New Developments in Search & Seizure Law

Lieutenant Colonel M. K. Jamison, U.S. Marine Corps
Associate Professor, Criminal Law Department
The Judge Advocate General's Legal Center and School, U.S. Army
Charlottesville, Virginia

"You've got to be very careful if you don't know where you are going because you might not get there."[1]

Introduction

The October 2004 Term of the U.S. Supreme Court and the 2005 Term of the Court of Appeals of the Armed Forces (CAAF) a period marked largely of consolidation and reiteration of the Fourth Amendment's fundamental benchmark measure of probable cause as an objective metric.[2] On the horizon, however, are several cases pending before the Supreme Court and the CAAF that may significantly change the legal landscape of search and seizure law. The potentially most significant case could be handed down by the CAAF, because the Navy Judge Advocate General has requested that the CAAF rule on a servicemember's reasonable expectation of privacy in government electronic mail (e-mail).[3]

This article addresses one of the four search and seizure cases the Supreme Court handed down during its October 2004 Term and provides a preview for two upcoming search and seizure cases for the Supreme Court's October 2005 Term.[4] The article also analyzes several significant cases from the CAAF and the service courts of criminal appeals. The primary focus of the military cases analyzed in this article deal with search and seizure concepts surrounding computers and other electronic media. In the 1967 case of *Katz v. United States*,[5] the Supreme Court fundamentally changed Fourth Amendment jurisprudence by establishing a threshold expectation of privacy requirement prior to receipt of any protection under the Amendment. In this regard, Part I of this article begins with an examination of three cases from the Navy-Marine Corps Court of Criminal Appeals (NMCCA) that analyze this threshold expectation of privacy requirement within the context of

---

[1] Yogi Berra, Yogi Berra Quotes: "Yogi-isms," http://www.umpirebob.com/DATA/yogiisms.htm (last visited Mar. 29, 2006).

[2] The U.S. Supreme Court's October 2004 Term began on 4 October 2004 and ended 3 October 2005. *See* Supreme Court of the United States, 2004 Term Opinions of the Court, http://www.supremecourtus.gov/opinions/ 04slipopinion.html (last visited Mar. 29, 2006). The CAAF 2005 term began on 1 October 2004 and ended 30 September 2005. *See* U.S. Court of Appeals for the Armed Forces, Opinions & Digest, http://www.armfor. uscourts.gov/Opinions.htm. (last visited Mar. 29, 2006).

[3] The issue of whether a servicemember has a reasonable expectation of privacy in computers generally, and e-mail specifically, has remained largely an open question. *See, e.g.*, Lieutenant Colonel Michael R. Stahlman, *New Developments in Search and Seizure: A Little Bit of Everything*, ARMY LAW., May 2001, at 24 (questioning whether servicemembers have a reasonable expectation of privacy when using a government computer for private and personal purposes); Lieutenant Commander Rebecca A. Conrad, *Searching for Privacy in All the Wrong Places: Using Government Computers to Surf Online*, 48 NAV. L. REV. 1 (2001) (concluding that servicemembers have, at best, a limited expectation of privacy in their private use of a government computer). *But see* U.S. DEP'T OF THE ARMY, REG. 25-2, INFORMATION ASSURANCE ch. 4, sec. 4-5, para. r(2) (14 Nov. 2003) (creating a regulatory expectation of privacy with respect to law enforcement activities whenever a Soldier uses Army information systems).

[4] Two of the search and seizure cases out of the Supreme Court's October 2004 Term were already masterfully explained and analyzed in the 2005 Military Justice Symposium. Lieutenant Colonel E. A. Harper, *Defending the Citadel of Reasonableness: Search and Seizure in 2004*, ARMY LAW., Apr. 2005, at 47-64. For an in-depth analysis of *Devenpeck v. Alford*, 543 U.S. 146 (2005) and *Illinois v. Caballes*, 543 U.S. 405 (2005), please consult Lieutenant Colonel Harper's article. The *Devenpeck* case established a firm and unanimous rebuke of the Ninth Circuit Court of Appeals's attempt to create a subjective metric for measuring probable cause. Sergeant Devenpeck arrested Mr. Alford for a violation of the Washington State Privacy Act; however, under the facts in *Devenpeck*, a Washington State Court-of-Appeals decision had previously held that Mr. Alford's conduct (surreptitious tape recording of Sergeant Devenpeck without his knowledge and consent) was not a crime under Washington State law. *See Devenpeck*, 543 U.S. at 151. Based on this fact, the Ninth Circuit held that Sergeant Devenpeck's arrest violated Mr. Alford's civil rights because it was a warrantless arrest premised on an act that was not a crime. The Ninth Circuit refused to consider Sergeant Devenpeck's alternative argument that probable cause existed to arrest Mr. Alford for other offenses because these unarticulated offenses (at the time of the arrest) were not "closely related" to the articulated arresting offense. *Id.* at 152. In a unanimous opinion, the Supreme Court reversed, holding that probable cause is an objective metric based on all facts available at the time of the arrest. In this regard, the subjective intent or subjective articulation of offenses on the part of an arresting officer is immaterial so long as the facts support probable cause to arrest. *Id.* at 153. Accordingly, the Supreme Court remanded the *Devenpeck* case to the Ninth Circuit for a determination whether the objective facts supported probable cause to arrest. In *Caballes*, the U.S. Supreme Court held in a six to two opinion (Rehnquist, CJ., took no part in the decision) that a dog sniff by a well-trained narcotics-detection dog "discloses only the presence or absence of narcotics, a contraband item." *Id.* at 409 (quoting United States v. Place, 462 U.S. 696, 707 (1983)). Thus, a dog sniff is not a search because no person has a legitimate expectation of privacy in contraband. Critical to the Court's determination was that the duration of the traffic stop was reasonable as the dog sniff occurred while the officer who stopped Mr. Caballes was still writing the speeding ticket. *Id.* at 408-09. In dicta, the Supreme Court suggested that the dog sniff could have been unreasonable if Mr. Caballes had been held as a result of the lawful traffic stop for an unreasonably long period (e.g., to accomplish the dog sniff), so as to constitute an unconstitutional seizure). The remaining Fourth Amendment case, *Brousseau v. Haugen*, 543 U.S. 194 (2004), had relatively little applicability to the military justice process in that it dealt with the legal parameters of qualified immunity.

[5] 389 U.S. 347 (1967).

computers and other digital information. Part I further discusses the consent exception to the Fourth Amendment when dealing with computers and digital information. Part II turns to an evaluation of the quantum of evidence needed to establish probable cause and how far law enforcement officials may go in detaining personnel when executing a search. Finally, Part III concludes with a look ahead to two significant cases pending before the Supreme Court that could have a lasting effect on search and seizure.

Part I: Computers and Digital Media

In 2005, the majority of military appellate cases dealing with the Fourth Amendment sought to formulate a reasonable expectation of privacy construct for e-mail and other types of digital information. It has been largely settled that a servicemember does not have a reasonable expectation of privacy in government-issued computer hardware;[6] however, there is little military jurisprudence that addresses a servicemember's privacy expectation in digital information stored on, or accessed through, a computer. This year, the NMCCA led the way in two published cases: one dealt with whether an accused had a reasonable expectation of privacy in non-content subscriber information typically given to an Internet service provider (e.g., name, address, and credit card number);[7] the other case explored whether an accused has a reasonable expectation of privacy in the content of government e-mail.[8]

A. Expectation of Privacy in Non-Content Subscriber Information

The NMCCA broke new ground in military jurisprudence when it considered Fourth Amendment applicability to non-content digital information. In *United States v. Ohnesorge*,[9] the NMCCA held that a servicemember has no reasonable expectation of privacy in subscriber information that has been provided to a commercial Internet site.[10]

Sergeant (Sgt) Jeffrey S. Ohnesorge, U.S. Marine Corps, was convicted of violating a general order by using his government-issued computer to download pornography, in violation of Article 92, Uniform Code of Military Justice (UCMJ).[11] A drilling reservist had been using Sgt Ohnesorge's government-issued computer to conduct official business during his drill period when he inadvertently discovered both adult and child pornography on the computer hard drive.[12] At the time the pornography was discovered, Sgt Ohnesorge was the unit's Information System Coordinator, responsible for the unit's software and hardware computer support.[13] The images had been stored on the "G drive," a password-protected shared drive that was accessible by other computers on the network.[14] Marine Corps officials conducted a forensic examination of the computer in question and determined that the images had been downloaded from an Internet site named EasyNews.com, which El Dorado Sales, Inc. (El Dorado) owned and operated.[15] The investigation also revealed that all the pornographic images had been downloaded from EasyNews.com through the user name "RuhRowRagy@AOL.com."[16]

---

[6] *See, e.g.*, United States v. Tanksley, 50 M.J. 609, 620 (N-M. Ct. Crim. App. 1999) (holding that there is no reasonable expectation in a government-issued computer laptop "even if capable of being secured" by the servicemember), *aff'd*, 54 M.J. 169 (2000); United States v. Plush, No. 35134, 2004 CCA LEXIS 230 (A.F. Ct. Crim. App. September 21, 2005) (unpublished) (holding that Captain Plush had no reasonable expectation of privacy in his government-issued laptop when he turned the laptop into the computer maintenance section for repair). Although, the CAAF affirmed the *Tanksley* case, its dicta seems to suggest that perhaps servicemembers may have a reasonable expectation of privacy in a government computer. The CAAF stated that Navy Captain Tanksley "had, at best, a reduced expectation of privacy" in his computer. *Tanksley*, 54 M.J. at 172. Unfortunately, the CAAF did not explain what it meant by a *reduced* expectation of privacy.

[7] United States v. Ohnesorge, 60 M.J. 946 (N-M. Ct. Crim. App. 2005).

[8] United States v. Long, 61 M.J. 539 (N-M. Ct. Crim. App. 2005).

[9] *Ohnesorge*, 60 M.J. 946.

[10] *Id.* at 948.

[11] *Id.* at 946.

[12] *Id.* at 947. It was common practice within the unit work spaces to have drilling reservist use computers that had been issued to permanent personnel.

[13] *Id.*

[14] *Id.*

[15] *Id.* The pornographic images had been downloaded from the following newsgroups: sex.preteen and sex.teens. A newsgroup is a continuous public discussion forum about a particular topic. Newsgroups, unlike forum or discussion boards, are decentralized. This means that messages and images are replicated to servers worldwide. *See* PRESTON GRALLA, HOW THE INTERNET WORKS 107 (7th ed. 2004).

[16] *Ohnesorge*, 60 M.J. at 947.

Unrelated to Sgt Ohnesorge's case, the U.S. Customs Service had been conducting an investigation into possible distribution of child pornography through EasyNews.com.[17] The staff judge advocate (SJA) for Sgt Ohnesorge's general court-martial convening authority contacted U.S. Customs Service Special Agent (SA) Judith Coulter to inform her of the Naval Criminal Investigative Service (NCIS) investigation into the child pornography images downloaded through EasyNews.com by someone identified as "RuhRowRagy@AOL.com."[18] As part of her larger investigation, SA Coulter visited Mr. Jeff Minor, President of El Dorado, and requested, among other things, any subscriber information for the user name "RuhRowRagy@AOL.com."[19] Special Agent Coulter assured Mr. Minor that she would provide him with the applicable administrative subpoena for the requested subscriber information.[20] Mr. Minor requested she call her office to verify that an administrative subpoena or summons would be forthcoming, and after she complied with the request, Mr. Minor provided her with subscriber information related to "RuhRowRagy@AOL.com."[21] A search of El Dorado's database revealed that a Jeff Ohnesorge had used "RuhRowRagy@AOL.com" to subscribe to EasyNews.com.[22] Mr. Minor also gave SA Coulter the service activation date and credit card number that Sgt Ohnesorge had used to purchase his account with EasyNews.com.[23] Armed with this information, SA Coulter provided the subscriber information to the SJA and to NCIS;[24] however, it was not until two weeks after she received this information that SA Coulter provided Mr. Minor with a U.S. Customs administrative summons requesting the subscriber information "associated with 'RuhRowRagy@AOL.com.'"[25]

At trial, Sgt Ohnesorge unsuccessfully moved to suppress the EasyNews.com subscriber information arguing he had a reasonable expectation of privacy in that information.[26] On appeal, Sgt Ohnesorge argued that the military judge erred in denying his motion to suppress, advancing two theories. First, he asserted he had a reasonable expectation of privacy in his subscriber information with EasyNews.com; therefore, Mr. Minor's release of the information without a search warrant, premised on probable cause, constituted an unreasonable search under the Fourth Amendment and Military Rule of Evidence (MRE) 311.[27] Second, he argued that SA Coulter obtaining his subscriber information without a warrant or similar authority violated his rights under the Electronic Communications Privacy Act (ECPA).[28]

To assert Fourth Amendment protection against unreasonable searches and seizures, a servicemember must demonstrate a reasonable expectation of privacy in the place to be searched or item to be seized.[29] Noting this to be an issue of first impression in the military, the NMCCA, citing the CAAF's opinion in *United States v. Allen*[30] and two other federal cases, held that there is no reasonable expectation of privacy in subscriber information provided to a commercial Internet service

---

[17] *Id.*

[18] *Id.*

[19] *Id.* at 948. An Internet search using the Google search engine reveals that El Dorado is headquartered in Phoenix, Arizona. *See* Eldorado, http://www.eldosales.com/ (last visited Mar. 29, 2006).

[20] *Ohnesorge*, 60 M.J. at 948.

[21] *Id.* At the time of her conversation with Mr. Minor, SA Coulter did not have a summons, subpoena, or search warrant for the requested information. *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.* at 947.

[27] *Id.* at 948; *see* MANUAL FOR COURTS MARTIAL, UNITED STATES, MIL. R. EVID. 311 (2005) [hereinafter MCM].

[28] *Ohnesorge*, 60 M.J. at 948. Specifically, Sergeant Ohnesorge alleged a violation Title II of the Electronic Communications Privacy Act (ECPA), 18 U.S.C.S. §§ 2510-2711 (LEXIS 2006). Title II of the ECPA has been referred to by several commentators as the "Stored Communications Act." *See* Orin Kerr, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy and the USA PATRIOT Act: Surveillance Law: Reshaping the Framework: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (Aug. 2004). With regard to Sergeant Ohnesorge's claim of a violation of the ECPA, the NMCCA initially noted that the ECPA does not list exclusion of evidence as a remedy for any violation, but ultimately declined to rule there had been a violation of the ECPA. *Ohnesorge*, 60 M.J. at 949. Presumably, such a finding would be unnecessary with the court's holding that Sergeant Ohnesorge did not have a reasonable expectation of privacy. Additionally, the violation of the ECPA would be relevant to the issue of Sergeant Ohnesorge's relationship with the Internet Service Provider (ISP). *See* 18 U.S.C.S. § 2703.

[29] *See* MCM, *supra* note 27, MIL. R. EVID. 311(a)(2). The concept of right to privacy as a predicate for Fourth Amendment protection can be traced to *Katz v. United States*, 389 U.S. 347 (1967). Prior to *Katz*, Fourth Amendment protection concerned itself with property rights rather than privacy rights until the Supreme Court proclaimed that the Fourth Amendment protects "people, not places." *Katz*, 367 U.S. at 351. The CAAF extended the expectation of privacy analysis to e-mail and digital media in *United States v. Maxwell*, 45 U.S. 406 (1996).

[30] 53 M.J. 402 (2000).

provider (ISP).[31] Relying on dicta in *United States v. Maxwell*,[32] the NMCAA explained that there is a fundamental difference between the content of private electronic communications and non-content information. The court found this difference particularly true in *Ohnesorge* because EasyNews.com required Sgt Ohnesorge to consent to the ISP's right to disclose any information "necessary to satisfy any law, regulation, or other government request."[33] Because Sgt Ohnesorge had no reasonable expectation of privacy in his subscriber information, he lacked any legal standing to assert either a Fourth Amendment claim or a claim of a violation of the Military Rules of Evidence.[34]

As an additional theory of admissibility, the NMCCA held that even if Sgt Ohnesorge had a reasonable expectation of privacy, the information and evidence uncovered as a result of SA Coulter's request would have been inevitably discovered through a proper authorization.[35] The NMCCA noted that SA Coulter eventually served an administrative summons for the subscriber information, and the trial counsel issued a subpoena to EasyNews.com for the same subscriber information.[36]

The NMCCA reaffirmed its holding in *Ohnesorge* in the unpublished case of *United States v. Szymcz*yk.[37] Major Wayne Szymczyk, U.S. Marine Corps, was convicted of possession of child pornography and conduct unbecoming an officer by possessing indecent computer images.[38] Major Szymczyk had a subscription with Infinity Internet Incorporated (Infinity), an ISP located in Temecula, California.[39] Using this ISP, Major Szymczyk accessed an Internet chatroom using the screen name "Aurther." Once in the chatroom, he started communicating with "SuzyQ17."[40] The "electronic conversation" turned sexual and culminated in Major Szymczyk sending "SuzyQ17" images of minors engaged in sexually explicit conduct.[41] Unfortunately for Major Szymczyk, "SuzyQ17" happened to be an undercover detective for the Miami-Dade County Police Department, who traced the screen name "Aurther" to Infinity and turned that information over to U.S. Customs officials.[42]

United States Customs officials turned the information over to the Riverside County Sheriff's Department in Riverside, California.[43] A Riverside County detective personally visited Infinity in Temecula in the hopes that Infinity would voluntarily provide the subscriber information to identify "Aurther."[44] The owner of Infinity turned over the subscriber information that revealed "Aurther" to be Major Szymczyk. Armed with this information, the Riverside County detective obtained a search warrant to search Major Szymczyk's house and computer. The search resulted in the seizure of hundreds of computer images of child pornography as well as images depicting bestiality and simulated rape.[45]

In due course, this evidence was turned over to military officials and charges were preferred and referred against Major Szymczyk. At trial, he moved to suppress the images, arguing that the search warrant contained information that had been seized from Infinity in violation of his Fourth Amendment right against a warrantless search, as well as in violation of the ECPA.[46] The military judge denied the motion to suppress.[47]

---

[31] *Ohnesorge*, 60 M.J. at 948-9. Specifically, the NMCAA relied on *United States v. Hambrick*, 55 F.Supp.2d 504 (W.D.Va. 1999) and *United States v. Kennedy*, 81 F. Supp. 2d 1103 (D.Kan.2000).

[32] 45 M.J. 406 (1996)

[33] *Ohnesorge*, 60 M.J. at 949 (citing to Appellate Exhibit IV).

[34] *Id.* at 949. Military Rule of Evidence 311(b)(2) requires that an accused establish a threshold requirement of a reasonable expectation of privacy in order to assert a violation of the military rules of evidence. MCM, *supra* note 27, MIL. R. EVID. 311(b)(2).

[35] *Ohnesorge*, 60 M.J. at 950 (citing Nix v. Williams, 467 U.S. 431 (1984)).

[36] *Id.* at 948 and 950.

[37] United States v. Szymczyk, No. 200000718, 2005 CCA LEXIS 184 (N-M. Ct. Crim. App. June 23, 2005) (unpublished).

[38] *Id.* at *3.

[39] *Id.*

[40] *Id.*

[41] *Id.* at *4.

[42] *Id.* at *4-5.

[43] *Id.*

[44] *Id.*

[45] *Id.* at *5.

[46] *Id.*

On appeal, the NMCCA relied heavily on the analysis of *Ohnesorge* and concluded that Major Szymczyk had no reasonable expectation of privacy in his subscriber information with Infinity and therefore could not assert a Fourth Amendment right.[48] The NMCCA also concluded that this information would have been inevitably discovered because the Riverside County detective who requested the information was ready to request a search warrant if Infinity had decided not to voluntarily turn over the subscriber information.[49]

Both *Ohnesorge* and *Szymczyk* are relatively non-controversial with regard to a finding of no reasonable expectation of privacy in subscriber information.[50] In fact, these holdings solidify the CAAF's suggestion in *Maxwell* that there is no reasonable expectation of privacy in subscriber information communicated to an ISP.[51] The issue left open for years has been whether, and how, a Fourth Amendment expectation of privacy extends to e-mail communications.[52] This issue has now been framed by the Navy Judge Advocate General in his appeal to the CAAF in *United States v. Long*.[53]

B. Expectation of Privacy in Government E-Mail Communications

Turning from non-content digital information to content digital information, the NMCCA held, in a remarkable opinion, that a naval servicemember has a reasonable expectation of privacy in government e-mail stored on a government server. Accordingly, the potentially most significant military case decided in 2005, within the context of search and seizure law, is *United States v. Long*.[54]

Lance Corporal (LCpl) (E-3) Jennifer N. Long, U.S. Marine Corps, was convicted of wrongful use of ecstasy, ketamine, and marijuana in violation of Article 112a, UCMJ.[55] Evidence used at trial consisted of eye-witness testimony and seventeen pages of e-mail transcripts in which LCpl Long discussed, with three separate individuals, her fear of testing positive for drugs in the event of a urinalysis and her efforts to attempt to mask her drug use.[56] One of LCpl Corporal Long's friends, Corporal (E-4) "U," testified during the government's case-in-chief and authenticated some of the e-mail correspondence as a back-and-forth e-mail exchange in which LCpl Long admitted use of marijuana and ecstasy and her concern about an upcoming urinalysis test.[57]

---

[47] *Id.*

[48] *Id.* at *9.

[49] *Id.* at *4 and *10.

[50] For those federal courts that have faced this particular issue, the trend has been a finding of no expectation of privacy in subscriber information. *See, e.g.*, Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).

[51] *See* United States v. Maxwell, 45 M.J. 406, 418 (1996) (analogizing the relationship between a computer network subscriber and the internet service provider as similar to that between a bank and it customer); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (no expectation of privacy in financial information voluntarily conveyed to banks); *cf.* Smith v. Maryland, 442 U.S. 735 (1979) (holding no reasonable expectation of privacy in the actual numbers dialed on a telephone as the capture of the numbers does not capture content). The CAAF declined to address the reasonable expectation of privacy issue with regard to subscriber information. *See* United States v. Allen, 53 M.J. 402, 409 (2000) (stating that "[w]e need not decide what type of privacy interest attached to the [subscriber] information in this case, however, because we agree with the military judge that a warrant would have inevitably been obtained for those very same records"). The Stored Communications Act part of the Electronic Communications Privacy Act, discussed at note 28, *supra*, requires disclosure by internet service providers of subscriber information (e.g. name, address, local and long distance telephone connection records, length or service, and means and source of payment) by use of an administrative subpoena. 18 U.S.C.S. § 2703(c)(2) (2006).

[52] In *Maxwell*, the CAAF concluded that Colonel Maxwell enjoyed an expectation of privacy in the content of his e-mails that had been sent on his America Online account; however, that expectation of privacy would necessarily turn on the type of e-mail involved and the intended recipients. *Maxwell*, 45 M.J. at 419.

[53] 61 M.J. 539 (N-M. Ct. Crim. App. 2005).

[54] *Id.* The impact of *Long* depends largely on how the CAAF decides the case. If the CAAF affirms the NMCCA's opinion, it could have a significant impact within the military because servicemembers would have an expectation of privacy in their government e-mail; however, if the CAAF vacates on narrow grounds, e.g., holding that LCpl Long did not establish that she had a subjective expectation of privacy because she did not testify at trial, the impact of *Long* would be relatively insignificant and limited to its facts.

[55] *Id*. at 540; *see* UCMJ art. 112a (2005).

[56] *Long*, 61 M.J. at 541. These e-mails were characterized as strings of e-mail exchanges between LCpl Long and three different individuals. *Id.* Presumably, these strings represented a digital recording of several e-mail exchanges between LCpl Long and the three recipients of her e-mail correspondence.

[57] *Id*. at 542.

Officials from the Inspector General's Office of Headquarters, U.S. Marine Corps (IGMC), requested the e-mail transcripts that had been seized from the network administrator for Headquarters, U.S. Marine Corps.[58] The network administrator accessed and retrieved the e-mails from the government network domain server at the specific request of government enforcement officials.[59] The request was made without a search warrant or search authorization.[60] Lance Corporal Long moved to suppress the e-mails, arguing that they had been seized in violation of her Fourth Amendment rights since the seizure had been without her consent and in the absence of a search authorization.[61]

The only witness to testify during LCpl Long's suppression hearing was the senior network administrator for Headquarters, U.S. Marine Corps.[62] The network administrator testified that LCpl Long had been assigned a government computer and an e-mail account.[63] Both the computer and the e-mail account were issued for official use; however, personal use of the government computer and the e-mail system was permissible provided such use did not "interfere with official business."[64] To access her government e-mail account, LCpl Long had to create her own password to protect against unauthorized users accessing her e-mail account and the government network.[65] Every e-mail that LCpl Long sent via her government computer went through a central government system domain server, where the e-mail was copied prior to its being sent to the intended recipient.[66] These copies of sent e-mail were automatically stored on the central domain server unless the user specifically configured the e-mail account *not* to save outgoing e-mail.[67] Any system administrator could access all e-mail accounts on the central domain server.[68] The senior system administrator testified that LCpl Long's e-mails were not retrieved during routine monitoring of the network system, but at the specific request of government officials.[69]

At trial, the military judge ruled that the actions of the network administrator constituted a search for evidence without LCpl Long's consent.[70] Additionally, the military judge ruled that the request by law enforcement had been made without a search authorization premised on probable cause.[71] The military judge admitted the evidence, however, based on his finding that LCpl Long had no reasonable expectation of privacy in her government e-mail account.[72]

On appeal, LCpl Long argued that the military judge committed error when he ruled that she had no reasonable expectation of privacy in her government e-mail account.[73] The NMCCA agreed that the military judge committed error in admitting the e-mail transcripts; however, the court held that the error was harmless beyond a reasonable doubt because the evidence of Long's guilt was otherwise overwhelming.[74] Despite the court affirming the case, the Navy Judge Advocate General certified this case to the CAAF.

---

[58] *Id*. at 541. Although unclear from the opinion, the investigation into LCpl Long's drug use began as an IGMC investigation. Officials from the IGMC requested the seizure of LCpl Long's e-mail.

[59] *Id.* at 540-41.

[60] *Id.* at 541.

[61] *Id*.

[62] *Id*.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] *Id.* Although unclear from the opinion, presumably LCpl Long did not configure her government issued computer e-mail account to delete outgoing messages. *Id.* If she had, the NMCCA would likely have mentioned that fact relative to the court's conclusion that she had a subjective expectation of privacy in her e-mail account.

[68] *Id*.

[69] *Id.*

[70] *Id.* Although unclear from the opinion, the government likely argued that LCpl Long consented to the search and seizure of the e-mails based on the "Notice and Consent to Monitoring" banner displayed each time she accessed the network via the government computer workstation. *Id.* In any event, the military judge appears to have rejected any consent theory that the government may have argued as an alternative theory of admissibility. *Id.*

[71] *Id.*

[72] *Id.* at 542.

[73] *Id.* at 540.

[74] *Id.* at 549.

The NMCCA's analysis and reasoning for why LCpl Long had a reasonable expectation of privacy is quite remarkable because two years earlier, the NMCCA reached the exact opposite holding in the unpublished case of *United States v. Geter*.[75] In any event, using *United States v. Monroe*[76]as a framework, the *Long* Court outlined the threshold requirement of establishing an expectation of privacy within the context of digital content information.[77] First, the NMCCA concluded that LCpl Long had a subjective expectation of privacy in her government e-mail account.[78] Notwithstanding that LCpl Long did not testify on the motion to establish how she had a subjective expectation of privacy, the NMCCA found a subjective expectation of privacy because her computer account required a password for access onto the government network.[79] Her use of a password to access the system "provided precautions necessary to safeguard her privacy in her e-mails, as well as her ability to exclude others from her e-mail account."[80] Additionally, the NMCCA concluded that the military judge "made no explicit finding" that LCpl Long had a subjective expectation of privacy.[81] Because of the lack of an explicit finding, the NMCCA made its own finding that LCpl Long had established a subjective expectation of privacy as to all other persons except for the network administrator.[82]

Having found a subjective expectation of privacy, the NMCCA moved to the next required step in the analytical process—whether LCpl Long's subjective expectation of privacy was "objectively reasonable."[83] Relying principally on two non-military federal cases, *Picha v. Wielgos*[84] and *United States v. Pryba*,[85] the NMCCA concluded that LCpl Long's subjective expectation of privacy was objectively reasonable.[86] The NMCCA's reliance on these two cases for the proposition that LCpl Long had a reasonable expectation of privacy is curious for several reasons. First, neither case had anything to do with electronic evidence. Second, neither case analyzed the concept of reasonable expectation of privacy. The issue in both cases dealt with whether there had been a government intrusion sufficient enough to trigger the protections of the Fourth Amendment.[87] The question of whether there is governmental intrusion sufficient to trigger Fourth Amendment protection is a separate question from whether a person has a reasonable expectation of privacy.[88]

---

[75] United States v. Geter, No. 9901433, 2003 CCA LEXIS 134 (N-M. Ct. Crim. App. May 30, 2003) (unpublished), *set aside and remanded on other grounds*, United States v. Geter, 60 M.J. 344 (2004) (summary disposition). In *Geter*, the NMCCA relied on the Air Force opinion of *United States v. Monroe*, 50 M.J. 550, 558 (A.F. Ct. Crim. App. 1999), for the proposition that when dealing "solely with a U.S. government owned and operated system, in which individual e-mail accounts are provided for official use only, there is no reasonable expectation of privacy." *Geter*, 2003 CCA LEXIS 134, at *7. On remand, the NMCCA rendered its *second* opinion on 8 November 2005. United States v. Geter, No. 9901433, 2005 CCA LEXIS 362 (N-M. Ct. Crim. App. Nov. 8, 2005) (unpublished). Curiously, the *Geter* court did not cite *Long*, and contrary to *Long*, concluded that the passwords LCpl Geter needed to access his government e-mail account, existed to "protect the integrity of the command information systems, not the personal interest of the appellant [Geter]." *Id.* at *5. Accordingly, the NMCCA concluded that LCpl Geter did not have a subjective expectation of privacy and thus the seizure of his e-mail did not implicate the Fourth Amendment.

[76] 52 M.J. 326, 330 (2000)

[77] *Long*, 61 M.J. at 543.

[78] *Id*. at 544.

[79] *Id. But see Geter*, 2005 CCA LEXIS 362, at *5 (stating that passwords exist and are created to "protect the integrity of the command information systems, not the personal interests" of the servicemember).

[80] *Long*, 61 M.J. at 544.

[81] *Id*. This conclusion does not support the other part of the opinion in which the court stated that the military judge found "that the appellant [Long] had no reasonable expectation of privacy in the e-mail account." *Id.* at 542. A plain reading of that sentence speaks to her personal and therefore *subjective* expectation of privacy.

[82] *Id.* at 544.

[83] *Id.* at 543 (quoting United States v. Monroe, 52 M.J. 326, 330 (2000)).

[84] 410 F. Supp. 1214 (N.D. Ill.1976)

[85] 502 F.2d 391 (D.C. Cir. 1974)

[86] *Long*, 61 M.J. at 545-46.

[87] The *Picha* case was a civil rights case in which thirteen-year old Renee Picha sued her school principal, Mr. Raymond Wielgos, after she was stripped-searched by the female school nurse on school property. The principal ordered Ms. Picha stripped-searched based on a phone tip that led him to believe Ms. Picha possessed drugs. Whether Renee Picha had a reasonable expectation of privacy against having her person stripped-searched was not an issue before the district court. The real issue was whether the search of Renee Picha by school officials constituted government intrusion sufficient to trigger her right against an unreasonable search and seizure. *Picha*, 410 F. Supp. at 1216. In its opinion, the *Picha* court simply held that the school officials were not entitled to a directed verdict based on being immune from civil liability. *Id*. at 1221. Similarly, in *Pryba*, the issue was not whether Mr. Pryba had a reasonable expectation of privacy in the search of the package that led to his prosecution for possession of pornographic videotapes; it was whether there had been sufficient governmental action to trigger Mr. Pryba's rights against a warrantless search. Based on the suspicious behavior on the part of the sender, United Airlines officials searched the package addressed to Mr. Pryba prior to its shipment via United Airlines cargo freight and then turned the package over to the Federal Bureau of Investigation. The *Pryba* Court rejected Mr. Pryba's Fourth Amendment claim holding that the initial search of the package by United Airlines officials was done on the carrier's own initiative, independent of any governmental action or intrusion. *Pryba*, 502 F.2d at 398.

Police participation or government intrusion may be germane to two issues: (1) the level of law enforcement involvement or participation sufficient to implicate protection under the Fourth Amendment; and, (2) the reasonableness of the warrantless search or seizure based on all factors. The level of government involvement or law enforcement participation should not turn on whether a person has a reasonable expectation of privacy. Objective expectation of privacy analysis should turn on objective factors relative to the person seeking protection.[89] Motivation of government officials is relevant to an evaluation of the reasonableness of a search, not to whether an individual has a reasonable expectation of privacy.[90]

When the NMCCA focused on the level of government intrusion and the purpose of the search, it found first a reasonable expectation of privacy and then *a fortiori* a per se unreasonable search. The NMCCA appears to have adopted the same general analytical standard that the Ninth Circuit adopted in *O'Connor v. Ortega*.[91] On appeal, the Supreme Court stated that this type of analysis was incomplete.[92] In reversing the *O'Connor* case, the Supreme Court held that the Ninth Circuit erred in finding a Fourth Amendment violation after concluding that Doctor Ortega had an expectation of privacy in his office.[93] The *O'Connor* plurality opinion makes clear that the Ninth Circuit should have extended the analysis to whether or not the search was reasonable under the circumstances given the "special needs" of public employers to supervise and control the work environment.[94]

The NMCCA also parsed the concept of reasonable expectation of privacy and concluded that it depended not only on the motivation of government officials, but also on the situational relationship between LCpl Long and other government officials.[95] The *Long* Court found the search per se unreasonable and rejected the government's assertion that based on the

---

> But where the search is made on the carrier's own initiative for its own purposes, Fourth Amendment protections do not obtain for the reason that only the activities of individuals or nongovernmental entities are involved. So frequently and so emphatically have the courts enunciated these principles that at least for the time being, they must be regarded as settled law.

Id. Not unlike *Picha*, the issue of whether Mr. Pryba had a reasonable expectation of privacy against officials searching the sealed package addressed to him was not a contested issue.

[88] *See, e.g.*, Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614-16 (1989) (stating that to implicate protections under the Fourth Amendment, there must be "clear indices of the Government's encouragement, endorsement, and participation" in the search or seizure).

[89] *Cf.* Soldal v. Cook County, 506 U.S. 56, 69 (1992) (finding that the subjective motivation of law enforcement officials provides an unworkable framework in determining whether Fourth Amendment protections apply).

[90] *See* O'Connor v. Ortega, 480 U.S. 709 (1987) (remanding case back to Ninth Circuit finding that the issue of reasonable expectation of privacy is only a threshold consideration based on objective factors) (plurality opinion).

[91] 764 F.2d 703 (9th Cir. 1985).

[92] *See O'Connor*, 480 U.S. at 719 (stating that to "hold that the Fourth Amendment applies to searches conducted by [public employers] is only to begin the inquiry into the standards governing such searches. . . . [W]hat is reasonable depends on the context within which a search takes place"); *see also* State v. Ziegler, 637 So. 2d 109, 112 (La. 1994).

> The O'Connor Court set forth a two-pronged analysis for determining whether an employee's Fourth Amendment rights were violated by an administrative search and seizure. First, the employee must have a reasonable expectation of privacy in the area searched, or in the item seized. . . . Second, if a reasonable expectation of privacy exists, the Fourth Amendment requires that the search be reasonable under the circumstances.

Id. at 112.

[93] "To hold that the Fourth Amendment applies to searches conducted by [public employees] is only to begin the inquiry into the standards governing such searches. . . . [W]hat is reasonable depends on the context with which the search takes place." *O'Connor*, 480 U.S. at 719 (quoting New Jersey v. T.L.O., 469 U.S. 325, 337 (1985)).

[94] *Id*. at 720.

> Employers and supervisors are focused primarily on the need to complete the government agency's work in a prompt and efficient manner. An employer may have need for correspondence, or a file or report available only in an employee's office while the employee is away from the office. Or . . . employers may need to safeguard or identify state property or records in an office in connection with a pending investigation into suspected employee misfeasance. In our view, requiring an employer to obtain a search warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome. Imposing unwieldy warrant procedures in such cases upon supervisors, who would otherwise have no reason to be familiar with such procedures, is simply unreasonable.

Id. at 721-22.

[95] United States v. Long, 61 M.J. 539, 546 (N-M. Ct. Crim. App. 2005). First, the *Long* court concluded that LCpl Long enjoyed a "subjective expectation of privacy in her e-mail account as to all others but the network administrator." *Id*. at 544. Second, the *Long* Court concluded that her subjective expectation of privacy was reasonable "vis-à-vis law enforcement." Such a legal construct appears flawed as it "would be anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior." *O'Connor*, 480 U.S. at 715 (quoting *T.L.O.*, 469 U.S. at 335).

"Notice and Consent for Monitoring" banner LCpl Long had no reasonable expectation of privacy. The court stated that because the banner does not "mention search and seizure of evidence of crimes unrelated to unauthorized use of government computer,"[96] the banner did not provide sufficient notice to LCpl Long so as to defeat her expectation of privacy for law enforcement purposes. Although unstated, the court must have concluded that the search was unjustified at its inception and per se unreasonable.[97] This search analysis, however, is separate from the reasonable expectation of privacy analysis under *O'Connor*.[98]

In reaching its conclusion that LCpl Long had an expectation of privacy, the court also did not analyze the *character* of the evidence. The evidence supports that the e-mail transcripts the government admitted at trial were actually e-mail strings demonstrating an "electronic conversation" with three separate individuals.[99] In fact, one of the witnesses who testified against LCpl Long authenticated ten out of seventeen pages as a "string of e-mails and response e-mails between himself" and LCpl Long.[100] In this regard, the *Long* court did not analyze whether or not the e-mails had been opened, which presumably would have some bearing on LCpl Long's expectation of privacy. The CAAF in *United States v. Maxwell*[101] compared e-mail to other types of mediums and held that "[e]xpectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient."[102] This analysis in *Maxwell* parallels the statutory scheme of the Stored Communications Act (SCA) of the ECPA.[103] When Congress enacted the SCA, it created a statutory expectation of privacy in certain types of e-mail.[104] An analysis of the SCA reveals that statutory protections apply differently depending on the *character* of the e-mail, the starkest difference being between unopened e-mail and e-mail that has been delivered and opened.[105] It follows that the *Long* court should have followed the *Maxwell* court by analyzing the e-mails according to their character when they were seized.[106] Unfortunately, the NMCCA did not differentiate between unopened e-mail, which would implicate a greater expectation of privacy, and opened e-mail.[107] In fact, the court created a greater right to privacy in *opened* e-mail stored on a government server than in opened e-mail stored on a commercial ISP.[108]

---

[96] *Long*, 61 M.J. at 544.

[97] *See O'Connor*, 480 U.S. at 725-26 (stating that searches by public employers should be judged by the "standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable").

[98] The *O'Connor* Court specifically left open the question of what the appropriate reasonableness standard should be "when an employee is being investigated for criminal misconduct." *Id.* at 729 n.*. Nevertheless, the opinion makes clear that the threshold finding of a reasonable expectation of privacy is different from whether the search is in scope and reasonable at its inception.

[99] *Long*, 61 M.J. at 541.

[100] *Id.* at 548.

[101] 45 M.J. 406, 418-19 (1996).

[102] *Id.* at 418-19.

[103] *See* 18 U.S.C.S. §§ 2701-2711 (2006). This statute was enacted as Title II of the Electronic Communications Privacy Act (ECPA), but given the formal title "Stored Wired and Electronic Communications and Transactional Records Access." According to one of the leading legal commentators on the ECPA, Associate Professor Orin S. Kerr, George Washington University Law School, the easiest and simplest way to refer to the statute is as the Stored Communications Act. *See* Kerr, *supra* note 28.

[104] *See* Kerr, *supra* note 28, at 1211 (questioning whether electronic files held by Internet Service Providers on "behalf of their users retain a Fourth Amendment reasonable expectation of privacy") (internal quotations omitted); *see also id.* n.14 (quoting United States v. Bach, 310 F.3d 197 (1st Cir. 2004) ("While it is clear to this court that Congress intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation or privacy derives from the Constitution")).

[105] To bolster its opinion, the NMCCA relied on 18 U.S.C.S. § 2702 of the Stored Communications Act. *Long*, 61 M.J. at 545. Reliance on that statute seems misplaced. The voluntary disclosure rules of 18 U.S.C.S. § 2702 are inapplicable to the case because the threshold consideration for statutory applicability is whether the "person or entity provid[es] electronic communication service to the public." *Id.* § 2702(a)(1). A government e-mail system is not available to the public so the SCA's voluntary disclosure limitations would be inapplicable. With regard to the compelled disclosure rules of the SCA, 18 U.S.C.S. § 2703, there is a fundamental difference between unopened e-mail, unopened e-mail held in electronic storage for one hundred and eighty days or less, and opened e-mail that are simply remotely stored on a server. *See* Kerr, *supra* note 28, at 1226-27. In fact, "opened e-mail held by a provider is protected" by the SCA *only* if the computer system and server "provides services to the public." *Id*. Thus, the protections of the SCA that the *Long* court mentions in its opinion are inapplicable given that the e-mail in question had been opened and read. Opened e-mail held in storage receives protection under the SCA, but only to the extent that a service provider qualifies as a "remote computing service." *See* 18 U.S.C.S. § 2703(b). To meet the definition of remote computing service, a computing service *must* provide services to the public. *See id.* § 2711(2). Since the computing services in this case dealt with a nonpublic provider, LCpl Long's opened e-mail would receive no protection under the SCA. A thorough analysis of the SCA is beyond the scope of this article; however, practitioners interested in a thorough and straight-forward analysis of the SCA, should consult Professor Kerr's article. *See* Kerr, *supra* note 28.

[106] *See Maxwell*, 45 M.J. at 419 (stating that "e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient"). The evidentiary character of the e-mails in question were probably not analyzed by the military judge at trial because such a finding would have been unnecessary.

[107] *Cf.* United States v. Miller, 425 U.S. 435, 443 (1976).

Due to the potential implications of *Long*, the Navy Judge Advocate General certified the case on 7 July 2005.[109] On 13 October 2005, LCpl Long filed a cross-appeal arguing that the NMCCA erred by finding harmless error.[110] On 21 February 2006, the CAAF heard oral argument on the *Long* case and a decision is pending.[111] The holding could have potentially wide implications with regard to carving out a reasonable expectation of privacy for certain types of digital evidence contained on a government-issued computer.[112]

C. Scope of Consent on Standard Computer Consent Search Form

In *United States v. Rittenhouse*,[113] the U.S. Army Court of Criminal Appeals (ACCA) had an opportunity to analyze the scope of consent within the context of a computer search. Sergeant Josh R. Rittenhouse (SGT), U.S. Army, was suspected of possession of child pornography located on his private computer in his barracks room.[114] Sergeant Rittenhouse was ordered to report to the local Army Criminal Investigation Command (CID) where he waived his rights and executed a sworn statement.[115] Special Agent Kristie Cathers conducted the interview of SGT Rittenhouse and also requested consent to search

---

> The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 435.

[108] The NMCCA in *Long* would require the government to get a search authorization premised on probable cause under the Fourth Amendment for e-mail content regardless of whether the e-mail had been opened. In contrast, if LCpl Long would have had her opened e-mails stored on a public ISP, AOL for example, the protections of the SCA would apply to the extent that AOL is a remote computing service for purposes of 18 U.S.C.S. § 2703. Under this hypothetical, one option available to the government would be to compel disclosure from AOL of stored e-mails via an 18 U.S.C.S. § 2703(d) order (with notice to the customer), in which the standard is much less than probable cause. *See* 18 U.S.C.S. § 2703(d) (disclosure by a public ISP will occur if a court of competent jurisdiction issues a court order provided that the government "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, . . . are relevant and material to an ongoing criminal investigation").

[109] Article 67(a)(2) of the UCMJ allows the service Judge Advocates General to order any case a Court of Criminal Appeals has reviewed to be sent to the Court of Appeals for the Armed Forces for review. *See* UCMJ art. 62 (2005), 10 U.S.C. § 862 (2000), This government "appeals process" is referred to as certification, in which the applicable Judge Advocate General certifies a particular legal issue. *See* United States Court of Appeals for the Armed Forces, Rules of Practice and Procedure R.4, *available at* http://www.armfor.uscourts.gov/Rules041001.pdf. The Navy Judge Advocate General certified the following two issues:

> I. WHETHER THE NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS ERRED WHEN THEY DETERMINED THAT, BASED ON THE EVIDENCE ADDUCED AT TRIAL, APPELLEE HELD A SUBJECTIVE EXPECTATION OF PRIVACY IN HER E-MAIL ACCOUNT AS TO ALL OTHERS BUT THE NETWORK ADMINISTRATOR.
>
> II. WHETHER THE NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS ERRED WHEN THEY DETERMINED THAT IT IS REASONABLE, UNDER THE CIRCUMSTANCES PRESENTED IN THIS CASE, FOR AN AUTHORIZED USER OF THE GOVERNMENT COMPUTER NETWORK TO HAVE A LIMITED EXPECTATION OF PRIVACY IN THEIR E-MAIL COMMUNICATIONS SENT AND RECEIVED VIA THE GOVERNMENT NETWORK SERVER.

61 M.J. 326-27 (7 July 2005) (certificate for review).

[110] On 13 October 2005, the Court of Appeals for the Armed Forces granted LCpl Long's request to review the following issue:

> WHETHER THE LOWER COURT ERRED IN FINDING THAT THE MILITARY JUDGE'S ERROR IN ADMITTING E-MAILS SENT AND RECEIVED BY LANCE CORPORAL LONG ON HER GOVERNMENT COMPUTER WAS HARMLESS BEYOND A REASONABLE DOUBT.

62 M.J. 316 (13 Oct. 2005) (order granting review.)

[111] *See* United States Court of Appeals for the Armed Forces, Daily Journal No. 06-095, http://www.armfor.uscourts.gov/journal/2006Jrnl/2006Feb.htm (last visited Mar. 30, 2006).

[112] The CAAF could answer the question it did not address in *United States v. Monroe*, 52 M.J. 326, 330 (2000). In *Monroe*, the CAAF's holding was narrower than the Air Force Court of Criminal Appeals. Whereas, the Air Force Court concluded Staff Sergeant Monroe had no reasonable expectation of privacy, the CAAF held Monroe had "no reasonable expectation of privacy in his e-mail messages or his e-mail box *at least from the personnel* charged with maintaining the [Government-owned] EMH [electronic mail host] system." (emphasis added).

[113] 62 M.J. 509 (Army Ct. Crim. App. 2005)

[114] *Id*. at 510.

[115] In addition to the Fourth Amendment issue in *Rittenhouse*, the military judge suppressed part of Sergeant Rittenhouse's sworn statement. *Id*. at 511. Following the CID interrogation, Special Agent Cathers had requested that Sergeant Rittenhouse write down in his own words what they had discussed. She then told Sergeant Rittenhouse not to "close out" his sworn statement because she planned to follow-up his written statement with a question-and-answer session. *Id.* at 510. When Sergeant Rittenhouse finished his statement, he wrote "End of Statement." The military judge concluded that this statement constituted an ambiguous or equivocal invocation of the right to remain silent and the CID agents should have sought clarification of this ambiguous

his computer.[116] Special Agent Cathers gave SGT Rittenhouse CID Form 87-R-E, Consent to Search.[117] Sergeant Rittenhouse signed the form consenting to the search of his computer.[118] Based on his admissions and the search of his computer, he was charged with violation of Article 134, UCMJ, for possession of child pornography.[119]

Prior to entry of pleas, SGT Rittenhouse moved to suppress the search and seizure of his computer.[120] Specifically, he argued that seizure and removal of his computer were beyond the scope of his consent.[121] Sergeant Rittenhouse's argument was premised on the consent form he signed, which authorized CID to *search* his computer, but did not authorize CID to *seize and remove* his computer.[122] Because the CID form did not explicitly authorize the seizure and removal of SGT Rittenhouse's computer from the premises, the military judge ruled that all evidence seized and removed was done without consent and in violation of the Fourth Amendment.[123] Based on the military judge's suppression of the evidence, the government filed an appeal to the ACCA.[124]

The ACCA vacated the military judge's ruling to suppress the evidence.[125] The *Rittenhouse* court analyzed the language allowing for the seizure of specific evidence to include "data including deleted files and folders."[126] Based in part on this language, the court concluded that any "reasonable person reading the consent form would have understood that the computer and disks could be seized."[127] Given standard computer forensic practice, the *Rittenhouse* court held that SGT Rittenhouse's consent to search his computer necessarily included inherent authorization to seize the computer and associated data storage media.[128] Despite this holding, practitioners and law enforcement officials should pay close and careful attention to any consent form so that the verbiage in the consent form makes it explicitly clear that the computer and associated data storage media and devices may be seized for follow-on forensic analysis.[129]

---

invocation. As a result, the military judge, finding a violation of Rittenhouse's Fifth Amendment right to remain silent, suppressed Rittenhouse's statements that were made subsequent to his having written "End of Statement." *Id.* As part of the government appeal, the ACCA also vacated that part of the military judge's ruling, holding that "End of Statement" may have constituted an ambiguous invocation to remain silent, but the CID agents did not have to stop questioning in order to seek clarification. The ACCA agreed it was an ambiguous invocation, but the law does not require an interrogator to stop and seek clarification of an ambiguous invocation. *Id*. at 512.

[116] *Id.* at 510.

[117] *Id*. The ACCA appended a copy of the consent form to its opinion. *Id.* at 515.

[118] *Id.*

[119] *Id*.; *see* UCMJ art. 134 (2005); 10 U.S.C. § 934 (2000).

[120] *Rittenhouse,* 62 M.J. at 510.

[121] *Id.*

[122] At the bottom of paragraph 5 of the consent form, Sergeant Rittenhouse consented to a search of "computers, hard disk drives, removable storage media, portable data storage devices, cameras, photographs, movies, manuals, notebooks, papers, and computer input and output devices;" however, the consent form also contained the following additional language:

> I am authorizing the above search(s) for the following types of property which may be *removed* by the authorized law enforcement personnel and retained as evidence under the provisions of Army Regulation 195-5, or other applicable laws or regulations:
>
> Text, graphics, electronic mail messages, and other data including deleted files and folders, containing material related to the sexual exploitation of minors; and/or material depicting apparent or purported minors engaged in sexually explicit conduct; and data and/or information used to facilitate access to, possession, distribution, and/or production of such material.

Id. at 515 (emphasis added).

[123] *Id.* at 511.

[124] *Id.* at 509. Under Article 62, UCMJ, the government may appeal any order or ruling—except for a finding of not guilty—that terminates the proceedings with respect to a charge or specification.

[125] *Id.* at 514.

[126] *Id.* at 513 n.6.

[127] *Id.* at 513.

[128] *Id.*

[129] This is particularly true given that under MRE 316, an accused may limit consent and withdraw consent at any time. *Compare* MCM, *supra* note 27, MIL.R.EVID. 316 (d)(2), *with id.* MIL.R.EVID. 314 (e)(3). In this regard, agents seizing computer assets would do well to image the computer hard drive as soon as possible after the seizure.

D. Scope of Voluntary Consent in Computer Search Following Illegal Search

The question of whether a servicemember has a reasonable expectation of privacy in government e-mail is not the only computer-type search and seizure issue that the CAAF will tackle in its 2006 term. On 13 July 2005, the CAAF granted review in *United States v. Conklin*,[130] in which the CAAF will decide the scope of consent following an initial illegal search.

Airman First Class (A1C) Steven L. Conklin, U.S. Air Force, had temporary duty orders to Keesler Air Force Base (AFB) as part of a five-phase training program.[131] He was assigned to an on-base dormitory room.[132] As part of a routine and random inspection, A1C Conklin's military training leader (MTL) inspected A1C Conklin's room.[133] Following the MTL's inspection of the dresser, A1C Conklin's computer monitor powered up and displayed an image of an actress wearing a fishnet top that clearly exposed her breasts.[134] This image was a violation of Keesler AFB dormitory regulations that prohibited the open display of nude or partially nude persons.[135] After seeing this image, the MTL contacted a senior MTL, Technical Sergeant (TSgt) Edward Schlegel, who searched A1C Conklin's computer.[136] Technical Sergeant Schlegel found a folder titled "porn" and a subfolder titled "teen."[137] He opened six to eight files, each containing images of young nude females.[138] He then secured the room and notified the Air Force Office of Special Investigations (OSI).[139] Two OSI agents contacted A1C Conklin in the dining hall and asked for consent to search his room and computer.[140] The agents did not tell A1C Conklin about the earlier inspection.[141] He consented to the search of his room and computer for evidence of child pornography.[142] The OSI agents found a large number of images of child pornography, and A1C Conklin subsequently confessed to the agents that he had borrowed some compact discs containing adult and child pornography from a friend and had copied the images onto his computer.[143]

At trial, A1C Conklin moved to suppress the images of child pornography based on the theory that the derivative evidence was seized as a result of an initial illegal search of his computer, which, in turn, rendered his consent invalid.[144] The military judge concluded that given the unique training environment, the initial search of A1C Conklin's personal computer by TSgt Schlegel was a valid inspection.[145] Additionally, the military judge concluded that A1C Conklin gave

---

[130] United States v. Conklin, No. 35217, 2004 CCA LEXIS 290 (A.F. Ct. Crim App. 2004) (unpublished). On 13 July 2005, the CAAF granted A1C Conklin's appeal on the following two issues:

> I. WHETHER THE MILITARY JUDGE ERRED IN ADMITTING EVIDENCE AT TRIAL THAT WAS OBTAINED AS A DIRECT RESULT OF AN ILLEGAL SEARCH OF APPELLANT'S PERSONAL COMPUTER.
>
> II. WHETHER THE EVIDENCE PRESENTED BY THE PROSECUTION AT TRIAL WAS LEGALLY INSUFFICIENT TO SUPPORT APPELLANT'S CONVICTION FOR POSSESSING CHILD PORNOGRAPHY.

61 M.J. 330 (2005) (order granting petition for review).

[131] *Conklin*, 2004 CCA LEXIS 290 at *3.

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] The dormitory regulation in this case, *Keesler Air Force Base Instr. 32-6003*, prohibited the "open display of pictures, statues, or posters which display the nude or partially nude human body." KEESLER AIR FORCE BASE INSTR. 32-6003, DORMITORY SECURITY AND LIVING STANDARDS FOR NON-PRIOR SERVICE AIRMEN 4.2.3 (30 Aug. 2003)

[136] *Conklin*, 2004 CCA LEXIS 290, at *3-4.

[137] *Id*. at *4.

[138] *Id.*

[139] *Id.*

[140] *Id*.

[141] *Id*.

[142] *Id*.

[143] *Id*. at *4-5.

[144] *Id*.

[145] *Id*. at *8.

voluntary consent to the search of his computer.[146] The military judge admitted the evidence and A1C Conklin was convicted of possession of child pornography.[147]

On appeal, and as a threshold matter, the Air Force Court of Criminal Appeals (AFCCA) held that A1C Conklin had a reasonable expectation of privacy in his personal computer, even though the computer was located in his government dormitory room.[148] With regard to the displayed image of the partially clad actress, the AFCCA concluded that A1C Conklin had forfeited his right to privacy;[149] however, the court held that he maintained his right to privacy as to the other non-displayed content on his personal computer.[150] Once the AFCCA concluded that A1C Conklin enjoyed a reasonable expectation of privacy to the non-displayed content, the court then analyzed whether or not there was any lawful basis for TSgt Schlegel's initial warrantless search of the computer files.[151]

The AFCCA held that the stated purpose of the Keesler AFB dormitory instruction, which authorized random inspections, was to ensure "standards of cleanliness, order, décor, safety, and security."[152] Since the initial search of A1C Conklin's computer had nothing to do with "cleanliness, order, décor, safety, [or] security" of his assigned dormitory room, the AFCCA held that TSgt Schlegel's search violated the scope of the inspection exception under MRE 313.[153] The court reached this conclusion because the warrantless search of the computer was unrelated to the purpose of the instruction and therefore exceeded the authorized scope and purpose of the inspection.[154]

Nevertheless, the AFCCA, citing *United States v. Murphy*,[155] concluded that A1C Conklin's consent to the subsequent search by OSI agents was voluntary.[156] The court based its rationale of voluntary consent on the fact that A1C Conklin "was not in custody, was not evasive or uncooperative, and acknowledged that he had the legal right to refuse to give his consent."[157] The court rejected A1C Conklin's argument that the OSI agents would not have requested consent "but for" the prior illegal search by TSgt Schlegel. The *Conklin* court did not fully analyze A1C Conklin's derivative evidence argument other than to cite to *Murphy*.[158] While the *Murphy* court rejected a simple "but for" test on whether to apply the "fruit of the poisonous tree" doctrine to derivative evidence, A1C Conklin was unaware of the prior constitutional violation.[159] Doubtless, this will be the issue that the CAAF will confront in shaping the legal boundaries of the consent exception to the Fourth Amendment.[160]

---

[146] *Id*.

[147] *Id*. at *9

[148] *Id*.

[149] *Id*. at *11.

[150] *Id.* at *12.

[151] *Id.* at *12-13.

[152] *Id.* at *13.

[153] *Id*. *13-15; *see* MCM, *supra* note 27, MIL. R. EVID. 313.

[154] *Conklin*, 2004 CCA LEXIS 290 at *15.

[155] 39 M.J. 486 (C.M.A. 1994)

[156] *Conklin*, 2004 CCA LEXIS 290, at *16.

[157] *Id*.

[158] 39 M.J. at 486.

[159] *Compare id.* at 487 (Staff Sergeant Murphy was factually (but maybe not *legally*) aware that her rights under Article 31(b) had been violated), *with Conklin*, 2004 CCA LEXIS 290, at *4 (the OSI agents did not tell A1C Conklin about TSgt Schlegel's earlier warrantless search).

[160] According to Wayne LaFave in his hornbook *Search and Seizure, A Treatise on the Fourth Amendment*, evidence should only be admissible "if it is determined that the consent was *both* voluntary and not an exploitation of the prior illegality." *See* 3 WAYNE LAFAVE, SEARCH AND SEIZURE, A TREATISE ON THE FOURTH AMENDMENT 656 (3d ed. 1996). The CAAF heard oral argument on A1C Conklin's case on 8 November 2005.

Part II: Scope of Probable Cause for Securing Search Authorization

A. Refined Legal Definition of Probable Cause

In its only Fourth Amendment opinion of its 2005 term, the CAAF refined the legal meaning of "probable" with regard to the quantum of evidence required to establish probable cause. *United States v. Bethea*[161] established a benchmark standard for the definition of "probable" as a legal term of art.[162] *Bethea* is likely to become a lodestar for practitioners and military judges, both trial and appellate, for evaluating, in terms of objective metrics, what constitutes probable cause sufficient for the issuance of a search authorization.[163]

Air Force Master Sergeant (MSgt) Terrence A. Bethea tested positive on a random urinalysis for the cocaine metabolite at 238 nanograms per milliliter.[164] When questioned by OSI agents, MSgt Bethea maintained that he had not knowingly used cocaine.[165] Following MSgt Bethea's denial of cocaine use, OSI Special Agent Michael Tanguay requested a search authorization from the Base Magistrate, Air Force Colonel Dale Hess, to seize a hair sample from MSgt Bethea.[166] Special Agent Tanguay presented an affidavit to Colonel Hess in which SA Tanguay explained the purpose of the hair seizure and that a hair may reveal whether or not MSgt Bethea had ingested cocaine.[167] Specifically, SA Tanguay stated in his affidavit that depending on the length of a person's hair, a scientific test of the hair will detect chronic drug use as well as binge use of cocaine ingested within the last several months.[168] Special Agent Tanguay did not inform Colonel Hess that hair testing would not necessarily reveal one-time use of a small amount of cocaine.[169] Colonel Hess approved the search authorization and the analysis of MSgt Bethea's hair revealed multiple uses of cocaine.[170] Based on the hair analysis, MSgt Bethea was charged with wrongful use of cocaine on divers occasions between 17 January and 16 February 2001.[171]

Master Sergeant Bethea moved to suppress the seizure of hair based on lack of probable cause.[172] Specifically, MSgt Bethea argued that there was no probable cause to seek the hair analysis because there was no evidence of binge or chronic use from the urinalysis test.[173] In other words, no probable cause existed because there was no causal connection between the underlying urinalysis that reveals one-time use and hair drug testing that cannot detect a "specific single use."[174] Additionally, MSgt Bethea argued that SA Tanguay had withheld evidence from the magistrate because he did not inform the magistrate that hair analysis would not reveal a single use of cocaine.[175] The military judge denied the motion to suppress. He found probable cause based on his conclusion that it was "more than reasonable to assume, based on the contents of the

---

[161] 61 M.J. 184 (2005).

[162] *See* WEBSTER'S UNABRIDGED DICTIONARY (Random House 2d ed. 1998) (defining probable as: "1. likely to occur or prove true; 2. having more evidence for than against; and, 3. affording ground for belief").

[163] Probable cause exists "when there 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 27, MIL. R. EVID. 315(f)(2).

[164] *Bethea*, 61 M.J. at 184.

[165] *Id.* at 185.

[166] Colonel Dale A. Hess, U.S. Air Force, was the Yokota Air Base's primary magistrate. *Id*.

[167] *Id.*

[168] *Id.* Special Agent Tanguay's affidavit also compared urine testing for drugs and hair testing for drugs: "While urine tests can determine whether a drug was used at least once within the recent past, hair analysis potentially provides information on binge use or chronic drug use ranging from months, depending on the length of the hair and the type of hair." *Id.*

[169] *Id.*

[170] *Id.*

[171] *Id.* at 184.

[172] *Id.* at 185.

[173] *Id*. at 185-86.

[174] *Id.* at 185. Special Agent Nuckols of the OSI testified at the suppression hearing that he did not know if hair analysis can reveal only a single use; however, he did testify that hair analysis would reveal a "binge" use. Special Agent Nuckols defined binge use as "numerous uses over a short period of time, 12, 24, 36 hours." *Id*.

[175] *Id.* at 186. The military judge concluded that there was no evidence that OSI intentionally or recklessly withheld relevant information from Colonel Hess.

affidavit, that hair drug testing can detect a . . . single drug use if the hair test is performed within two months of the alleged use, regardless of how that use may be characterized."[176]

In affirming the case, the CAAF refused to engage in the "semantic" analysis of what "binge use" meant or whether hair analysis would be able to detect a single use of cocaine.[177] Without expressing an opinion of the correctness of the military judge's conclusion regarding whether or not hair analysis can detect a single use, the CAAF elegantly side-stepped the issue, and in the process, changed military jurisprudence with regard to the definition of probable cause.[178] Citing *Illinois v. Gates*[179] and *Texas v. Brown*,[180] the CAAF held that there was probable cause to support the search authorization despite the fact that hair analysis would not necessarily be indicative of a one-time use of cocaine.[181] "A probable cause determination merely requires that a person of 'reasonable caution' could believe that the search may reveal evidence of a crime; 'it does not demand any showing that such a belief be correct or more likely true than false.'"[182] The CAAF then cited several federal cases that stand for the proposition that "probable cause does not require a showing that an event is more than 50% likely."[183]

Once the CAAF refined the legal definition of probable cause, the next analytical step was easy, because the urinalysis results could be consistent with single use or multiple uses.[184] Accordingly, it was as "likely as not that evidence of cocaine use would be found in [MSgt Bethea's] hair."[185] The holding in *Bethea* is important for several reasons. First, it reflects that the proper evaluation for probable cause by appellate courts is by an objective metric.[186] Second, it refines further the legal definition of the quantum of evidence necessary for probable cause. Third, it signals a green light for commanders, magistrates, and military judges to order search authorizations for the seizure of hair based on a positive urinalysis.

B. Reasonableness of Seizure in Executing a Search Warrant

Inasmuch as the CAAF refined the definition of probable cause in *Bethea*, the Supreme Court refined and extended its earlier holding of *Michigan v. Summers*,[187] which held that when executing a search warrant on a residence, law enforcement officials have the inherent authority to detain or seize an occupant of the residence while the search is conducted. In *Muehler v. Mena*,[188] the Court further extended the limits of when a detention rises to the level of an unreasonable seizure for Fourth Amendment purposes. In doing so, the Supreme Court vacated another opinion from the Ninth Circuit.[189]

---

[176] *Id.*

[177] *Id*. at 187.

[178] *Id*. at 186-87. In fact, the CAAF specifically cautioned practitioners and military judges that the court expressed no opinion as "to the correctness of the military judge's interpretation of 'binge' of the accuracy of the military judge's characterization of the ability of hair analysis to detect a single use of a controlled substance." *Id.* at 186 n.3.

[179] 462 U.S. 213 (1983).

[180] 460 U.S. 730 (1983).

[181] *Bethea*, 61 M.J. at 187.

[182] *Id.* (quoting *Brown*, 460 U.S. at 742).

[183] *Id*. (citing United States v. Olson, No. 03-CR-51-S, 2003 U.S. Dist. LEXIS 24607, at *16 (W.D. Wis. July 11, 2003) (citing United States v. Garcia, 179 F.3d 265, 269 (5th Cir. 1999)); *see also* Ostrander v. Madsen, Nos. 00-35506, 00-35538, 00-35541, 2003 U.S. App. LEXIS 1665, at *8 (9th Cir. Jan. 28, 2003) ("Probable cause is met by less than a fifty percent probability, so that even two contradictory statements can both be supported by probable cause."); Samos Imex Corp. v. Nextel Communications, Inc., 194 F.3d 301, 303 (1st Cir. 1999) ("The phrase 'probable cause' is used, in the narrow confines of Fourth Amendment precedent, to establish a standard less demanding than 'more probable than not.'"); United States v. Burrell, 963 F.2d 976, 986 (7th Cir. 1992) ("'Probable cause requires more than bare suspicion but need not be based on evidence sufficient to support a conviction, nor even a showing that the officer's belief is more likely true than false.'") (quoting Brinegar v. United States, 338 U.S. 160, 175, 93 L. Ed. 1879, 69 S. Ct. 1302 (1949)); United States v. Cruz, 834 F.2d 47, 50 (2d Cir. 1987) ("In order to establish probable cause, it is not necessary to make a prima facie showing of criminal activity or to demonstrate that it is more probable than not that a crime has been or is being committed.") (internal quotation marks and citation omitted)).

[184] *Bethea*, 61 M.J. at 188.

[185] *Id.*

[186] In this regard, the CAAF mirrors the Supreme Court's repeated pronouncements most recently articulated in a different context in *Devenpeck v. Alford*, 543 U.S. 146 (2005), that probable cause is to be evaluated based on objective factors at the time of arrest.

[187] 452 U.S. 692 (1981).

[188] 125 S. Ct. 1465 (2005).

[189] In its October 2004 Term, the Supreme Court reversed or vacated every Fourth Amendment case that came out of the Ninth Circuit. *See, e.g.*, *Devenpeck*, 543 U.S. 146 (holding that when evaluating probable cause to arrest, the touchstone is whether the facts, viewed objectively, support probable cause to arrest regardless of whether the arresting officer specifically articulates the offense at the time of arrest); *Mena*, 125 S. Ct. 1465 (vacating the Ninth

Police Officers Darin Muehler and Robert Brill obtained a broad search warrant to search a residence for weapons and evidence of gang activity.[190] They had probable cause to believe one member of the gang "West Side Locos" lived at the residence.[191] Due to the possibility that the search of the residence may involve contact with suspected armed gang members, Officers Muehler and Brill requested a Special Weapons and Tactics (SWAT) team to help secure the residence prior to the search.[192] Officer Muehler, Officer Brill, and the SWAT team executed the warrant at 0700 on 3 February 1998. Officers handcuffed, at gunpoint, Ms. Mena and three other individuals who were on the property.[193] During the search, which lasted two to three hours, the four detainees were placed in a converted garage.[194] In addition to requesting the SWAT team, Officers Muehler and Brill had contacted the Immigration and Naturalization Service (INS) because of the reasonable likelihood that the "West Side Locos" had illegal immigrants as gang members.[195] An INS officer accompanied the police officers and asked all the handcuffed detainees about their immigration status.[196]

Ms. Mena sued Officers Muehler and Brill under 42 U.S.C. § 1983 alleging that her detention in handcuffs was "for an unreasonable time and [conducted] in an unreasonable manner" in violation of her Fourth Amendment rights.[197] The district court found in her favor and awarded Ms. Mena $60,000.00.[198] The Ninth Circuit affirmed the judgment concluding that it was objectively unreasonable under the Fourth Amendment to keep Ms. Mena handcuffed during the search.[199] The Ninth Circuit held that the officers should have released Ms. Mena as soon as they ascertained that she posed no threat.[200] Additionally, the Ninth Circuit concluded that the questioning of Ms. Mena regarding her immigration status, "constituted an independent Fourth Amendment violation."[201] Finally, the court concluded that Officers Meuhler and Brill were not entitled to qualified immunity because Ms. Mena's Fourth Amendment rights were clearly established at the time of her detention.[202]

The Supreme Court vacated the Ninth Circuit's opinion and remanded the case.[203] The Court held that under the circumstances of this case, the detention of Ms. Mena in handcuffs during the search was reasonable.[204] The fact that the police had to detain and guard multiple persons made the detention all the more reasonable.[205] Because Ms. Mena's detention was reasonable, the questioning by the INS officers did not constitute an additional seizure since the detention was

---

Circuit decision and holding that a two to three hour detention in handcuffs was plainly permissible under *Michigan v. Summers*, 452 U.S. 692 (1981), which held that officers executing a warrant have authority to detain occupants on the premise during search); Brosseau v. Haugen, 543 U.S. 194 (2004) (reversing the Ninth Circuit and holding that Officer Brosseau, in shooting Mr. Haugen in the back, was nevertheless entitled to qualified immunity because her action did not violate "clearly established" law).

[190] *Mena*, 125 S. Ct. at 1468.

[191] *Id.*

[192] *Id*.

[193] *Id.* Ms. Iris Mena was the only person in the house. *Id.* at 1475. The other three (a fifty-five-year-old Latina female, a forty-year-old Latino male, and a white male in his thirties) were found in trailers located in the back yard of the property. *Id.*

[194] *Id.* at 1471.

[195] *Id.* at 1468.

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] *Id.*

[200] *Id.*

[201] *Id.*

[202] *Id.*

[203] *Id.* at 1469. The late Chief Justice William Rehnquist wrote the majority opinion for the five-Justice majority. Justice Anthony Kennedy concurred in the opinion of the Court, but added the observation that it is important to mention that the opinion should not stand for the proposition that handcuffing should become a routine matter while conducting a search. Four Justices concurred in the judgment, but believed the proper course of action would be to remand the case to the Ninth Circuit in order to have that court consider Ms. Mena's additional claim that her detention in handcuffs was, in fact, extended beyond the time that the police finished their search. Id. at 1472-73. The majority of the Court declined to address the issue because the Ninth Circuit did not consider it. Id. at 1472

[204] *Id.* at 1471.

[205] *Id.*

not prolonged by the questioning.[206] Citing *Florida v. Bostick*,[207] the Supreme Court made it clear that "mere police questioning does not constitute a seizure" even if the police have no basis to suspect the individual of a crime.[208] Because the questioning of Ms. Mena did not prolong her detention, there was no additional seizure.[209]

Part III: Looking Ahead for 2006

Search and seizure jurisprudence during the Supreme Court's October 2004 Term continued a refinement of the established principle that when dealing with the Fourth Amendment the applicable touchstone is objective in nature. The Court also struck down the Ninth Circuit when it tried to step outside established Fourth Amendment precedent.[210] The Court's October 2005 Term, however, promises to break new ground by addressing significant splits among the judicial circuits: one case tests the limits of the consent exception to the Fourth Amendment and another will explore the inevitable discovery doctrine exception to the exclusionary rule.

The first Fourth Amendment case from the October 2005 Term in which the Supreme Court granted certiorari was *Georgia v. Randolph*.[211] This case involves a narrowly framed legal issue that seeks to define further the scope of consent by co-tenants.[212] Mr. and Mrs. Randolph were having marital problems and had been separated for about two months prior to the incident that formed the basis for Mr. Randolph's interlocutory appeal.[213] She had taken their son to Canada.[214] While visiting Mr. Randolph in July of 2001, Mrs. Randolph reported a domestic disturbance.[215] The police arrived outside the Randolph residence and found a distraught Mrs. Randolph.[216] She accused Mr. Randolph of kidnapping their child and using "large amounts of cocaine."[217] Shortly thereafter, Mr. Randolph arrived on the scene without the child.[218] Mr. Randolph explained to the police that he had placed the child in the custody of a neighbor because he was concerned that Mrs. Randolph would leave the country with the child.[219] Sergeant Brett Murray confronted Mr. Randolph about his wife's allegations of cocaine use and asked to search his residence.[220] Mr. Randolph refused consent.[221] The police then asked Mrs. Randolph whether she would consent to the search of the house.[222] She responded "yes" and took the police to Mr.

---

[206] *Id.*

[207] 501 U.S. 429 (1991)

[208] *Mena*, 125 S. Ct. at 1471 (quoting *Bostick*, 501 U.S. at 434 ("[e]ven when officers have no basis for suspecting a particular individual, they may generally ask questions of that individual; ask to examine the individual's identification; and request consent to search his or her luggage")).

[209] *Id.* at 1471. The Court cited to *Illinois v. Caballes*, 125 S. Ct. 834 (2005) for the proposition that so long as the initial detention was otherwise lawful and the questioning did not extend the time that Ms. Mena was detained, no additional Fourth Amendment justification was required. *Id*. at 1471-72.

[210] *See, e.g.*, Devenpeck v. Alford, 543 U.S. 146 (2005) (reversing the Ninth Circuit's holding that because Sergeant Devenpeck's arrest for an unarticulated offense was not "closely related" to the one actually articulated, Sgt Devenpeck violated Mr. Alford's civil right under the Fourth Amendment); Muehler v. Mena, 125 S. Ct. 1465 (2005) (reversing the Ninth Circuit's holding that the police violated Ms. Mena's civil rights by detaining her in handcuffs for two to three hours while they searched the residence and also reversing holding of the Ninth Circuit that the questioning of her by an INS Agent while she was handcuffed constituted an independent constitutional violation of her Fourth Amendment rights).

[211] 125 S. Ct. 1840 (2005).

[212] Specifically, the question presented before the Supreme Court is as follows: "Should this Court grant certiorari to resolve the conflict among federal and state courts on whether an occupant may give law enforcement valid consent to search the common areas of the premises shared with another, even though the other occupant is present and objects to the search?" To access the actual question or questions presented, consult the U.S. Supreme Court's official website. *See* U.S. Supreme Court, 04-1067, Georgia v. Randolph, http://www.supremecourtus.gov/qp/04-01067qp.pdf (listing the question presented).

[213] Randolph v. Georgia, 590 S.E. 2d 834, 836 (Ga. Ct. App. 2003).

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] *Id.*

[218] *Id.*

[219] *Id.*

[220] *Id*.

[221] *Id*.

[222] *Id.*

Randolph's bedroom where Officer Murray observed a cut straw with cocaine residue.[223] Officer Murray then called back to the district attorney's office and was told to stop the search and obtain a warrant.[224] The ensuing search of the Randolph residence uncovered "numerous drug related items." Mr. Randolph was indicted for possession of cocaine.[225]

At trial, Mr. Randolph moved to suppress the cocaine, claiming the initial search that uncovered the cocaine residue violated his Fourth Amendment rights.[226] The trial court denied the motion and Mr. Randolph filed an interlocutory appeal with the Court of Appeals of Georgia.[227] The Georgia Court of Appeals reversed.[228] The State petitioned the Georgia Supreme Court, which affirmed the holding of the Georgia Court of Appeals.[229] The Georgia Supreme Court agreed with the appellate court that consent by one occupant is not valid in the face of another occupant who is physically present at the scene and objects to the search.[230] Based on a conflict among state and federal circuits as to this issue, the Supreme Court granted certiorari.[231]

In addition to *Randolph*, the Supreme Court will consider whether the exclusionary rule should apply in the event that a search is conducted in an unreasonable manner. In *Michigan v. Hudson*,[232] the Supreme Court will determine whether to apply the exclusionary rule for a violation of a "knock and announce" warrant.[233]

On 27 August 1998, officers from the Detroit Police Department executed a "knock and announce" warrant for Mr. Booker T. Hudson's residence.[234] Although some of the officers shouted "police, search warrant" prior to entering the residence, none of the officers knocked.[235] Instead, they waited three to five seconds to enter Mr. Hudson's house.[236] The prosecutor conceded that the police violated the "knock and announce" requirement of the search warrant.[237] The trial court suppressed the evidence found during the search.[238] The State of Michigan appealed to the Michigan Court of Appeals arguing that the holding in *People v. Stevens*[239] should control. In *Stevens*, the Michigan Supreme Court held that a "knock

---

[223] *Id*.

[224] *Id.*

[225] *Id.*

[226] *Id*.

[227] *Id.*

[228] *Id*. at 840.

[229] State v. Randolph, 604 S.E.2d 835 (Ga. 2004).

[230] *Id*. at 836. The NMCCA had occasion to rule on a very similar issue as an issue of first impression in the military in *United States v. Garcia*, 57 M.J. 716, 720 (N-M. Ct. Crim. App. 2002). Based on the majority of the circuits, the NMCCA held that an *absent* co-tenant can consent if the *present* co-tenant objects. The *Garcia* case was set aside by the CAAF on other grounds. *See* United States v. Garcia, 59 M.J. 447 (2004) (setting aside conviction on ineffective assistance of counsel grounds).

[231] Subsequent to the submission of this article, but prior to its publication, the Supreme Court handed down its decision in *Randolph v. Georgia*, 126 S.Ct. 413 (2006). In a five-to-three opinion, the majority affirmed the opinion of the Georgia Supreme Court and held on narrow grounds that when a *physically present* co-occupant refuses to give consent, the consent granted by the other co-occupant is legally invalid.

[232] 125 S. Ct. 2964 (2005). To access the text of the actual question presented that the Supreme Court granted for its October 2005 Term, see U.S. Supreme Court, 04-1360, Booker T. Hudon v. Michigan, http://www.supremecourtus.gov/qp/04-01360qp.pdf.

[233] *See* Wilson v. Arkansas, 514 U.S. 385 (1995) (holding that the Fourth Amendment requires law enforcement officials executing a warrant to knock on the door and announce their presence prior to making any forcible entry); *see also* Richards v. Wisconsin, 520 U.S. 385, 387 (1997) (explaining the holding in *Wilson* and rejecting a blanket exception to the knock-and-announce requirement for felony drug cases). In *United States v. Banks*, 540 U.S. 31 (2003), the Supreme Court explained that each knock-and-announce requirement is subject to a reasonableness test depending on the facts of each case. In *Banks*, the Court concluded that after knocking and announcing, the police were justified in waiting only fifteen to twenty seconds prior to breaking down the door because the apartment was small and the search warrant was for cocaine, a substance easily disposable.

[234] Because the prior appellate history of the *Hudson* case is largely unpublished, the limited facts cited here are taken from the Brief of the United States as Amicus Curiae Supporting Respondent (Michigan). Brief for the United States as Amicus Curiae Supporting Respondent, Michigan v. Hudson, 125 S. Ct. 2964 (2005) (No. 04-1360).

[235] *Id.* at *1.

[236] *Id*.

[237] *Id*. at *2.

[238] *Id*.

[239] 597 N.W.2d 53 (Mich. 1999)

and announce" violation is not subject to suppression because the evidence would have been inevitably discovered.[240] Based on a conflict among the state supreme courts and federal circuits that have previously considered this issue, the Supreme Court granted certiorari.[241]

While there were some refinements of established Fourth Amendment concepts in 2005, this year has largely been one of incubation in which several cases have made their way up to both the CAAF and the Supreme Court. The CAAF is poised to not only decide whether servicemembers enjoy a reasonable expectation of privacy in the content of their e-mail, but also to decide if consent can be voluntary following an unconstitutional search of a computer when the person who consents is unaware of the prior constitutional violation. Additionally, the Supreme Court will determine whether to apply the exclusionary rule where there has been a "knock-and-announce" violation. It is unclear upon what path either court will embark; however, it is clear both courts know exactly where they want to go.

---

[240] *Id*. at 55.

[241] 125 S. Ct. 2964 (2005). The specific question granted is as follows:

> [d]oes the inevitable discovery doctrine create a per se exception to the exclusionary rule for evidence seized after a Fourth Amendment "knock and announce" violation, as the Seventh Circuit and the Michigan Supreme Court have held, or is evidence subject to suppression after such violations, as the Sixth and Eighth Circuits, The Arkansas Supreme Court, and the Maryland Court of Appeals have held?

See U.S. Supreme Court, 04-1360, Booker T. Hudon v. Michigan, http://www.supreme courtus.gov/qp/04-01360qp.pdf. The case was argued on 9 January 2006.