and analyze all three devices before 28 September 2008.[3] This is so given the

[3] In reversing the military judge's ruling, AFCCA noted the following:

"permanent and static nature" of the evidence preserved on the hard drive, and the fact that the government's seizure of the drive in July 2008 preserved the evidence on the drive just as it would have been at the time of its seizure. (J.A. at 103.) Despite his privacy interest assertion on appeal, Appellant suffered no prejudice in terms of property or possessory interest, as there is no evidence in the record that he ever made any request for the return of his property over this purportedly "unreasonable" span of time while the government's investigation was ongoing. (J.A. at 91.)

Finally, the delay involved in completing the forensic analysis of the devices was a function not of bad faith, but

---

> We find error in the military judge's conclusion that the evidence would not have been 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 [Appellant] 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.

Cote, unpub. op. at 6, n.4.

well-intentioned initial government ignorance over the possibility of employing scarce government resources to repair the damaged WD external hard drive. The military judge made no findings of fact asserting that the government acted in bad faith; rather she merely criticized the government for not requesting an extension of the warrant's search deadline. *See* Cote, unpub. op. at 7; (J.A. at 106-07). Bad faith will not be presumed merely by virtue of the relative absence of constant government diligence in propelling the investigation. *See* Burgess, 576 F.3d at 1097 (finding no bad faith in 45-day delay because "any delay was due to [law enforcement] efforts to make sure the job was done right"); Burns, 2008 U.S. Dist. LEXIS at *26 (declining to assume bad faith where 10-month delay in completion of forensic analysis of computer and no factual explanation offered by government).

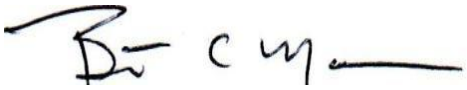
SA Harstad expended all reasonable efforts within his professional proficiency in attempting to facilitate timely forensic analysis by "imaging" the Sony, HP, and WD. (J.A. at 56-58.) To adduce "bad faith" because a determined trial counsel later dared to challenge the status quo and sought a way to repair and analyze the WD that had gone undisturbed in an evidence locker (while there was still probable cause to believe child pornography was on it) is not evidence of bad faith. Rather, it is evidence of due diligence "to make sure the job is

done right." Burgess, 576 F.3d at 1097. Accordingly, both the military judge's and AFCCA's finding that the government exhibited no bad faith in the execution of this warrant must be sustained.

Applying the Syphers factors as the appropriate level of constitutional review mandated by Mil. R. Evid. 315(h)(4) in evaluating whether alleged technical violations of warrant execution procedures require suppression of the evidence at trial proves the evidence should have been admitted. Accordingly, AFCCA was correct in reversing the military judge's ruling and holding that under the circumstances of this case, the delay in completing the forensic analysis of Appellant's hard drive was "reasonable" within the meaning of the Fourth Amendment. Cote, unpub. op. at 7. Appellant has provided no basis upon which this Court should disturb that well-founded decision on this issue.

CONCLUSION

WHEREFORE, the United States respectfully requests this Honorable Court uphold AFCCA's ruling affirming the findings and sentence.



BRIAN C. MASON, Capt, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd. Ste. 1190
Joint Base Andrews, MD 20762
(240) 612-4800
Court Bar No. 33634

C. Taylor Smith, Lt Col, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd. Ste. 1190
Joint Base Andrews, MD 20762
(240) 612-4803
Court Bar No. 31485

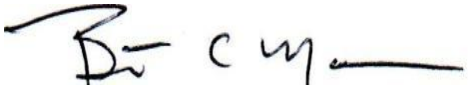
GERALD R. BRUCE
Senior Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd. Ste. 1190
Joint Base Andrews, MD 20762
(240) 612-4800
Court Bar No. 27428

FOR

DON M. CHRISTENSEN, Col, USAF
Chief, Government Trial and Appellate
Counsel Division
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd. Ste. 1190
Joint Base Andrews, MD 20762
(240) 612-4800
Court Bar No. 35093

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing was delivered to the Court and to Appellate Defense Division, on 5 September 2012.



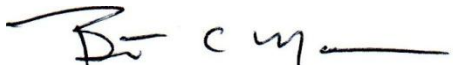
BRIAN C. MASON, Capt, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd. Ste. 1190
Joint Base Andrews, MD 20762
(240) 612-4800
Court Bar No. 33634

COMPLIANCE WITH RULE 21 (b)

1. This brief complies with the size limitation of Rule 21(b) because the brief is 18 pages.

2. This brief complies with the typeface and type style requirements of Rule 37 because:

☒ This brief has been prepared in a monospaced typeface using Microsoft Word Version 2007 with 10 characters per inch using Courier New.



BRIAN C. MASON, Capt, USAF

Attorney for USAF, Government Trial and Appellate Counsel Division

Date: 5 September 2012