"Damn the Torpedoes! Full Speed Ahead!"[1]—Fourth Amendment Search and Seizure Law in the 2008 Military Appellate Term of Court

Lieutenant Colonel Stephen R. Stewart, USMC
Professor, Criminal Law Department
The Judge Advocate General's Legal Center and School, U.S. Army
Charlottesville, Virginia

The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and 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.[2]

Introduction

This year's new developments in search and seizure jurisprudence saw the military appellate courts "comfortable in their own skin" as they handed down opinions on Fourth Amendment law as it related to computers and electronic media. This development is significant since over the past several years the courts have been circumspect in their decisions on computer related search and seizure issues.[3] This year's decisions from the Court of Appeals of the Armed Forces (CAAF)[4] and the service courts of criminal appeals[5] were confident and sure. If last year's term of court was viewed as "the collective military courts . . . applying the rudder, and aligning the course, of Fourth Amendment jurisprudence in terms of reasonable expectation of privacy in computers and digital media, as well as, scope of consent,"[6] then this was the year of "Damn the torpedoes! Full speed ahead!"[7]

If the military courts of appeals were considered dynamic this term of court, then the U.S. Supreme Court was somnolent.[8] The Supreme Court did not "damn" anything this year, and proceeded at about "quarter" speed in regard to the Fourth Amendment with a single case: *Virginia v. Moore*.[9] However, the coming October Term 2008 is truly exciting and should make up for the 2007 term with the following cases: *Pearson v. Callahan*,[10] *Arizona v. Gant*,[11] *Arizona v. Johnson*,[12] and *Herring v. United States*.[13]

---

[1] During the Civil War Battle of Mobile Bay in 1864, Rear Admiral Farragut rallied his fleet by uttering the words: "Damn the Torpedoes! Full Speed Ahead!" *See* National Park Service, David Glasgow Farragut, http://www.nps.gov/archive/vick/visctr/siteblt n/farragut.htm (last visited Feb. 11, 2009).

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

[3] *See, e.g.*, United States v. Long, 64 M.J. 57 (C.A.A.F. 2006).

[4] The CAAF 2008 term of court began on 1 October 2007 and ended 31 August 2008. *See* U.S. Court of Appeals for the Armed Forces, Opinions & Digest, http://www.armfor.uscourts.gov/Opinions.htm (last visited Feb. 11, 2009); *see infra* sec. II (discussing United States v. Larson, 64 M.J. 559 (A.F. Ct. Crim. App. 2006); United States v. Rader, 65 M.J. 30 (C.A.A.F. 2007); United States v. Gallagher, 65 M.J. 601 (N-M. Ct. Crim. App. 2007); United States v. Weston, 65 M.J. 774 (N-M. Ct. Crim. App. 2007)).

[5] *See generally* UCMJ art. 66 (2008); *see also* MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 1203 (2008) [hereinafter MCM].

[6] Lieutenant Colonel Stephen R. Stewart, *Practicing What the Court Preaches—2007 New Developments in Fourth Amendment Search and Seizure Law*, ARMY LAW., June 2008, at 1, 2; *see, e.g.*, *Larson*, 64 M.J. 559: *Rader*, 65 M.J 30.

[7] *Supra* note 1.

[8] The U.S. Supreme Court's October 2007 term began on 1 October 2007 and ended 30 September 2008. *See* Supreme Court of the United States 2007 Term Opinions of the Court, http://www.supremecourtus.gov/opinions/07slipopinion.html (last visited Feb. 16, 2009).

[9] 128 S. Ct. 1598 (2008). The *Moore* case, although not insignificant in its own right, addressed whether the police violated the Fourth Amendment "when they made an arrest that was based on probable cause but prohibited by state law, or when they performed a search incident to arrest." *Id.* at 1600. This case arose after Mr. Moore was pulled over and arrested for driving on a suspended license. *Id.* at 1601. He was searched incident to apprehension and sixteen grams of crack cocaine and $516 in cash was discovered on his person. *Id.* Under state law, Mr. Moore should have been issued a citation instead of arrested. *Id.* at 1602. Consequently, Mr. Moore argued that the evidence should be suppressed under the Fourth Amendment. *Id.* The Virginia Supreme Court agreed with Mr. Moore and reasoned "that since the arresting officers should have issued Moore a citation under state law, and the Fourth Amendment does not permit search incident to citation, the arrest search violated the Fourth Amendment." *Id.* at 1602. The U.S. Supreme Court overturned the Supreme Court of Virginia stating that "linking Fourth Amendment protections to state law would cause them to 'vary from place to place and from time to time.'" *Id.* at 1607 (citing Whren v. United States, 517 U.S. 806, 815 (1996)). Therefore, the Court ruled that "[w]hen officers have probable cause to believe that a person has committed a crime in their presence, the Fourth Amendment permits them to make an arrest, and to search the suspect in order to safeguard evidence and ensure their own safety." *Id.* at 1608.

[10] 129 S. Ct. 808 (2009). This case "raises the question of whether police officers may enter a home without a warrant immediately after an undercover informant buys drugs inside, and whether qualified immunity protects officers from civil rights claims arising from such searches." Kimberly Atkins, *October Term of U.S. Supreme Court Term Set to Begin*, LAWREADER, Sept. 29, 2008, http://news.lawreader.com/?p=2012.

This article is divided into two-parts and carries the same admonishment as stated in last year's article: "this year's symposium article should, and needs to, be viewed as the next in a series of articles regarding the continuing evolution of Fourth Amendment law."[14] Part I of this article addresses the new confidence demonstrated by the CAAF and the Air Force Court of Criminal Appeals (AFCCA) in applying search and seizure law in the context of computers.[15] Part II looks ahead to the 2008 Supreme Court term of court and the possible effect *Herring v. United States*[16] may have on the Exclusionary Rule.[17]

I. Computers and Search and Seizure Law

A. Introduction

Evidence that involves computers, or is derived from computers, can cause the most nimble legal mind to freeze when determining its admissibility. Whether it is the fear of technology, or the cognitive dissonance that occurs when a military court rules that a servicemember has a reasonable expectation of privacy in a government computer system,[18] the Fourth Amendment practitioner inevitably pauses to consider how search and seizure law is applied to new technology. Consequently, the advent of computer crime law helps us compartmentalize, organize, and analyze these seemingly nascent issues.

Computer crime law is fundamentally no different than typical criminal law. It is merely recognition of a shift from physical crimes to digital crimes.[19] The changes can be found in the facts of how and where crimes are committed as well as how and where evidence is collected.[20] Hence, computer crime law is bifurcated into two areas: substantive computer crime law and procedural computer crime law.[21]

Substantive computer crime law is the law governing the use of a computer to commit a crime.[22] It can be divided into two basic categories: computer misuse crimes and traditional crimes.[23] "Computer misuse crimes are a new type of criminal

---

[11] No. 07-542 (U.S. filed Oct. 24, 2007). The "Court will consider whether the Fourth Amendment requires law enforcement officers to demonstrate a threat to their safety or a need to preserve evidence related to the crime before conducting a warrantless search of a car after the occupants have been detained and removed from the vehicle." Atkins, *supra* note 10.

[12] 129 S. Ct. 781 (2009). "The justices will decide whether an officer conducting a pat-down after a stop for a minor traffic violation can search a passenger he believes to be armed and dangerous, even if he has no basis for believing the passenger is committing, or has committed, a criminal offense." Atkins, *supra* note 10.

[13] 129 S. Ct. 695 (2009). "The Court will consider whether evidence must be suppressed when an officer obtained the evidence in an arrest and car search relying solely upon seemingly credible—but factually erroneous—information negligently provided by another law enforcement agent." Atkins, *supra* note 10.

[14] Stewart, *supra* note 6, at 1.

[15] *See* United States v. Wallace, 66 M.J. 5 (C.A.A.F. 2008) (computers and the scope of consent); United States v. Larson, 66 M.J. 212 (C.A.A.F. 2008) (computers and the reasonable expectation of privacy); United States v. Michael, 66 M.J. 78 (C.A.A.F. 2008) (computers and the reasonable expectation of privacy in mislaid property and the reasonableness of a search); United States v. Osorio, 66 M.J. 632 (A.F. Ct. Crim. App. 2008) (computers and the scope of search vis-à-vis the execution of a valid search warrant).

[16] *Herring*, 129 S. Ct. at 695.

[17] The exclusionary rule is defined as "[a]ny rule that excludes or suppresses evidence obtained in violation of an accused person's constitutional rights." BLACK'S LAW DICTIONARY 587 (7th ed. 1999). There is academic debate on the import of the *Herring* decision on the Exclusionary Rule. Chief Justice Roberts, writing for the majority, stated that "unlawful police conduct should not require the suppression of evidence if all that was involved was isolated carelessness." Adam Liptak, *Justices Step Closer to Repeal of Evidence Ruling*, N.Y. TIMES, Jan. 31, 2009, at A1, *available at* http://www.nytimes.com/2009/01/31/washington/31scotus.html.

[18] United States v. Long, 64 M.J. 57 (C.A.A.F. 2006). In *Long*, the CAAF found that Corporal Long possessed a reasonable expectation of privacy in her government e-mail account on very specific facts supporting her subjective expectation of privacy. *Id.* at 66. Anecdotally, a number of Judge Advocates have expressed amazement that there would even be consideration of any expectation of privacy in government computer networks and systems as the networks and systems are used by the servicemember for the benefit of the government.

[19] ORIN S. KERR, COMPUTER CRIME LAW 1 (2006) ("There are two reasons to label criminal conduct a computer crime. First, an individual might use a computer to engage in a criminal activity. Second, the evidence needed to prove a criminal case might be stored in computerized form.").

[20] *Id.* "When the facts change, the law must change with it. Old laws must adapt and new laws must emerge to restore the function of preexisting law." *Id.* at 3. "Computer crime law is the search for and study of new answers to timeless questions of criminal law when the facts switch from a physical environment to a digital environment." *Id.*

[21] *Id.* at 1.

[22] *Id.*

offense involving intentional interference with the proper functioning of computers,"[24] whereas "traditional crimes are traditional criminal offenses facilitated by computers."[25]

Procedural computer crime law is the law governing the collection of computerized evidence.[26] Like its substantive aspect, procedural computer crime law consists of two discrete areas: statutory privacy law and the Fourth Amendment.[27] Where statutory privacy law addresses the law regulating digital evidence collection,[28] the Fourth Amendment aspect of procedural computer crime law measures the constitutional limits on digital evidence collection.[29]

The constitutional limits may be measured in the form of three questions: "When is retrieving evidence from a computer a search?"[30] "When is it a seizure?"[31] "When is the search or seizure reasonable?"[32] It is this last question that preoccupied the CAAF and the AFCCA this past term of court.

Four of the eight published Fourth Amendment cases in the collective military term of court addressed procedural computer crime law. These cases touched upon a plethora of seminal issues involving search and seizure law. For instance, *United States v. Wallace* addressed the issue of consent;[33] *United States v. Larson* revisited the issue of reasonable expectation of privacy in government computer systems;[34] *United States v. Michael* concerned the reasonableness of a search regarding misplaced property;[35] and *United States v. Osorio* analyzed the reasonableness of the execution of a valid search warrant.[36] These cases deserve a full discussion.

B. Computers and the Scope of Consent

The *Wallace* case illustrates the complexity of procedural computer crime law in regard to the issue of consent in computer searches.[37] Staff Sergeant (SSgt) Wallace, United States Air Force (USAF), was investigated for a sexual relationship he pursued with a fifteen-year-old female military dependent.[38] The Air Force Office of Special Investigations

---

[23] *Id.*

[24] *Id.* ("Examples include hacking offenses, virus crimes, and denial of services attacks. These offenses punish interference with the intended operation of computers, either by exceeding a user's privileges (e.g. hacking) or by denying privileges to others (e.g. denial of service attack).").

[25] *Id.* ("Examples include internet fraud schemes, online threats, distributing digital images of child pornography, and theft of trade secrets over the internet.").

[26] *Id.* at 2.

[27] *Id.*

[28] *Id.* ("[T]he law regulating digital evidence collection derives from three privacy statutes: The Wiretap Act, the Pen Register statute, and the Stored Communications Act."). "The Wiretap Act, Stored Communications Act, and Pen Register statute are complex surveillance statutes that were enacted to create a statutory form of the Fourth Amendment applicable to computer networks." *Id.* at 178. The Wiretap Act is shorthand for 18 U.S.C. § 2511—Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. 18 U.S.C. § 2511 (2006). The criminal provision of the Wiretap Act penalizes one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication." KERR, *supra* note 19, at 179 (citing 18 U.S.C. § 2511(1)(a)). "[T]he Pen Register statute is violated when a person obtains in real time the dialing, routing, addressing, and signaling information relating to an individual's telephone calls or Internet Communications." *Id.* (citing 18 U.S.C. § 3121). The Stored Communications Act is a "prohibition [of] a specific type of unauthorized access law, punishing one who 'intentionally accesses without authorization a facility through which an electronic communication while it is in electronic storage in such system." *Id.* at 179–80 (citing 18 U.S.C. § 2701(a)).

[29] KERR, *supra* note 19, at 2.

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] 66 M.J. 5 (C.A.A.F. 2008).

[34] 66 M.J. 212 (C.A.A.F. 2008).

[35] 66 M.J. 78 (C.A.A.F. 2008).

[36] 66 M.J. 632 (A.F. Ct. Crim. App. 2008).

[37] *Wallace*, 66 M.J. 5.

[38] *Id.* at 6.

(AFOSI) conducted the investigation.[39] Staff Sergeant Wallace was questioned by the AFOSI agents where he was read his Article 31 rights,[40] and agreed to speak with the agents without the presence of a lawyer.[41]

During and after the course of questioning, several dispositive actions by the AFOSI agents were taken to facilitate SSgt Wallace's cooperation. First, the agents informed SSgt Wallace "their investigation would reveal enough evidence to sentence [him] to confinement for life and would require [him] to register as a sex offender."[42] Staff Sergeant Wallace acknowledged that he had contacted the minor via e-mail and instant messenger.[43] Consequently, the agents sought and received SSgt Wallace's consent to search his personal computer and home for evidence.[44] After giving his consent, SSgt Wallace was escorted to his home by the agents, and they were joined by another AFOSI agent, SSgt Wallace's first sergeant, and a chaplain.[45] Staff Sergeant Wallace's wife arrived shortly thereafter, and SSgt Wallace and his wife then objected to the seizure of their home computer since it had "their life on it."[46] Finally, despite the protests of SSgt Wallace and his wife, the agents insisted that "they had to take [the computer]," leading SSgt Wallace to consent to its removal.[47] These actions led to the crux of the voluntariness issue, which the court considered.

The trial court and AFCCA were unsympathetic to SSgt Wallace's motion to suppress evidence which was "obtained from the search of [Wallace's] computer on the theory that [Wallace] involuntarily consented in the first place or, alternatively, revoked consent when he told agents not to take the computer."[48] The trial court denied the motion and found that SSgt Wallace freely consented, and that, in the alternative, if he had revoked his consent, the Government would have inevitably discovered[49] the images "because there was probable cause to search for e-mails and instant messages related to [Wilson's] relationship with the minor."[50] Staff Sergeant Wallace was found guilty at a general court-martial of carnal knowledge, sodomy, and possessing child pornography.[51] The CAAF addressed three issues in the context of voluntariness: (1) whether SSgt Wallace's initial consent to search his residence included seizure of his computer;[52] (2) whether SSgt Wallace's ultimate consent to seizure of his computer at his residence after revocation of his initial consent to do so was voluntary;[53] and (3) whether the doctrine of inevitable discovery was applicable to render admissible evidence of child pornography found on SSgt Wallace's computer subsequent to its illegal seizure pursuant to SSgt Wallace's involuntary

---

[39] *Id.*

[40] UCMJ art. 31(b) (2008).

> No person subject to this chapter may interrogate, or request any statement from an accused or a person suspected of an offense without first informing him of the nature of the accusation and advising him that he does not have to make any statement regarding the offense of which he is accused or suspected and that any statement made by him may be used as evidence against him in a trial by court-martial.

Id.

[41] *Wallace*, 66 M.J. at 6 ("He agreed to proceed without a lawyer when investigators could not make contact with the Area Defense Counsel.").

[42] *Id.*

[43] *Id.*

[44] *Id.* ("Appellant signed an AF Form 1364, entitled, 'Consent for Search and Seizure,' and consented to the general search of his home and computer.").

[45] *Id.*.

[46] *Id.* Staff Sergeant Wallace stated:

> [The computer] has our life on it. It has our photo albums on it. It's got our banking on it. All of our financial stuff is on there. You know, I use it to do all of our bill paying and everything else. Our online business is on there. I was like "You can't take it." Then my wife even started going nuts at that time.

Id.

[47] *Id.* ("[F]orensic analysis revealed the e-mail and chat traffic between [Wallace] and [the minor].").

[48] *Id.* at 7.

[49] *See* MCM, *supra* note 5, MIL. R. EVID. 311(b)(2) ("Evidence that was obtained as a result of an unlawful search or seizure may be used when the evidence would have been obtained even if such unlawful search or seizure had not been made.").

[50] *Wallace*, 66 M.J. at 7.

[51] *Id.*

[52] *Id.* at 5.

[53] *Id.*

consent.[54] As with most Fourth Amendment issues involving voluntariness, the facts and circumstances of this case are dispositive.[55]

Voluntariness is derived from all the circumstances,[56] or, as the Supreme Court has applied it, "totality-of-the-circumstances."[57] Hence, the CAAF applied this standard to two of the three claims SSgt Wallace made regarding his consent.[58] Staff Sergeant Wallace's first argued that his consent to the search of his home should have been limited in scope, especially after he revoked consent to seize his computer and then acquiesced to the AFOSI agents' authority.[59] The court recognized that SSgt Wallace could limit the scope of any search,[60] and found that the "argument [did] not fit the facts of this case."[61] The court simply looked to the "Consent for Search and Seizure" form which showed SSgt Wallace's explicit consent and the broad permission for investigators to "take any letters, papers, materials, articles or other property they consider to be evidence of an offense."[62] The interpretation the court gave this document is based on "objective reasonableness of the consent—not [Wallace's] supposed impression—that controls."[63] So, based on the "typical reasonable person," the court concluded that the AFOSI investigators were within their right to not only search, but to "remove the computer from the premises."[64] Staff Sergeant Wallace, however, did not concede the point. He argued that his wife's objection to the computer's removal constituted consent revocation.[65]

Staff Sergeant Wallace insisted his wife's objection constituted consent revocation based on the Supreme Court's holding in *Georgia v. Randolph*.[66] The CAAF is unconvinced. *Randolph* stands for the proposition that a "warrantless search of a shared dwelling for evidence over the express refusal of consent by a physically present resident cannot be justified as reasonable as to him on the basis of consent given to the police by another resident."[67] Whereas SSgt Wallace saw his circumstances in the same light as *Randolph*, the CAAF interpreted *Randolph* as not permitting a "non-accused co-resident to supersede the wishes of the accused co-resident."[68] In simpler words, the CAAF shut down this argument because "Fourth Amendment rights 'are personal rights which, like some other constitutional rights, may not be vicariously asserted.'"[69] Staff Sergeant Wallace, however, found his stride on his third argument regarding consent.

The CAAF agreed with SSgt Wallace that his second "so-called" consent amounted to mere "passive acquiescence to the color of authority" when the AFOSI agents informed him that "'they would have to take the computer' as 'a matter of routine.'"[70] The significance of this finding is the CAAF's formal adoption of the AFCCA non-exhaustive six *Murphy* factors in determining voluntariness under *Schneckloth's* totality of the circumstances analysis.[71] The factors are:

---

[54] *Id.*

[55] MCM, *supra* note 5, MIL. R. EVID. 314(e)(4) ("To be valid, consent must be given voluntarily. Voluntariness is a question to be determined from all the circumstances.").

[56] *Id.*

[57] *Wallace*, 66 M.J. at 8.

[58] *Id.*

[59] *Id.* at 7.

[60] *Id.* The CAAF looks to MRE 314(e)(3) which states that "consent to search may be limited in any way by the person granting consent, including limitations in terms of time, place, or property and may be withdrawn at any time." *Id.* (citing MCM, *supra* note 5, MIL. R. EVID. 314(e)(3)).

[61] *Id.*

[62] *Id.* at 7–8.

[63] *Id.* at 8.

[64] *Id.*

[65] *Id.*

[66] *Id.* (citing Georgia v. Randolph, 547 U.S. 103 (2006)). *See generally* Lieutenant Colonel Stephen R. Stewart, *Katy Bar the Door—2006 New Developments in Fourth Amendment Search and Seizure Law*, ARMY LAW., June 2007, at 2–4.

[67] *Wallace*, 66 M.J. at 9 (citing *Randolph*, 547 U.S. at 120).

[68] *Id.*

[69] *Id.* (citing Alderman v. United States, 394 U.S. 165, 174 (1969)).

[70] *Id.*

[71] *Id.* (citing United States v. Murphy, 36 M.J. 732, 734 (A.F.C.M.R. 1992); Schenckloth v. Bustamonte, 412 U.S. 218, 226–27 (1973)).

> (1) the degree to which the suspect's liberty was restricted; (2) the presence of coercion or intimidation; (3) the suspect's awareness of his right to refuse based on inferences of the suspect's age, intelligence, and other factors; (4) the suspect's metal state at the time; (5) the suspect's consultation, or lack thereof, with counsel; and (6) the coercive effects of any prior violations of the suspect's rights.[72]

According to the CAAF, four of the six factors were met.[73] First, SSgt Wallace "clearly faced restrictions on his liberty" with "three individuals escort[ing Wallace] from the AFOSI building to his home—the two AFOSI agents . . . and [Wallace's] first sergeant."[74] The court concluded that if Wallace "faced no restrictions on his liberty," then his first sergeant as an "escort would have been unnecessary."[75] Second, "the facts of the escort and the presence of several authority figures also created a coercive and intimidating atmosphere."[76] Third, despite the fact Wallace was "a twenty-six-year-old staff sergeant with nearly eight years of service, it is doubtful that he knew he could withdraw consent once given."[77] Additionally, Article 31, UCMJ, warnings do not provide a disclaimer indicating that consent, once given, can be withdrawn, and the agents commented that they "'would have to take the computer' as a matter of routine" left SSgt Wallace believing that he could not refuse consent.[78] Finally, SSgt Wallace "never consulted counsel throughout his questioning and the subsequent search."[79] Consequently, SSgt Wallace's "ultimate consent to the seizure of the computer was not a valid consent, but rather mere acquiescence to the color of authority."[80] Despite this conclusion, the CAAF still supported the military judge in denying SSgt Wallace's motion to suppress.

The CAAF relied on the doctrine of inevitable discovery to admit the evidence discovered on SSgt Wallace's computer. This doctrine "creates an exception to the exclusionary rule allowing admission of evidence that, although obtained improperly, would have been obtained by other lawful means."[81] Military Rule of Evidence (MRE) 311(b)(2) articulates this exception as "[e]vidence that was obtained as a result of an unlawful search or seizure may be used when the evidence would have been obtained even if such unlawful search or seizure had not been made."[82] The CAAF, therefore, relied on SSgt Wallace's statements made to the AFOSI agents prior to giving his consent to search as the basis for applying the inevitable discovery exception.

Staff Sergeant Wallace's admission of a "sexual relationship with a young girl with whom he communicated mostly via e-mail and instant messenger" to the AFOSI agents provided the foundation in which the inevitable discovery doctrine rests.[83] This statement "encouraged investigators to focus on the computer as a source of evidence and created sufficient probable cause to allow AFOSI to obtain an authorization to search for, and seize e-mails and messages between [Wallace] and [the minor child]."[84] As a result, "the files containing child pornography would have been inevitably discovered" through a valid search.[85]

---

[72] *Id.* (citing *Murphy*, 36 M.J. at 734).

[73] *Id.* at 10.

[74] *Id.* at 9.

[75] *Id*.

[76] *Id*. The authority figures were the first sergeant and the chaplain. *Id*.

[77] *Id*.

[78] *Id*.

[79] *Id*. at 10.

[80] *Id*.

[81] *Id*. (citing Nix v. Williams, 467 U.S. 431, 444 (1984)); *see supra* note 19.

[82] MCM, *supra* note 5, MIL. R. EVID. 311(b)(2).

[83] *Wallace*, 66 M.J. at 10.

[84] *Id*.

[85] *Id*. Judge Baker concurs in the result, but sees things differently than the majority. *Id*. at 10–11 (Baker, J., concurring). He calls the majority approach "could have-would have." *Id.* at 11 (Baker, J., concurring). He further cites: "As the Fourth Circuit has held, the inevitable discovery doctrine 'cannot rescue evidence obtained via an unlawful search simply because probable cause existed to obtain a warrant when the government presents *no* evidence that the police would have obtained a warrant. Any other rule would emasculate the Fourth Amendment.'" *Id*. at 11 (Baker, J., concurring) (citing United States v. Allen, 159 F.3d 832, 842 (4th Cir. 1998)). Additionally, Judge Baker, "balance[s] the factors differently than the majority and conclude[s] that [Wallace] did not merely acquiesce to authority in consenting to the search of his computer." *Id*. at 12 (Baker, J., concurring).

Wallace illustrates the effect computers, or rather digital media, has in the application of Fourth Amendment jurisprudence in issues of consent. Although a computer may be a 13" x 9" x 1" plastic and metal box, it may exponentially yield as much evidence as a modest size home in toto. Therefore, the impact and implications of consenting to search a computer appear initially benign, but quickly grow more complicated as the reality of the consent settles on the owner. Consequently, motions practice to suppress evidence contained in the computer becomes more aggressive as *Wallace* demonstrates. However, if *Wallace* illustrates complexity within Fourth Amendment law, then the *Larson* case illustrates the CAAF's straightforward approach in applying it.

C. Computers and the Reasonable Expectation of Privacy

United States v. Larson was a much-anticipated decision.[86] The *Larson* case is the second case by the CAAF addressing the reasonable expectation of privacy in a government computer system.[87] The anticipation in this case rested on the premise of whether the CAAF's previous holding in *United States v. Long* would be overturned.[88] The *Long* case caused much consternation due to its holding that Corporal Long enjoyed a reasonable expectation of privacy in her government e-mail stored on a government server and, therefore, evidence derived from the search of her computer without a proper search authorization was excluded.[89] Thus, *Long* turned the common perception that there was no reasonable expectation of privacy in government e-mail upside down. In *Larson*, the CAAF did not deliver a definitive, black-letter, decision on a reasonable expectation of privacy in government computer systems, but instead simply reaffirmed the analysis to determine a reasonable expectation of privacy.

The facts of the case are straightforward. Air Force Major (Maj) Larson used his "government computer in his military office to obtain sexually explicit material, to include pornographic images and video, from the Internet and to initiate instant message conversations with 'Kristin,' someone he believed to be a fourteen-year-old girl."[90] "Kristin," however, was "a civilian police detective working to catch online sexual predators."[91] Major Larson arrived at a pre-arranged meeting place to see Kristin and was arrested in the sting operation.[92] The AFOSI, while working in cooperation with the civilian police, initiated its own investigation upon Maj Larson's arrest.[93]

During the course of the investigation, AFOSI seized and searched Larson's government computer without a search authorization.[94] The search of the computer's hard drive yielded "pornographic material, a web browser history that showed [Larson] visited pornographic websites and engaged in sexually explicit chat sessions in his office on his government computer, and other electronic data implicating [Larson] in the charged offenses."[95] Major Larson moved to suppress this evidence at trial.[96] The military judge ruled against him, stating:

> [T]he Government had established by a preponderance of the evidence that Appellant had no reasonable expectation of privacy in the government computer because the computer had "consent to monitoring" banner that had to be acknowledged with each log on, the system administrator had access to every part of the computer, including the hard drive, and the computer was government property.[97]

---

[86] *See* 66 M.J. 212 (C.A.A.F. 2008); Stewart, *supra* note 6, at 12–15.

[87] 64 M.J. 57 (C.A.A.F. 2006).

[88] *Id*. at 59. The certified issue is: "WHETHER THE AIR FORCE COURT OF CRIMINAL APPEALS ERRED IN HOLDING THAT APPELLANT HAD NO REASONABLE EXPECTATION OF PRIVACY IN HIS GOVERNMENT COMPUTER DESPITE THIS COURT'S RULING IN UNITED STATES V. LONG, 64 M.J. 57 (C.A.A.F. 2006)." *Larson*, 66 M.J. at 213.

[89] *See* Stewart, *supra* note 66, at 7–17.

[90] *Larson*, 66 M.J. at 214.

[91] *Id*.

[92] *Id*.

[93] *Id*.

[94] *Id*. ("[Larson's] commander, using a master key to the government office occupied by [Maj Larson], allowed AFOSI agents to enter and to seize the government computer in the office.").

[95] *Id*.

[96] *Id.*

[97] *Id*. at 215.

The AFCCA affirmed the decision by the trial judge, and Maj Larson appealed the decision to the CAAF on the belief that he enjoyed the same reasonable expectation of privacy in his government computer as Corporal Long did in hers as decided in *United States v. Long*.[98] Major Larson, unfortunately, failed to recognize the narrow scope of the *Long* holding, and that CAAF is not a rubber stamp.

The CAAF got straight to the point. The court focused on the rebuttable presumption that Maj Larson had no expectation of privacy in a government computer provided for official use based on Military Rule of Evidence (MRE) 314(d). It states:

> Government property may be searched under this rule unless the person to whom the property is issued or assigned has a reasonable expectation of privacy therein at the time of the search. Under normal circumstances, a person does not have a reasonable expectation of privacy in government property that is not issued for personal use; but the determination as to whether has a reasonable expectation of privacy in government property issued for personal use depends on the facts and circumstances at the time of the search.[99]

The court analyzed whether Maj Larson was able to prove a reasonable expectation of privacy based on the totality of the circumstances.[100] First, the CAAF looked to whether Maj Larson could prove he actually had a subjective expectation of privacy in the government computer.[101]

At trial, Maj Larson presented no evidence that he had a subjective expectation of privacy in his government computer.[102] Instead, he offered only the holding in *Long* as proof of his expectation of privacy.[103] This was insufficient. Not only did he not testify as to his subjective expectation of privacy, but also the following facts were dispositive.[104] First, the computer Maj Larson used had a log on banner identifying "that it was a DOD computer."[105] Second, the computer "[was] for official use, [and] not to be used for illegal activity."[106] Third, "[i]t also had a statement that users of the computer consent to monitoring."[107] Finally, Maj Larson's commander and the military judge's findings of fact established both monitoring of and command access to the government computer."[108] The sum of these facts led the CAAF to conclude that Maj Larson has no expectation of privacy in the government computer despite their holding in *Long*.[109]

The court distinguished the *Long* holding and found that Maj Larson's reliance on it is misplaced.[110] *Long* was "rooted in the 'particular facts of that case.'"[111] Specifically, the "testimony of the network administrator [as to the agency practice of recognizing the privacy interests of users in their e-mail] is the most compelling evidence in supporting the notion that [Long] had a subjective expectation of privacy."[112] The significance of this case is that "*Long* does not control the decision here."[113]

---

[98] *Id.*

[99] *Id.* (citing MCM, *supra* note 5, MIL. R. EVID. 314(d)).

[100] *Id.* (citing Samson v. California, 547 U.S. 843, 848 (2006)).

[101] *Id.*

[102] *Id.* ("There is no evidence appellant had a subjective expectation of privacy in the government computer, and he did not testify that he did.").

[103] *Id.*

[104] *Id.* at 215–16 (citing United States v. Flores, 64 M.J. 451, 454 (C.A.A.F. 2007)) ("[F]actoring into the reasonable expectation of privacy analysis the fact that the accused did not testify on the motion to suppress.").

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.* (quoting United States v. Long, 64 M.J. 57, 63 (C.A.A.F. 2006)).

[112] *Id.* (citing *Long*, 64 M.J. at 63).

[113] *Id.* at 216.

Larson represents a model approach to Fourth Amendment issues involving government property, vis-à-vis government computers. Simply, and brilliantly, CAAF applied MRE 314(d).[114] This approach may be summarized as a brilliance-in-the-basics methodology as it removes any preconceived bias applying a Fourth Amendment analysis to government property. It solely emphasized the rebuttable presumption that there is no expectation of privacy in government property.[115] Therefore, the burden shift to the moving party simplifies a perceived complex Fourth Amendment analysis regarding government computers. Fortunately, the CAAF took this straightforward approach to in its Fourth Amendment treatment of a mislaid laptop computer in *United States v. Michael*.[116]

D. Computers and the Reasonable Expectation of Privacy in Mislaid Property and the Reasonableness of a Search

The *Michael* case is one of first impression for the CAAF in addressing reasonable expectation of privacy in mislaid property.[117] What makes this case even more compelling is the nature of the mislaid property—a laptop computer.[118] This seems like a straightforward issue when you consider identifying this type of property until you realize that unlike a book, or piece of gear, the owner's name isn't going to be on the inside cover, or conspicuously marked. Instead, it may entail powering the computer up and opening files to determine ownership. Thus, the crux of the *Michael* case is: how far may the government go to identify mislaid property and does the owner have a reasonable expectation of privacy in that mislaid property in terms of evidence discovered during the course of identification.

Photographer's Mate Airman Recruit (AR) Michael mislaid his laptop computer.[119] This was unknown to him or his shipmates.[120] At the Defense Information School, in which AR Michael was attending, "a student found a laptop computer while cleaning the male lavatory of the Navy student barracks."[121] "The laptop was closed, in the off mode, and had no outward markings identifying the owner."[122] The student turned the computer into the military training instructors (MTIs) on staff duty that morning.[123] Since there were no identifying outward marks on the laptop, one of the MTIs started the computer in an attempt to identify the owner.[124] The log-on identified a single name: "Josh."[125] The computer was not password protected so the MTI went to the desktop, opened "control panel" and then "system properties" where the singe name—"Josh"—was listed as the registered owner.[126] Methodical in his examination, the MTI then went to the student roster where he identified three sailors with the name "Josh."[127] The MTI returned to the desktop computer and "navigated to 'Recent Documents' tab" in the hopes of finding recent school work with the owner's full name.[128] Instead, the tab displayed "files with names suggesting they might contain child pornography."[129] The MTI turned the computer to the legal office which identified AR Michael as the owner.[130]

---

[114] *Id*.

[115] *Id*.

[116] 66 M.J. 78 (C.A.A.F. 2008).

[117] *Id*. at 81.

[118] *Id*. at 79.

[119] *Id.*

[120] *Id.*

[121] *Id*.

[122] *Id*.

[123] *Id*.

[124] *Id.*

[125] *Id*.

[126] *Id*.

[127] *Id*.

[128] *Id*.

[129] *Id.*

[130] *Id.*

Airman Recruit Michael moved to suppress the evidence.[131] According to AR Michael, the MTI's actions taken in identifying the laptop could have been done by less intrusive means and were entirely "avoidable, unnecessary, and accordingly, unreasonable."[132] The Navy-Marine Corps Court of Criminal Appeals (NMCCA) reversed.[133] Like the *Larson* case, the CAAF took a straightforward approach in its analysis.

The CAAF addressed this search by relying on the touchstone of Fourth Amendment analysis: reasonableness.[134] The court importantly noted that the "Fourth Amendment does not protect against all searches," just unreasonable ones.[135] It also distinguished what a search is under military law: "a government intrusion into an individual's reasonable expectation of privacy."[136] Using this definition as a stepping-stone, the CAAF analyzed the expectation of privacy that AR Michael may have in mislaid property.[137] Although mislaid property "is that which is intentionally put into a certain place and later forgotten,"[138] an owner "retains some expectations of privacy" in it.[139] This expectation, however, is "outweighed by the interest of law enforcement officials in identifying and returning such property to the owner."[140] This balance between privacy interest and governmental interest, to be decided by "reasonableness" of the search, is a case of first impression for the CAAF.[141]

The reasonableness of the search is decided not on "whether less intrusive means were available,"[142] but rather, whether AR Michael had an objectively reasonable subjective expectation of privacy in the mislaid laptop.[143] The CAAF turns not, per se, to the item searched, but rather the location of that item when found and "nature and scope of the government intrusion."[144] Buoyed by its recent precedent in *United States v. Conklin*, the CAAF saw the restroom differently than a barracks or dormitory room.[145] The public restroom, "does not provide the same sanctuary as the threshold of a private room."[146] Airman Recruit Michael's expectation of privacy is therefore diminished in his laptop due to where it was discovered.[147] Next, the court addressed whether the MTI had a good reason for powering up Michael's computer to identify ownership.

The CAAF found that "the legitimate governmental interest in identifying the owner of mislaid property and safekeeping it until its return to the owner outweighed the interest [Michael] retained in his mislaid and subsequently found laptop."[148] There are two parts to this determination.[149] First, a repudiation of the trial judge's "could have-would have" approach to reasonableness. The subtlety lies in whether the Fourth Amendment requires such steps, and which CAAF determines there

---

[131] *Id.*

[132] *Id.*

[133] *Id.* at 79–80.

[134] *Id.* at 79. "The ultimate standard set forth in the Fourth Amendment is reasonableness." *Id.* (citing Cady v. Dombrowski, 413 U.S. 433 (1973)).

[135] *Id.*

[136] *Id.* (citing United States v. Daniels, 60 M.J. 69, 71 (C.A.A.F. 2004)).

[137] *Id.* ("Here, the military judge's findings indicate that under the circumstances of its recovery, the computer could appropriately have been characterized as mislaid property.").

[138] *Id.* (citing AM.JUR.2D *Abandoned, Lost, and Unclaimed Property* § 14 (2007)).

[139] *Id.*

[140] *Id.* at 80.

[141] *Id.*

[142] *Id.* at 81.

[143] *Id.*

[144] *Id.*

[145] *Id.* (citing United States v. Conklin, 63 M.J. 333, 337 (C.A.A.F. 2006)); *see* Stewart, *supra* note 66, at 14–17 (providing a detailed discussion of the *Conklin* decision).

[146] *Michael*, 66 M.J. at 81.

[147] *Id.* ("In this case, on these facts, Appellant possessed a diminished expectation of privacy in his personal computer that was mislaid in a common area.").

[148] *Id.*

[149] *Id.* The court relies on the Supreme Court holding in *Illinois v. Lafayette*, in which the issue of reasonableness: "The reasonableness of any particular governmental activity does not necessarily or invariably turn on the existence of alternative 'less intrusive' means." *Id.* (citing Illinois v. Lafayette, 462 U.S. 640, 647 (1983)). "Rather, it depends on whether [Michael] had a subjective (actual) expectation of privacy in the property searched that was objectively reasonable." *Id.* (citing *Conklin*, 63 M.J. at 337).

is no "less intrusive means" requirement.[150] Second, a focus on the government intrusion, and a determination that "[i]n the military context, it was reasonable for the MTI to seek to determine the ownership of the computer and do so by powering it up and performing a cursory examination of folders likely to reveal the owner's identity."[151]

The *Michael* case is straightforward, but yet complex in the "soul-searching" that occurs by CAAF in determining reasonableness. The context of a mislaid computer search illustrates how computer crime challenges the court to determine subjective expectation of privacy, as well as the objective reasonableness of government actions within the scope of that search. What would the Constitutional Framers think of such a context for the Fourth Amendment? What, however, remains true throughout the *Michael*'s case is one principle the Constitutional Framers may have been proud of: "brilliance in the basics."

E. Computers and the Scope of Search vis-à-vis the Execution of a Valid Search Warrant

If "brilliance in the basics" is a tool for success within Fourth Amendment analysis, then the AFCCA should take pride in their analysis for *United States v. Osorio*.[152] The AFCCA addressed the issue of the scope of a computer search warrant.[153] Again, the scope of what may be searched seems straightforward in a search warrant, but yet acquires Fourth Amendment complexity and subtlety when a search warrant includes a computer. The analysis is without pretense and provides a concise Fourth Amendment methodology, as well as, valuable proscriptions for the military practioner.[154]

Senior Airman (SrA) Osorio did more than attend a party where strip poker ensued.[155] He also took photos.[156] This became an important fact when the AFOSI began investigating an alleged sexual assault that occurred at the party.[157] When questioned by AFOSI, SrA Osorio "told the agents he had saved the pictures on his laptop."[158] They then went to his off-base apartment to view the photos.[159] Senior Airman Osorio offered to give copies of the photos to the AFOSI agents, but would not consent to turning over his computer to them.[160] After viewing the photos, the agents sought and received an oral search authorization to search SrA Osorio's off-base apartment.[161]

The agents then seized the laptop and a digital memory card since they contained possible evidence.[162] A short time later, SrA Osorio dropped off a power cord for his laptop to the agents, and an external hard drive which he explained he used with his laptop.[163] After acknowledging that he was not a suspect in the investigation, SrA Osorio signed a consent form permitting the search of his external hard drive.[164]

---

[150] "Whether [MTI's] search was reasonable or unreasonable in this case does not hinge on whether less intrusive means were available." *Id*. at 80–81.

[151] *Id*. The MTI "testified that his duties s an MTI included receiving and securing valuable personal effects of the students depending on what 'phase' of training the students had entered." *Id*. at 81.

[152] 66 M.J. 632 (A.F. Ct. Crim. App. 2008).

[153] *Osorio* raised four issues on appeal, three of them relate to the search of his laptop computer:

> (1) whether the military judge erred in failing to suppress evidence of images found on the appellant's laptop computer hard drive; (2) whether the military judge erred in failing to suppress the evidence of images found on the appellant's external hard drive; (e) whether the military judge erred in failing to suppress the appellant's oral and written confessions and the additional evidence obtained during a search of the appellant's apartment as fruit of the poisonous tree.

Id. at 633.

[154] *Id*. at 634.

[155] *Id*.

[156] *Id*. The photos included "partially nude people who attended the party." *Id*.

[157] *Id*. Osorio "was not the suspect of the alleged assault." *Id*.

[158] *Id*.

[159] *Id.*

[160] *Id*.

[161] *Id*. The agents explained that they would provide him with written authorization later." *Id*.

[162] *Id*.

[163] *Id*.

[164] *Id*.

The following week the AFOSI agents realized they had executed an off-base search improperly, and sought a valid search authorization from a U.S. magistrate.[165] The magistrate narrowly authorized the search for "one Toshiba laptop computer and one digital memory card used to record photographs taken on February 12, 2005."[166] No mention of the external hard drive was made in the warrant.[167] Nor was there any communication to the forensic investigator on the limited parameters of the authorized search.[168]

The AFOSI forensic investigator, Special Agent (SA) JL was a victim of her own forensic methodology, ignorance, and initiative. The forensic methodology for examining computer hard drives required SA JL to make a mirror image of the hard drives and use forensic software to view all photos at once as thumbnails.[169] Once SA JL made the mirror image of the hard drives she had fulfilled her technical requirement.[170] However, having completed her task, and unaware of the limitations placed upon the actual investigative agents in their search of the hard drives, she opened up thumbnails that she had noticed might contain nude persons to see if they were "contraband."[171] After some examination, she concluded that the nude persons were indeed nude minors.[172] She brought this to the attention of the AFOSI agents who then questioned SrA Osorio.[173]

Senior Airman Osorio confessed to downloading and possessing child pornography.[174] Additionally, he consented to a search of his apartment where several compact disks were seized.[175] The AFOSI agents also exacted an additional, separate search authorization for his laptop and memory card.[176] Full forensic examination of the laptop, memory card, external hard drive, and compact disks revealed images believed to be child pornography.[177]

In examining SrA Osorio's appeal of error by the military judge in failing to suppress this evidence, the AFCCA examined the lawfulness of the search in terms of the validity and execution of the search warrant. Precedent dictates that "[s]earch warrants must be specific and specificity has two aspects, particularity and breadth."[178] The federal warrant, "despite the initial problem of going to the wrong search authority," was valid and sufficiently specific, to the items to be search (computer and digital memory card), the items sought (photographs), and when (taken on February 12, 2005).[179] The execution of this valid warrant, however, is problematic.

The AFCCA found that the AFOSI forensic investigator, SA JL, exceeded the scope of the search warrant.[180] The court relied on the persuasive holding in *United States v. Carey*, in which an investigator was found to have exceeded the scope of the warrant when he continued to examine a computer for child pornography when his original search was for records of drug distribution.[181] Likewise, in *Osorio* SA JL was only authorized to make a copy of the digital media, and exceeded her authority and scope of search when she clicked on the nude persons identified by her in the thumbnail images.[182]

---

[165] *Id*. ("The first warrant was obtained from the installation's military magistrate, despite the fact the appellant's apartment was not on the base.").

[166] *Id*.

[167] *Id*.

[168] *Id*.

[169] *Id*. at 635.

[170] *Id*.

[171] *Id*.

[172] *Id*.

[173] *Id*.

[174] *Id*.

[175] *Id*.

[176] *Id*. The Defense Computer Forensic Laboratory, "recognizing that the same computer was being used for two different cases, contacted OSI and requested a separate search authorization to search the media for child pornography prior to their analysis of the laptop and memory card." *Id*.

[177] *Id*.

[178] *Id*. (citing United States v. Hill, 459 F.3d 966, 973 (9th Cir. 2006)).

[179] *Id*. at 635–36.

[180] *Id.*

[181] *Id*. at 636 (citing United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)).

[182] *Id.*

Furthermore, the court looked to SA JL's intent in determining the issue of scope.[183] Her intent in "clicking on the nude photographs was . . . to determine 'contraband' and child pornography."[184] Hence, she was conducting a general search much like the investigator in *Carey*, and "searching beyond the date exceeded the warrant's scope."[185] The AFCCA used this determination as a case study for the military justice practitioner.

Again, the AFCCA relied on the Federal Tenth Circuit for guidance. In *United States v. Walser*, a similar situation as in *Osorio* occurred, but with a better outcome.[186] Here, an investigator came across a file that happened to be child pornography.[187] But, unlike in *Osorio*, "as soon as he found the first suspect file, beyond the scope of his search authority, he suspended his search and went to the magistrate for a *new warrant for child pornography*."[188] Hence a lesson and an admonition the *Osorio* court segues nicely for the military law practioner.

The lesson the Tenth Circuit provides is insightful. "[C]omputers make tempting targets in searches for incriminating information, and electronic storage is likely to contain a greater quantity and variety of information than any previous storage methods."[189] So,

> [w]here officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant what types of files are sought.[190]

Just as practicable, the *Osorio* AFCCA court has turned this lesson into a useful admonition:

> This court finds that when dealing with search warrants for computers, there must be specificity in the scope of the warrant which, in turn, mandates specificity in the process of conducting the search. Practitioners must generate specific warrants and search processes necessary to comply with that specificity and then, if they come across evidence of a different crime, stop their search and seek a new authorization.[191]

In finding the search invalid, the AFCCA explored and discounted six exceptions to the Fourth Amendment probable cause[192] and exclusionary rule[193] requirements: plain view doctrine,[194] good faith exception,[195] consent,[196] inevitable

---

[183] *Id.*

[184] *Id.*

[185] *Id.*

> SA JL testified that at the time of her search she did not know the terms of the warrant. We recognized this oversight was probably due to the fact that her job was not to investigate the computer data, instead it was to make a mirror image of the hard drive; however, as an OSI agent, when she began to search for contraband, she should have become familiar with the terms of the warrant.

Id.

[186] 275 F.3d 981 (10th Cir. 2001).

[187] *Osorio*, 66 M.J. at 636 (citing *Walser*, 275 F.3d at 987).

[188] *Id.* (citing *Walser*, 275 at 987).

[189] *Id.* at 637 (citing United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999)).

[190] *Id.* (citing *Carey*, 172 F.3d at 1275).

[191] *Id.*

[192] "Probable cause is a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched." MCM, *supra* note 5, MIL. R. EVID. 315(f).

[193] *See* Weeks v. United States, 232 U.S. 383 (1914) (holding that evidence obtained directly or indirectly through illegal government conduct is inadmissible); Mapp v. Ohio, 376 U.S. 643 (1961) (finding that exclusionary rule is a procedural rule that has no bearing on guilt, only in respect for dignity or fairness).

[194] *Osorio*, 66 M.J. at 637. Under the plain view doctrine, property may be seized when: the property is in plain view, the person observing the property is lawfully present, and the person observing the property has probable cause to seize it. *See* MCM, *supra* note 5, MIL. R. EVID. 316(d)(4)(c); United States v. Fogg, 52 M.J. 144 (C.A.A.F. 1999); Arizona v. Hicks, 480 U.S. 321 (1987).

[195] *Osorio*, 66 M.J. at 637. The good faith exception means that evidence is admissible when obtained by police relying in good faith on a facially valid warrant that later is found to lack probable cause or is otherwise defective. *See* MCM, *supra* note 5, MIL. R. EVID. 311(b)(3); United States v. Leon, 468 U.S. 897 (1984).

discovery,[197] the independent source doctrine,[198] and attenuation of a taint.[199] First, the court addressed the government's argument that the "discovery of the images on the laptop could be saved because the images were in plain view when discovered."[200] The "act of SA JL opening the thumbnails to see if they were images of child pornography"[201] "exceeded the authorized scope of the authorized search."[202] Citing the Supreme Court, "the plain view doctrine may 'not be used to extend a general exploratory search from one object to another until something incriminating emerges"[203]

Next, the AFCCA dismissed the Government's notion that the "good faith exception applies to justify admission of the child pornography on the laptop."[204] As *United States v. Leon* states, "[t]he good faith exception applies only when police rely on the terms of the warrant."[205] Here, SA JL did not rely on the terms of the warrant, and therefore the good faith exception does not apply.[206]

Likewise, where the Government exceeded the scope of the search warrant of SA Osorio's computer and memory card, the Government also exceeded SrA Osorio's consent to search his external hard drive.[207] Senior Airman Osorio's consent to search his external hard drive was limited to the party pictures from 12 February 2005.[208] The court considered what the reasonable person would have understood as the exchange between SrA Osorio and the AFOSI agents.[209] Based on the exchange between the parties, the AFCCA believed the record supports a finding that consent was limited to "searching for the party pictures from 12 February 2005 and not to a general search of the external hard drive."[210]

Regardless, the Government believed that the Defense Computer Forensic Laboratory (DCFL) would have inevitably discovered the child pornography on either the laptop or the external hard drive.[211] The AFCCA remained unconvinced. The "DCFL could and would have limited themselves to the warrant or consent parameters."[212] Additionally "all the child pornography images on the laptop were contained in hidden folders or were contained in hidden folders or were in deleted files that were only recovered through the use of forensic software."[213] For these reasons, the AFCCA did not find that the "inevitable discovery doctrine would have validated the ultimate seizure of the child pornography images from the laptop or the external hard drive."[214]

---

[196] *Osorio*, 66 M.J. at 638. A consent search applies when a person voluntarily consents to a search of his person or property under his control, no probable cause or warrant is required. *See* MCM, *supra* note 5, MIL. R. EVID. 314(e). Consent may be limited to certain places, property and times. *Id.* MIL. R. EVID. 314(e)(3); United States v. Rittenhouse, 62 M.J. 504 (A. Ct. Crim. App. 2005).

[197] *Osorio*, 66 M.J. at 639. As a general rule, the inevitable discovery doctrine applies when illegally obtained evidence is admissible if it inevitably would have been discovered through independent, lawful means. *See* MCM, *supra* note 5, MIL. R. EVID. 311(b)(2); Nix v. Williams, 467 U.S. 431 (1984).

[198] *Osorio*, 66 M.J. at 639. The independent source doctrine applies when evidence discovered through a source independent of illegality is admissible. *See* MCM, *supra* note 5, MIL. R. EVID. 311(e)(2); Murray v. United States, 487 U.S. 533 (1988); *Fogg*, 52 M.J. at 144, 151; United States v. Camanga, 38 M.J. 249 (C.M.A. 1993).

[199] *Osorio*, 66 M.J. at 639–40. The attenuation of a taint exception concerns evidence that would not have been found but for official misconduct and is admissible if the causal connection between the illegal act and the finding of the evidence is so attenuated as to purge that evidence of the primary taint. *See* MCM, *supra* note 5, MIL. R. EVID. 311(e)(2); Wong Sun v. United States, 371 U.S. 471, 484–87 (1963) (holding that the unlawful arrest did not taint subsequent confession where it was made after appellant's arraignment, released on his own recognizance, and voluntary return to the police station several days later).

[200] *Osorio*, 66 M.J. at 637.

[201] *Id*.

[202] *Id*.; *see* United States v. Conklin, 63 M.J. 333 (C.A.A.F. 2006).

[203] *Osorio*, 66 M.J. at 637 (citing Arizona v. Hicks, 480 U.S. 321, 328 (1987)).

[204] *Id*.

[205] *Id*. (citing United States v. Leon, 468 U.S. 897, 922–23 (1984)).

[206] *Id*.

[207] *Id*. at 639.

[208] *Id*. at 638.

[209] *Id*. The AFCCA considered eight significant specifics of that exchange. *Id*.

[210] *Id*. at 639.

[211] *Id*.

[212] *Id*.

[213] *Id*.

[214] *Id*.

Moreover, the court discounted the independent source doctrine as a remedy for the illegal search. "The only source of information regarding the possession of child pornography appeared as a result of the unlawful search conducted by SA JL . . . ."[215] Therefore, the AFCCA determined that the search authorization for child pornography, "required by DCFL and authorized by the military magistrate, has no independent source."[216]

Lastly, the AFCCA shut the door on the Government's final attempt to introduce the fruits of the illegal search under the attenuation of a taint exception.[217] The court applied the *Brown* test to determine whether SrA Osorio's consent was an "independent act of free will, breaking the causal chain between the consent and the constitutional violation."[218] In applying the three prong test the court determined the factors all favor SrA Osorio.[219] So, the confession and the consent were not sufficiently attenuated from the taint of the illegal search of the laptop.[220] Therefore, "all derivative evidence, to include [Osorio's] admission, the full search of the external hard drive, and the CDs are fruit of the poisonous tree and therefore not admissible."[221]

Osorio is a standout case. Although only a service court case, it highlights an important aspect of procedural computer crime law—search authorizations and warrants. Additionally, the case stands out for its application and discussion of probable cause and exclusionary rule exception within the context of a computer search. But, the most important aspect of *Osorio* is Judge Heimann's prescription to military law practitioner's to "generate specific warrants and search processes" for computer searches.[222]

II. Next Term of Court Search and Seizure Cases

A. The Supreme Court Examines the Exclusionary Rule

If the military service courts fully embraced Fourth Amendment methodology, then the U.S. Supreme Court started to push back. The next, or rather, the current term of court for the Supreme Court, has several important Fourth Amendment cases under consideration or already published: *Herring v. United States*,[223] *Arizona v. Gant*,[224] *Arizona v. Johnson*,[225] and

---

[215] *Id*.

[216] *Id*.

[217] *Id*. at 639–40.

[218] *Id.* at 640 (citing Brown v. Illinois, 422 U.S. 590 (1975); U.S. v. Conklin 63 M.J. 333, 338–39 (C.A.A.F. 2006)).

> To determine whether the defendant's consent was an independent act of free will, breaking the causal chain between the consent and the constitutional violation, we must consider three factors: (1) the temporal proximity of the illegal conduct and the consent; (2) the presence of intervening circumstances; and (3) the purpose and flagrancy of the initial misconduct.

Id.

[219] *Id*.

> First, the illegal search of the computer was relatively close in time to the OSI actions which led to the additional evidence. . . . Second, there were no intervening circumstances sufficient to remove the taint from the initial search. . . .
>
> In regard to the third factor, while we find no improper motive on behalf of the government agents in this case, we do find that their actions were unnecessary and unwise.

Id.

[220] *Id*.

[221] *Id*. at 639.

[222] *Id*. at 637.

[223] *See* DEPARTMENT OF HOMELAND SECURITY, THE FEDERAL LAW ENFORCEMENT TRAINING CENTER, LEGAL TRAINING DIVISION, THE FEDERAL LAW ENFORCEMENT INFORMER (Nov. 2008) [hereinafter INFORMER], *available at* Dep't of Homeland Security, Federal Law Enforcement Training Ctr., www.fletc.gov/legal; Herring v. United States, 129 S. Ct. 695 (2009). Does the Fourth Amendment require suppression of evidence found during a search incident to an arrest when the arresting officer conducted the arrest and search in sole reliance upon facially credible but erroneous information negligently provided by another law enforcement agent? INFORMER, *supra.*

[224] INFORMER, *supra* note 223; Arizona v. Gant, No. 07-542 (U.S. filed Oct. 24, 2007). Does the Fourth Amendment require law enforcement officers to demonstrate a threat to their safety or a need to preserve evidence related to the crime of arrest in order to justify a warrantless vehicular search incident to arrest conducted after the vehicle's recent occupants have been arrested and secured? INFORMER, *supra* note 223.

Pearson v. Callahan.[226] Although these cases will be left for the next symposium article, one particular case deserves brief attention in this current article.

The Supreme Court's holding in *Herring v. United States* represents a continuing shift in the application of the exclusionary rule.[227] Three years ago in *Hudson v. Michigan*, the Court ruled, "a violation of the Fourth Amendment knock-and-announce rule, without more, will not result in suppression of evidence at trial." Similarly, three years later in *Herring*, the Court held that "when police mistakes are the result of negligence [based on erroneous and carelessly maintained information], rather than systemic error or reckless disregard of constitutional requirements," the exclusionary rule does not apply.[228] The holding in *Herring* can be read broadly or narrowly.[229] A broad reading of this decision by lower courts could mean "the death of the exclusionary rule as a practical matter."[230] The most debated shift though, is from requiring suppression of physical evidence due to police misconduct[231] to "other ways to deter police wrongdoing directly, including professional discipline, civil lawsuits and criminal prosecution."[232] This approach, is a major shift of Fourth Amendment jurisprudence in place since 1961 when the exclusionary rule was applied to the states through the Fourteenth Amendment in *Mapp v. Ohio*.[233]

III. Conclusion

This year's term of court was an affirmative year for the military courts of appeals. Where past years' terms of court have been pregnant with anticipation, the courts, especially the CAAF, handled this year's cases with confidence. If past years' symposium articles have concluded with an admonition seeking Fourth Amendment clarity, this year's conclusion can be summarized as wanting more of these confident and affirmative decisions from the military appellate courts. Therefore: "Damn the torpedoes! Full speed ahead!"[234]

---

[225] INFORMER, *supra* note 223; Arizona v. Johnson, 129 S. Ct.781 (2009). In the context of a vehicular stop for a minor traffic infraction, may an officer conduct a pat-down search of a passenger when the officer has an articulable basis to believe the passenger might be armed and presently dangerous, but has no reasonable grounds to believe that the passenger is committing, or has committed, a criminal offense? INFORMER, *supra* note 223.

[226] INFORMER, *supra* note 223; Pearson v. Callahan, 129 S. Ct. 808 (2009). Can a police officer enter a home without a warrant immediately after an undercover informant buys drugs inside, or does the warrantless entry in such circumstances violate the Fourth Amendment? INFORMER, *supra* note 223.

[227] Hudson v. Michigan, 126 S. Ct. 2159 (2006); *see* Stewart, *supra* note 66, at 7 (citation omitted); *Herring*, 129 S. Ct. at 695; *see also Hudson*, 126 S. Ct. at 2165.

[228] *Herring*, 129 S. Ct. at 704.

[229] Liptak, *supra* note 17.

[230] *Id.*

[231] *See* Weeks v. United States, 232 U.S. 383 (1914).

[232] Liptak, *supra* note 17.

[233] *See* 367 U.S. 643 (1961).

[234] *Supra* note 1.