

A Reasonable Expectation of Privacy: Is a Government E-mail Account the Equivalent of a Wall Locker in a Barracks Room?

Major Lawrence A. Edell*

*Illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.*¹

I. Introduction

The current Army computer-monitoring policy fails to overcome the reasonable expectation of privacy established by *United States v. Long (Long II)*² because it encourages personal use of electronic mail (e-mail), recognizes privilege in these communications, and is designed with the primary purpose of gathering information for law enforcement use.³ E-mail has become an increasingly important part of modern society and has attained the status of the telephone and traditional mail.⁴ The Army has recognized the importance of e-mail. Soldiers use government e-mail for official purposes and for personal communications.⁵ Since the decision in *Long II*, the Army has reshaped its policy on computer monitoring to act as a tool for evidence collection against individuals using a government computer network.⁶ This creates Fourth Amendment issues that did not exist under prior Army computer network monitoring policies.⁷

The use of e-mail has become commonplace in today's military and many units use it to accomplish their daily communications.⁸ As the use of e-mail and computers expands in the Army, there is a need to ensure that government computer networks continue to operate properly and adequately safeguard operational information.⁹ This will create an inherent tension between the desire to protect the network and the privacy concerns of Soldiers who use the network for personal use. The Court of Appeals for the Armed Forces (CAAF) has provided some guidance on this issue.

* Judge Advocate, U.S. Army. Currently assigned as Group Judge Advocate, 3d Special Forces Group (Airborne), Fort Bragg, N.C. LL.M., 2008, The Judge Advocate General's School, U.S. Army, Charlottesville, Va.; J.D., 2002, University of Georgia; B.S., 1996, U.S. Naval Academy. Previous assignments include Chief of Justice, U.S. Army Transportation Ctr. & Sch. (USATC&S), Fort Eustis, Va., 2006–2007; Administrative Law Attorney, USATC&S, Fort Eustis, Va., 2005–2006; Trial Counsel, 3d Brigade Combat Team (BCT), 1st Cavalry Division, Fort Hood, Tex., 2003–2005; Chief of Legal Assistance, 2003, 1st Cavalry Division, Fort Hood, Tex. Member of the bars of Georgia and the Court of Appeals for the Armed Forces. This article was submitted in partial completion of the Master of Laws requirements of the 56th Judge Advocate Officer Graduate Course.

¹ *Boyd v. United States*, 116 U.S. 616, 635 (1886).

² 64 M.J. 57 (C.A.A.F. 2006).

³ This article is limited to discussion of e-mail recovered from a government server on behalf of law enforcement from an unclassified computer network. Information transmitted over a classified network is beyond the scope of this article. This article will focus on Army policy and regulations. See U.S. DEP'T OF ARMY, REG. 25-1, ARMY KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY (15 July 2006) [hereinafter AR 25-1]; U.S. DEP'T OF ARMY, REG. 25-2, INFORMATION ASSURANCE (24 Oct. 2007) [hereinafter AR 25-2]; U.S. DEP'T OF ARMY, REG. 380-53, INFORMATION SYSTEMS SECURITY MONITORING (29 Apr. 1998) [hereinafter AR 380-53]; *infra* App. A for a brief overview of the delivery of e-mail messages.

⁴ See Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 447–48 (2007).

⁵ See AR 25-1, *supra* note 3, para. 1–10 (authorizing Soldiers to use their government e-mail accounts for personal use).

⁶ See also Memorandum from Assistant Sec'y of Def. (Command, Control, Communication, and Intelligence), to Secretaries of the Military Dep'ts et al., subject: Policy on Department of Defense Electronic Notice and Consent Banner (16 Jan. 1998) [hereinafter ASoD (C4I) Memo] (on file with author); Memorandum from Forces Command (FORSCOM) Staff Judge Advocate, to FORSCOM G6, subject: FORSCOM Log-On Banner (18 Jan. 2007) [hereinafter FORSCOM Memo] (on file with author). Compare AR 25-2, *supra* note 3, with U.S. DEP'T OF ARMY, REG. 25-2, INFORMATION ASSURANCE (14 Nov. 2003) [hereinafter AR 25-2 (2003)].

⁷ U.S. CONST. amend. IV. The previous Army computer monitoring policy specifically stated that computer users had a reasonable expectation of privacy. AR 25-2 (2003), *supra* note 6, para. 4-5r.

⁸ See AR 25-1, *supra* note 3, para. 1–11.

⁹ See generally AR 25-2, *supra* note 3; AR 380-53, *supra* note 3; U.S. DEP'T OF DEFENSE, MANUAL 8570.01-M, INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM (19 Dec. 2005) (explaining why there is a need to monitor government computer systems from both internal and external threats).

In 2000, the CAAF held in *United States v. Monroe* that a Soldier does not have a reasonable expectation of privacy in e-mails sent over a government network from monitoring by a system administrator.¹⁰ In 2006, the CAAF answered a question left unanswered by *United States v. Monroe*: Is there a reasonable expectation of privacy in the content of e-mail sent from a government server vis-à-vis law enforcement?

Long II may be the most important case decided by the CAAF during the 2006 court term because of its effects outside the legal community.¹¹ In *Long II*, the CAAF determined that Lance Corporal (LCpl) Long had a reasonable expectation of privacy in her government e-mail account against a search conducted on behalf of law enforcement.¹² The decision in *Long II* has created concerns at the highest levels of Department of Defense (DOD) regarding the ability to monitor its computer networks and has resulted in new warning banners and changes in regulations concerning the monitoring of computer networks.¹³ Arguably, *Long II* is limited to a very specific set of facts,¹⁴ but revised Army and DOD policies have unsuccessfully attempted to undermine its holding. The new policies may inadvertently create an unconstitutional monitoring scheme despite legitimate reasons to monitor government computer networks. This article discusses how the Fourth Amendment adapts to technology, the legitimate reasons to monitor computer networks, the CAAF's previous rulings on computer privacy, and current Army policy on monitoring e-mail. This article concludes by recommending that law enforcement agents obtain a search authorization before searching government servers, despite the current Army policy that attempts to circumvent that requirement.

II. Why are Government Computer Networks Monitored?

Legitimate societal reasons argue for law enforcement monitoring of the Internet.¹⁵ The Internet has provided a platform for the spread of several illicit activities.¹⁶ Crimes such as identity theft, fraud, cyber stalking, and distribution of child pornography occur directly on the Internet.¹⁷ The involvement of law enforcement in systems monitoring inherently implicates the Fourth Amendment. However, others have reasons to monitor the use of the Internet as well.

Employers who provide Internet and e-mail access to their employees have a multitude of reasons to monitor employees' usage.¹⁸ First, it helps document and observe employee activities.¹⁹ It can gauge productivity by viewing an employees' use of the Internet and e-mail for matters not related to work.²⁰ Second, it ensures those employees were working at their assigned tasks.²¹ Third, it can ensure that trade secrets or proprietary information are not being improperly disseminated.²² Finally, employers are liable for employees' actions related to the inappropriate use of e-mail.²³ As an employer, the government has an interest in monitoring its employees' use of the Internet and e-mail.

¹⁰ 52 M.J. 326 (C.A.A.F. 2000).

¹¹ Lieutenant Colonel M.K. Jamison, U.S. Marine Corps, *New Developments in Search and Seizure Law*, ARMY LAW., Apr. 2006, at 9, 13.

¹² *Long II*, 64 M.J. 57 (C.A.A.F. 2006).

¹³ ASoD (C4I) Memo, *supra* note 6; FORSCOM Memo, *supra* note 6; *Long II*, 64 M.J. at 58 (certifying the Navy Judge Advocate General's issues); Interview with Major Kevin Harris, U.S. Marine Corps, Judge Advocate, in Charlottesville, Va. (Nov. 26, 2007) [hereinafter Harris Interview]. Major Harris was the Appellate Government Counsel for *Long II*, 64 M.J. 57, and *United States v. Long (Long I)*, 61 M.J. 539, 540 (N-M. Ct. Crim. App. 2005). *Id.*

¹⁴ Lieutenant Colonel Stephen R. Stewart, U.S. Marine Corps, *Katy Bar the Door—2006 New Developments in Fourth Amendment Search and Seizure Law*, ARMY LAW., June 2007, at 1, 12.

¹⁵ *See id.*; Lieutenant Colonel Joginder S. Dhillon & Lieutenant Colonel Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques*, 50 A.F. L. REV. 135, 159 (2001).

¹⁶ U.S. DEP'T OF JUSTICE, SEARCH AND SEIZURE MANUAL, SEARCHING AND SEIZING COMPUTERS AND OBTAINING EVIDENCE IN CRIMINAL INVESTIGATIONS intro. (2002) [hereinafter SSCOECI MANUAL] (Computer Crime and Intellectual Property Section); U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES ch. I (Feb. 2007) (Computer Crime and Intellectual Property Section).

¹⁷ SSCOECI MANUAL, *supra* note 16, intro.

¹⁸ *See Smythe v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (holding that companies have a vital interest in monitoring their employees' e-mail messages); Myrna Wigod, *Privacy in Public and Private E-Mail and Online Systems*, 19 PACE L. REV. 95, 97 (Fall 1998).

¹⁹ Wigod, *supra* note 18, at 97.

²⁰ *Id.* at 97–98.

²¹ *Id.* at 98–99.

²² *Id.* at 99.

²³ *Id.* at 98 (preventing the use of e-mail to commit sexual harassment, libel, copyright infringement, and hate crimes).

The government has additional reasons for monitoring the use of the Internet and e-mail by its employees. The first and most important reason is to protect national security.²⁴ Government computer systems are critical to the national defense.²⁵ Attacks against government networks could arise either from inside or outside of the network.²⁶ The government also has a proprietary interest.²⁷ “Employees shall protect and conserve federal property and shall not use it for other than authorized activities.”²⁸ Finally, the Supreme Court recognized the special nature of the military society and its requirement for discipline.²⁹ Society holds the military to a higher standard of conduct and this provides for a substantial government interest in monitoring a Soldier’s conduct in cyberspace “when accessing the Internet through a government computer system.”³⁰ The Army has recognized the need to monitor its computer networks.³¹

The Army has three monitoring requirements to ensure proper use of government computer systems. First, monitoring ensures that operational security of systems networks is not vulnerable to disclosure of classified material or attacks by outside sources.³² Second, monitoring serves a law enforcement purpose.³³ Through means such as an intercept or pen register,³⁴ law enforcement agents determine if the communication is evidence of a crime.³⁵ Finally, monitoring ensures that the network is operating properly, prevents the misuse of resources, and verifies that only authorized users have access to government computer networks.³⁶ Known as systems protection monitoring,³⁷ this task is performed by system administrators.³⁸ They are not law enforcement agents, but are often the ones who discover evidence of criminal conduct.³⁹ So, when does monitoring of a government computer system become a search under the Fourth Amendment?

III. What Triggers a Search Under the Fourth Amendment?

The Fourth Amendment protects against unreasonable searches and seizures conducted by government agents.⁴⁰ One must first determine if the government conducted the search or seizure before determining if the Fourth Amendment protects an individual.⁴¹

²⁴ Lieutenant Colonel LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See*, 46 A.F. L. REV. 155, 156–57, 157 n.6 (1999) (quoting Lieutenant General William Donahue, *Special Month Focuses on Cyber Responsibilities*, A.F. MIL. NEWS (23 Jan. 1999)).

²⁵ *Id.*; WALTER G. SHARP, SR., *CYBERSPACE AND THE USE OF FORCE* 23 (1999) (citing Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 17, 1996)).

²⁶ See SHARP, *supra* note 25, at 20–22; John C. Dolak & Anna E. Dolak, *Information Systems Security and Privacy Issues in the Armed Forces*, 8 COMP. L. REV. & TECH. J. 1, 2–4 (Fall 2003) (citing numerous attacks on DOD computer systems).

²⁷ U.S. DEP’T OF DEFENSE, DIR. 5500.7R, JOINT ETHICS REGULATION § 2–301 (C6, 29 Nov. 2007) [hereinafter JER].

²⁸ Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.101(b)(9) (2001). Public confidence in the military is important and ensuring that government resources are used properly is part of this confidence. Lieutenant Commander R. A. Conrad, *Searching for Privacy in All the Wrong Places: Using Government Computers to Surf Online*, 48 NAV. L. REV. 1, 23 (2001).

²⁹ See generally *Parker v. Levy*, 417 U.S. 733 (1974).

³⁰ Conrad, *supra* note 28, at 14–15.

³¹ See generally AR 25-1, *supra* note 3; AR 25-2, *supra* note 3; AR 380-53, *supra* note 3.

³² Coacher, *supra* note 24, at 155–56; see AR 380-53, *supra* note 3.

³³ Coacher, *supra* note 24, at 156; see U.S. DEP’T OF ARMY, REG. 190-53, INTERCEPTION OF ORAL AND WIRE COMMUNICATIONS FOR LAW ENFORCEMENT PURPOSES (3 Nov. 1986) [hereinafter AR 190-53].

³⁴ A pen register is a device that can determine the destination (address or phone number) of a call or e-mail, but cannot determine the content of the transmission. See SSCOECI MANUAL, *supra* note 16, at IV.C.

³⁵ Coacher, *supra* note 24, at 156; AR 190-53, *supra* note 33, para. 1-1.

³⁶ Coacher, *supra* note 24, at 156–57.

³⁷ *Id.* at 168.

³⁸ AR 25-2, *supra* note 3, para. 3-3.

³⁹ See *United States v. Monroe*, 52 M.J. 326 (C.A.A.F. 2000); SSCOECI MANUAL, *supra* note 17, at I.D.

⁴⁰ See *Rakas v. Illinois*, 439 U.S. 128, 140–49 (1978) (holding that a person must have a legitimate property interest in the area or item searched by a government agent for the Fourth Amendment to apply); see also *United States v. Portt*, 21 M.J. 333 (C.M.A. 1986) (holding that the initial entry was not a governmental intrusion because the Airmen were not acting in their capacity as Security Forces); *United States v. Hodges*, 27 M.J. 754 (A.F.C.M.R. 1988) (holding that the search by the employee of a public freight company was not a search protected under the Fourth Amendment).

⁴¹ See *Portt*, 21 M.J. 333; see also *Hoffa v. United States*, 385 U.S. 293, 302 (1967) (holding that an informant’s disclosure of a private conversation does not invoke Fourth Amendment protection).

The Supreme Court has considered the issue of whether a law enforcement agent or a private actor conducted a search. In *United States v. Jacobsen*,⁴² employees of Federal Express (FedEx), a private company, opened the defendant's package to determine if they damaged its contents during shipment.⁴³ The employees believed the package contained cocaine after inspecting it and contacted the Drug Enforcement Agency (DEA).⁴⁴ The Court held that the search of the defendant's package by the FedEx employees did not violate his Fourth Amendment rights because the actions of the employees were clearly of a private character.⁴⁵ The Court also held that the DEA's subsequent action was not a search as long as it did not exceed the scope of the FedEx employees' search.⁴⁶

The CAAF has applied *Jacobsen*⁴⁷ to the military.⁴⁸ In *United States v. Reister*,⁴⁹ the CAAF held that the warrantless search of the appellant's apartment by Naval Criminal Investigative Service subsequent to discovery of the evidence by the victim, a Sailor (a government employee), did not violate the Fourth Amendment.⁵⁰ The court determined that "the exclusionary rules were not triggered by any private invasion of appellant's privacy."⁵¹ The victim, the appellant's girlfriend, had access to appellant's apartment.⁵² Using the key the appellant provided her, the victim entered the appellant's apartment and discovered the evidence while looking around his apartment.⁵³ In the military, the focus should be on the capacity of the person who discovered the evidence at the time of the search, not the subsequent actions of the Soldier or his duty position.⁵⁴ Only a search by a government agent or employee while acting in a law enforcement capacity implicates the Fourth Amendment.

If a government search occurred, Justice Harlan's concurring opinion in *Katz v. United States*⁵⁵ provides the framework for analyzing whether a person has a reasonable expectation of privacy. First, the person must have exhibited an actual expectation of privacy.⁵⁶ This requires the court to determine if the person had a subjective belief that he had a reasonable expectation of privacy. The second part requires the expectation of privacy be one that society is prepared to recognize as reasonable.⁵⁷ The objective test looks at the competing values of society and the original intent of the framers of the Fourth Amendment.⁵⁸

⁴² 466 U.S. 109 (1984).

⁴³ *Id.* at 111. A post-trial affidavit indicated that the employee opened the package because he thought it might contain contraband, not to determine if damage occurred to the contents of the tube. *Id.* at 115 n.10.

⁴⁴ *Id.* at 111.

⁴⁵ *Id.* at 115; *cf.* *United States v. Sims*, 2001 U.S. Dist. LEXIS 25819 (D.N.M. 2001) (holding that when law enforcement directs an employer to conduct a search of an employee's computer, it is a search under the Fourth Amendment).

⁴⁶ *Jacobsen*, 466 U.S. at 120–22.

⁴⁷ *Id.* at 109.

⁴⁸ *See generally* *United States v. Reister*, 44 M.J. 409 (C.A.A.F. 1996) (holding that a warrantless search by law enforcement did not violate the Fourth Amendment because the scope of the search did not exceed the scope of intrusion by a private actor); *United States v. Hahn*, 44 M.J. 360 (C.A.A.F. 1996) (holding that law enforcement's observation of stolen property is not a search or seizure if law enforcement were permitted to be at the location where the contraband was discovered); *United States v. Visser*, 40 M.J. 86 (C.M.A. 1994) (holding that a private moving company's decision to delay transporting appellant's property at the request of law enforcement is not a search); *United States v. Bruci*, 52 M.J. 750 (N-M. Ct. Crim. App. 2000).

⁴⁹ *Reister*, 44 M.J. 409.

⁵⁰ *Id.* at 416.

⁵¹ *Id.*

⁵² *Id.* at 411–12.

⁵³ *Id.*

⁵⁴ *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 311(a) (2008) [hereinafter MCM]; *see also* *United States v. Portt*, 21 M.J. 333 (C.M.A. 1986) (holding that the actions of Air Force Security Police acting in their private capacity is not a search).

⁵⁵ 389 U.S. 347, 360–63 (1967) (Harlan, J., concurring).

⁵⁶ *Id.* at 361 (Harlan, J., concurring).

⁵⁷ *Id.*

⁵⁸ *Rakas v. Illinois*, 439 U.S. 128, 153 (1973).

IV. The Fourth Amendment Adopts to Technology

The number of Internet users has vastly increased in the past twenty years⁵⁹ and e-mail has replaced traditional means of communication for both personal and professional considerations.⁶⁰ In comparing the current use of electronic communications to the use of the telephone at the time of *Katz v. United States*,⁶¹ a modern court should find them “as crucial as the public telephone of 1967.”⁶² Most users of e-mail simply assume that they have the same amounts of privacy in e-mail as they do in regular mail, which enjoys a longstanding societal expectation of privacy.⁶³ However, federal courts⁶⁴ have not recognized a reasonable expectation of privacy for e-mail recovered from an Internet service provider’s (ISP’s) server.⁶⁵ The Supreme Court has not ruled on this issue.⁶⁶ However, as a new form of technology develops and society accepts it, courts eventually recognize a reasonable expectation of privacy.⁶⁷ With this in mind, Americans are using e-mail for every facet of their lives.

E-mail and Internet use are increasing as more citizens, businesses, and government entities rely upon electronic communications for their needs. Only 8% of American households had a computer in 1984.⁶⁸ However, in less than thirty years, that number has skyrocketed to nearly 62%.⁶⁹ There are approximately thirty-five billion e-mail messages sent every day.⁷⁰ Numerous financial institutions offer their customers the ability to receive their banking documents via e-mail and to check their bank accounts on the World Wide Web.⁷¹ Even state governments have begun to process administrative tasks for their residents on the Internet and by e-mail.⁷² The Army is likewise more connected.

⁵⁹ See JENNIFER CHEESEMAN DAY ET AL., COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003, at 1, fig.1 (2005), available at <http://www.census.gov/prod/2005pubs/p23-208.pdf>; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1575 (2004) (“Approximately 102 million U.S. individuals use e-mail, with about 60 million using it on any given day. Fifty-two million US individuals have used instant messaging, with over 10 million using it on a typical day.”).

⁶⁰ Conrad, *supra* note 28, at 41–42.

⁶¹ 389 U.S. 347, 351 (1967).

⁶² Susan Freiwald, *First Principles in Communications Privacy*, 2007 STAN. TECH. L. REV. 3, para. 32 (2007).

⁶³ Randolph S. Sergeant, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1226 (1995).

⁶⁴ U.S. CONST. art. III, § 1.

⁶⁵ Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored E-mail: The Law Professor’s Brief in Warshak v. United States*, 41 U.S.F. L. REV. 559, 565 (Spring 2007). Courts have not favored finding a reasonable expectation of privacy in e-mail either intercepted during transmission or retrieved from an ISP’s server. *Id.* Justice Harlan’s test, derived from *Katz v. United States*, expands the Fourth Amendment to searches that do not involve a physical trespass. Scott A. Sundstrom, *You’ve Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2070 (1998) (citing *Katz*, 389 U.S. at 361). The search of e-mail from an Internet service provider’s (ISP) server is one such search.

⁶⁶ *Id.* Justice Stevens has argued that the Supreme Court should allow Congress to tackle the issue of balancing privacy concerns with technological advancements. See *Kyllo v. United States*, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting). Arguably, the Supreme Court (or at least Justice Stevens) is not inclined to tackle this issue.

⁶⁷ See Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 563 (1998) (arguing that American law looks to history for answer and has trouble with technological advances, but that societal expectations of privacy help drive the change).

⁶⁸ DAY ET AL., *supra* note 59.

⁶⁹ *Id.* Households earning over \$100,000 are more likely to have a computer and Internet access, but all economic classes have a significant percentage of users. *Id.* Households earning over \$100,000 reported that 92.2% have Internet connection in their homes, while those earning less than \$24,999 reported that 30.7% have an Internet connection. *Id.*

⁷⁰ See Craig Rhinehart, *Email Management and Sarbanes-Oxley Compliance*, SARBANES-OXLEY COMPLIANCE J., June 8, 2006, <http://www.s-ox.com/feature/article.cfm?articleID=913>. In comparison, the U.S. Post Office delivered 213,138 million pieces of traditional mail in 2006. See U.S. POSTAL SERV., UNITED STATES POSTAL SERVICE ANNUAL REPORT 2006, available at http://www.usps.com/financials/_pdf/anrpt2006_final.pdf.

⁷¹ See U.S. Automobile Ass’n, www.usaa.com (last visited Oct. 9, 2008); Pentagon Federal Credit Union, www.penfed.org (last visited Oct. 9, 2008); Navy Federal Credit Union, www.nfcu.org (last visited Oct. 9, 2008). These three financial institutions are a small sampling of financial institutions that offer electronic banking services.

⁷² In Texas, a resident may renew his vehicle registration or driver’s license on the Internet. See Tex. Dep’t of Motor Vehicles, <http://rts.texasonline.state.tx.us> (last visited Oct. 9, 2008). The Texan must provide basic information and a credit card number to renew his driver’s license or vehicle registration. *Id.* The Texas Department of Motor Vehicles will then send an e-mail to the user confirming receipt of payment for proof of compliance until the vehicle registration or driver’s license arrives in the mail. *Id.*

The Army provides its Soldiers, retirees, civilian employees, and even family members e-mail accounts.⁷³ Army Knowledge Online (AKO) provides information to Soldiers and other eligible families. It also allows Soldiers to keep in touch with other Soldiers and family members.⁷⁴ Army Knowledge Online has provided the Soldier with a tool to keep himself informed of his professional status and obligations, while it also provides a readily accessible e-mail account for personal use whenever the Internet is available.⁷⁵

Although AKO is an official DOD website, it has services that allow a Soldier to send video messages to his family while deployed.⁷⁶ For a Soldier in a deployed environment, AKO may be the only method available to communicate with his family and friends.⁷⁷ The Soldier, unlike an employee in the United States, often does not have the option to use a private computer network.⁷⁸ The unique position of Soldiers further reinforces the need to respect the privacy of e-mail messages sent over a government network. The growing use of e-mail and the unique privacy concerns of Soldiers require the recognition of a reasonable expectation of privacy in e-mail. The Supreme Court has recognized this concept for other means of communication as they gained acceptance in society.⁷⁹

As previously noted, when new technology becomes more prevalent in society, courts begin to recognize a reasonable expectation of privacy in the new technology.⁸⁰ In 1928, the Supreme Court did not extend the Fourth Amendment to warrantless wiretapping of telephones.⁸¹ The Supreme Court's rejection of *Olmstead v. United States*⁸² demonstrates how the

⁷³ See Army Knowledge Online (AKO), How Do I Register for an AKO/DKO Account?, <https://help.us.army.mil/cgi-bin/akohd.cfg/php/enduser/home.php> (follow "Find Answers" hyperlink; then follow "How do I register for an AKO/DKO account?" hyperlink) (last visited Oct. 9, 2008) [hereinafter AKO]. The exhaustive list of those authorized access to a U.S. Army e-mail account is contained on this page. *Id.*

⁷⁴ See Army Knowledge Online (AKO), <https://www.us.army.mil> (follow "White Pages" hyperlink) (last visited Oct. 9, 2008). On the main AKO page, a user can simply click on White Pages hyperlink to find another registered user's e-mail address and contact information. *Id.* To begin the search the AKO user is required to know at least the first and last name of the person whom they are trying to contact. *Id.*

⁷⁵ *Id.* The AKO site has numerous links that inform Soldiers about everything from their dental readiness status to their enlisted record brief. *Id.*

⁷⁶ *Id.* The AKO site offers the following option for its users:

This holiday season don't forget to use AKO/DKO Video Messaging to contact your loved ones that are deployed. The AKO Video Messaging System is designed to keep military families and troops stationed around the world connected using personal video messages. The program is easy-to-use, secure, and accessible through the Video icon at the top of the portal home page. All you need is a webcam and an Internet connection to send high-quality personal video messages to other AKO/DKO users.

Id. The AKO user agreement includes consent to monitoring and informs the user that evidence of unauthorized use of AKO discovered during monitoring could lead to criminal action. *Id.* The terms of service are:

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. -Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Id.

⁷⁷ This assertion is based on the author's professional experiences as the Trial Counsel, 3d BCT, 1st Cavalry Division, Fort Hood, Tex., from 1 November 2003 to 15 June 2005.

⁷⁸ See U.S. Army Information Assurance Training Ctr., Dep't of Defense Information Assurance Awareness Training, <https://ia.gordon.army.mil/dodiaa/default.asp> (last visited Oct. 9, 2008) (forbidding Soldiers from accessing commercial e-mail accounts via a government computer network).

⁷⁹ See *Berger v. New York*, 388 U.S. 41 (1967) (holding that there was a reasonable expectation of privacy in telephone conversations); *Ex parte Jackson*, 96 U.S. 727, 732-33 (1878) (holding that letters and packages sent through the U.S. Postal Service are protected from inspection by the Fourth Amendment); see also *United States v. Maxwell*, 45 M.J. 406, 416-17 (C.A.A.F. 1996) (comparing e-mail to letter and phone calls).

⁸⁰ Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 DRAKE L. REV. 239, 242 (2000).

⁸¹ *Olmstead v. United States*, 277 U.S. 438 (1928) (holding that wire taps of phone conversation did not violate the Fourth Amendment and that Congress should develop of statutory suppression remedy). It was not until 1967 that the Supreme Court applied the Fourth Amendment to wiretaps. See *Berger*, 388 U.S. 41. Congress provided the first statutory suppression remedy for secret recordings of telephone conversations. Mulligan, *supra* note 59, at 1559-60.

⁸² 277 U.S. 438.

prevalence of telephones in society created a reasonable expectation of privacy, but this took nearly forty years.⁸³ The CAAF has already recognized the importance and prevalence of e-mail in society and has had the foresight to recognize a reasonable expectation of privacy in e-mail stored on an ISP's server, but with limitations in the *Maxwell*, *Monroe*, and *Long* cases.⁸⁴

V. The CAAF Ventures into Cyberspace

A. *United States v. Maxwell*—Establishing a Reasonable Expectation of Privacy in E-Mail

United States v. Maxwell is the CAAF's first look into cyberspace.⁸⁵ The CAAF concluded that a person has a reasonable expectation of privacy in e-mail sent, stored, or received through a commercial ISP.⁸⁶ The court easily applied traditional Fourth Amendment rules to e-mail to provide Soldiers with a reasonable expectation of privacy in their e-mail communications transmitted on a personal computer via a commercial ISP.⁸⁷

Evidence gathered from a commercial ISP's server convicted Colonel (COL) Maxwell of communicating indecent language under Article 134, Uniform Code of Military Justice (UCMJ) and other charges resulting from his e-mail communications.⁸⁸ A private citizen provided the FBI and America Online (AOL), a commercial ISP, with a list of screen names of AOL subscribers who were transmitting pornography via e-mail.⁸⁹ Colonel Maxwell, an AOL subscriber, owned one of the screen names that appeared on the list provided to the FBI.⁹⁰ Eventually, the FBI received a search warrant to seize the e-mails and subscriber information of the screen names mentioned in the letter. America Online retrieved the screen name that appeared on the list and all other screen names registered to an account.⁹¹ The FBI searched all of the screen names belonging to COL Maxwell's account, despite the search warrant only authorizing the search of the screen name "Reddel."⁹² Colonel Maxwell's defense objected to the search of the screen names not listed on the search warrant.⁹³

The central issue facing the CAAF was whether there was a reasonable expectation of privacy in e-mail.⁹⁴ The CAAF analogized e-mail to both letters and phone calls.⁹⁵ The technology exists to monitor phone calls, but simply having the ability to monitor a phone call does not erase the expectation of privacy in that phone call.⁹⁶ The same is true for e-mail. The ability of the system administrators to retrieve the e-mail from the server does not erase the reasonable expectation of privacy in e-mail.⁹⁷

⁸³ Amy E. Wells, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 110 (Spring 2000).

⁸⁴ See *Maxwell*, 45 M.J. 406; *United States v. Monroe*, 52 M.J. 326 (C.A.A.F. 2000); *Long II*, 64 M.J. 57 (C.A.A.F. 2006).

⁸⁵ *Maxwell*, 45 M.J. 406; see also Major Charles N. Pede, *Driving 'Naked'; Privacy in Cyberspace; and Expansive 'Primary Purpose' Developments in Search, Seizure and Urinalysis*, ARMY LAW., May 1996, at 20, 20.

⁸⁶ *Maxwell*, 45 M.J. 406.

⁸⁷ Pede, *supra* note 85, at 20.

⁸⁸ *Maxwell*, 45 M.J. at 410.

⁸⁹ *Id.* at 413. AOL management received the list as well. *Id.* at 412.

⁹⁰ *Id.* at 411 ("These screen names are codes akin to CB handles, nicknames, and the like. . . . No two users may have the same screen name.").

⁹¹ *Id.* at 413. This resulted in the release of all four of Colonel (COL) Maxwell's screen names. *Id.* One account may have several screen names. *Id.* at 411.

⁹² *Id.* at 413–14.

⁹³ *Id.* at 414.

⁹⁴ Pede, *supra* note 85, at 21.

⁹⁵ *Maxwell*, 45 M.J. at 417–19; see Allegra Knopf, *Privacy and the Internet: Welcome to the Orwellian World*, 11 J. LAW. & PUB. POL'Y 79, 91 (Fall 1999) (concluding that an e-mail is akin to a first class letter by relying on the decision of *United States v. Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997)); Bayens, *supra* note 80, at 250–52 (concluding that e-mail is analogous to a letter or phone conversation); cf. Freiwald, *supra* note 62, paras. 15–19 (arguing that the analogy between e-mail and telephone calls is faulty because of the differences in the two mediums, but agreeing with the decision of the CAAF).

⁹⁶ *Katz v. United States*, 389 U.S. 347, 353–54 (1967). Each e-mail remains on the server of the Internet service provider of the sender and recipient. See Freiwald, *supra* note 62, para. 14. As for telephone calls, there will be a record made of the time and number dialed with the telephone company, just as with an e-mail. Mulligan, *supra* note 60, at 1562. The telephone company's switchboard does not record the content of the telephone call unlike the content of an e-mail that resides on a server. *Id.* at 1580.

⁹⁷ Mulligan, *supra* note 59, at 1580.

Electronic mail, as its name implies, consists of a message sent in an electronic envelope delivered to the recipient's electronic mailbox.⁹⁸ The e-mail sent by COL Maxwell required him to provide a password to enter AOL and the same was required for his intended recipient to retrieve the message.⁹⁹ This was not a message posted on a message board that anyone could view, but intended for one recipient.¹⁰⁰ In other words, an electronic envelope "sealed" the e-mail message COL Maxwell sent. The content of the e-mail was not viewable without opening the electronic envelope.¹⁰¹ The CAAF determined that COL Maxwell had a subjective and objective expectation of privacy with respect to the e-mail sent to another user.¹⁰²

Maxwell is important because it recognizes a reasonable expectation of privacy in e-mail, although it is limited to e-mail sent over a commercial ISP. This decision "comports comfortably with the historical development of the Fourth Amendment, expectations of privacy, and the guiding principles that it 'protects people not places.'"¹⁰³ The CAAF courageously provides Fourth Amendment protections to e-mail retrieved from an ISP's server, a step that no other court has done. However, *Maxwell* did not address whether there was a reasonable expectation of privacy in e-mail retrieved from a government server.

B. *United States v. Monroe*—No Reasonable Expectation of Privacy for Systems Monitoring

In *United States v. Monroe*, the CAAF provided useful guidance on the question left unanswered by *Maxwell*¹⁰⁴: Is there a reasonable expectation of privacy in e-mail transmitted over a government computer network?¹⁰⁵ The system administrators of an Air Force computer network in Korea found fifty-nine undeliverable files addressed to Staff Sergeant (SSgt) Monroe.¹⁰⁶ The system administrators opened several of the files to determine why they failed to deliver in an attempt to clear the network.¹⁰⁷ Upon opening the files, the system administrators noticed that several contained pornographic images.¹⁰⁸ The system administrators notified the Air Force Office of Special Investigations (AFOSI).¹⁰⁹ The AFOSI obtained a search authorization and then searched SSgt Monroe's dormitory room, where he had his computer, and discovered both adult and child pornography stored on his computer.¹¹⁰ On appeal, SSgt Monroe sought to suppress the evidence discovered by the system administrators, asserting his claim of a reasonable expectation of privacy in his government e-mail account.¹¹¹

⁹⁸ See *infra* App. A.

⁹⁹ *Maxwell*, 45 M.J. at 417–18. The searched e-mail messages were sent to another AOL user and not disclosed to the FBI by the private citizen. *Id.* "The user also has a password which is used to access the system before the screen name is used, and the quantity of usage of the screen names, as measured by time on-line, is tracked for billing purposes." *Id.* at 411.

¹⁰⁰ *Id.* at 417. Evidence obtained by FBI agents who were lawfully monitoring an AOL chatroom is admissible at trial. *Id.* A message left on a message board is the equivalent to an "electronic postcard." *Id.* at 411; see also *United States v. Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997) (holding the defendant ran the risk that when he sent the messages to the "public at large" that they would be read by law enforcement officials). If one allows exposure of his communications or privacy to outsiders, then he has demonstrated that he has no intention to keep it to himself. See *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

¹⁰¹ However, if the intended recipient provided the e-mail message to police, then COL Maxwell would have no expectation of privacy. See *United States v. Hoffa*, 385 U.S. 293 (1966).

¹⁰² See *Maxwell*, 45 M.J. 406.

¹⁰³ *Pede*, *supra* note 85, at 21–22 (citing *Katz*, 389 U.S. at 351).

¹⁰⁴ *Maxwell*, 45 M.J. 406.

¹⁰⁵ *United States v. Monroe*, 52 M.J. 326 (C.A.A.F. 2000).

¹⁰⁶ *Id.* at 328.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ *Id.* at 329–30.

¹¹⁰ *Id.*

¹¹¹ *Id.* at 329.

The CAAF stopped short of finding that no reasonable expectation of privacy existed at all in government computer systems.¹¹² “Instead, the CAAF hedged by agreeing with the lower court that there was no reasonable expectation of privacy *vis-à-vis* the system administrators performing their official duties in monitoring the system and not viewing the files for law enforcement purposes.”¹¹³ The CAAF also relied on statutory privacy protections of the Electronic Communications Protection Act (ECPA)¹¹⁴ in reaching this conclusion.¹¹⁵

1. Application of the Secured Communications Act to Government E-Mail

The ECPA provides the framework for statutory protection rights that govern voice, wire, and electronic communications.¹¹⁶ The Stored Communications Act (SCA),¹¹⁷ a subsection of the ECPA, deals with the retrospective surveillance of electronic communication.¹¹⁸ The CAAF did not suppress the evidence because it determined the system administrator did not violate the ECPA’s provisions.¹¹⁹ In particular, the CAAF relied on the SCA in *Monroe*.¹²⁰

The version of [§] 2702(b) in effect at the time of trial in 1995 specifically states that “[a] person . . . may divulge the contents of a [stored electronic] communication . . . (6) to a law enforcement agency, if such contents (A) were inadvertently obtained by the service provider; and (B) appear to pertain to the commission of a crime.”¹²¹

The SCA derived from an area in which the Supreme Court has provided Congress with little guidance and where the differences between electronic and traditional means of communication are the greatest.¹²² Designed to regulate the conduct of governmental and private actors, the SCA provides the basic framework for privacy of stored electronic communications. The SCA is different from the Wire Tap Act¹²³ in that it covers both content and context (non-content) of the information that

¹¹² *Id.* at 330. The Air Force Court of Criminal Appeals held that there was no reasonable expectation of privacy on a government computer. *See* United States v. Monroe, 50 M.J. 550, 560 (A.F. Ct. Crim. App. 1999).

¹¹³ *See* United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (holding that appellant, a government employee, had no reasonable expectation of privacy when evidence of child pornography was discovered on a government computer by the system administrator who reported it to the Federal Bureau of Investigation); Conrad, *supra* note 28, at 4 (citing *Monroe*, 52 M.J. at 329–30).

¹¹⁴ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. (2000)). The court determined that since the e-mails were on the server and not in transit that the provisions of the Stored Communications Act, a section of the Electronic Communications Protection Act, would apply. *Monroe*, 52 M.J. at 331.

¹¹⁵ *Monroe*, 52 M.J. 326.

¹¹⁶ ORIN S. KERR, COMPUTER CRIME LAW 449 (2006).

¹¹⁷ *See* Stored Wired and Electronic Communications and Transactional Records Access, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701–2712).

The statute has been given various names by different commentators. Its names have included: (1) the “Electronic Communications Privacy Act” or “ECPA” because it was first enacted as part of that statute; (2) “Chapter 121” because it has been codified in Chapter 121 of Title 18 of the United States Code; (3) the “Stored Wired and Electronic Communications and Transactional Records Access” statute or “SWECTRA” because that is the formal title given to Chapter 121 in Title 18; and (4) “Title II” because it was enacted as the second title of ECPA.

Orin S. Kerr, *User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 n.1 (Aug. 2004). It is most commonly referred to as the SCA. *Id.*

¹¹⁸ KERR, *supra* note 116, at 500.

¹¹⁹ *See Monroe*, 52 M.J. 331. Even though the CAAF has subsequently held that the SCA does not provide a suppression remedy in other cases. *United States v. Allen*, 53 M.J. 402 (C.A.A.F. 2000) (holding that there was no suppression remedy under the ECPA and allowing the evidence under a theory of inevitable discovery). However, the CAAF’s analysis of the SCA provides insight that it is taking notice of privacy concerns raised by the governmental intrusion into e-mail stored on a government server.

¹²⁰ *Monroe*, 52 M.J. at 330–31.

¹²¹ *Id.* (citing 18 U.S.C. § 2702(b) (1994)). However, this determination might not be valid since this section of the ECPA would not apply to the Air Force. *See infra* notes 126–44 and accompanying text.

¹²² Mulligan, *supra* note 59, at 1567. Electronic communication is often stored on a server and is retrievable after the communication is complete, unlike a telephone conversation. *Id.*; *see also* Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. TECH. L. & POL’Y 135, 142–44 (2003).

¹²³ Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2522 (2000)). The Wire Tap Act prohibits the interception of oral, wire, or electronic communications unless a statutory exception applies or a search warrant exists. *See* 18 U.S.C.S. § 2511(1) (LexisNexis 2008). The Department of Justice instructs law enforcement and prosecutors to ask the following questions to determine if the Wire Tap Act is applicable: (1) Is the communication to be monitored a protected communication?; (2) Will the proposed surveillance be

it governs.¹²⁴ The SCA breaks down the information into three categories.¹²⁵ The legislative history indicates that the purpose of this distinction was to distinguish information concerning the identity of the user from more revealing transactional information.¹²⁶ The actual substance of the message or data stored on a computer network falls into content.¹²⁷ It is important to determine what is being sought, the content or non-content of a stored electronic communication.

The SCA affords greater protection to the content information of stored communications than to the non-content information.¹²⁸ The reasons for this are intuitive: the actual body of a message provides greater privacy concerns than the information containing the address of the intended recipient.¹²⁹ The SCA provides several mechanisms, depending on the type of information sought, for the government to acquire evidence.¹³⁰ They are consent of user, subpoena, subpoena with prior notice to the customer, a court order in compliance with section 2703(d), and a search warrant.¹³¹

To acquire un-accessed content information stored on a server for less than one hundred and eighty days the government must attain a search warrant.¹³² There are three options to acquire the contents of information maintained on a server for more than one hundred and eighty days.¹³³ The government may use a search warrant, a subpoena, or a court order under 18 U.S.C. § 2703(d).¹³⁴ This so-called “d” order is a combination of both a subpoena and a search warrant presented to a judge.¹³⁵ If the judge determines that government has provided specific and articulable facts showing that there are reasonable grounds to believe that the information to be compelled is “relevant and material” to a criminal investigation, he may sign the order.¹³⁶ The ISP responds to the “d” order like a normal subpoena.¹³⁷ The “d” order may contain language that forbids the ISP from notifying the subscriber that the government has compelled his information.¹³⁸ If information is

an “intercept”); and (3) If the answer is yes to these first two questions, does a statutory exception exist? SSCOECI MANUAL, *supra* note 16, at IV.D.1; *see also* Steve Jackson Games v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994) (holding the seizure of computer containing unretrieved e-mail is not an “intercept”); Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997) (viewing e-mail on another’s computer screen not an intercept because it does not involve use of “electronic, mechanical, or other device”); United States v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997) (ruling that “intercept” requires acquisition contemporaneous with transmission); Bohach v. Reno, 932 F. Supp. 1232 (D. Nev. 1996) (holding that in determining whether “intercept” occurred, must distinguish between very narrow “transmission phase” and much broader “storage phase”); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) (stating that “the acquisition of the data [must] be simultaneous with the original transmission of the data”).

¹²⁴ KERR, *supra* note 116, at 450. The SCA covers both the content of the message and information concerning who established the e-mail account. *Id.* Non-content information is the “envelope” information, which is sending and receiving the information. Orin S. Kerr, *Internet Surveillance Law After the Patriot Act: The Big Brother That Isn’t*, 72 NW. U. L. REV. 607, 611–14 (2003).

¹²⁵ SSCOECI MANUAL, *supra* note 16, at III.C. The first of these categories is basic subscriber information that includes basic information of the Internet user and his usage of the Internet. 18 U.S.C.S. § 2703(c)(2). It includes name; address; local and long distance telephone connection records, or records of session times and durations; length of service and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service. *Id.* The second category is a catchall for all information that is not content. 18 U.S.C. § 2703(c)(1); *see* SSCOECI MANUAL, *supra* note 16, at III.C.2; *see also* United States v. Allen, 53 M.J. 402, 409 (C.A.A.F. 2000) (holding that a record identifying the date, time, user, and detailed Internet address of sites accessed by a user constitute information under 18 U.S.C.S. § 2703(c)(2) (2000)). The final category is content. 18 U.S.C.S. § 2711(1) (citing the definition for content in 18 U.S.C.S. § 2510).

¹²⁶ SSCOECI MANUAL, *supra* note 16, at III.C.2.

¹²⁷ 18 U.S.C.S. § 2711(1) (citing the definition for content in 18 U.S.C. § 2510); *see also* Kerr, *supra* note 124, at 646 (arguing that the subject line of an e-mail should be considered content as well).

¹²⁸ *See* SSCOECI MANUAL, *supra* note 16, at III.D.1–5 (providing what information may be compelled with the different procedural requirements).

¹²⁹ Kerr, *supra* note 117, at 1228 n.142 (discussing in detail the opinion of Professor Daniel Solove, who argues that the some non-content information raises even greater privacy concerns).

¹³⁰ 18 U.S.C.S. § 2703.

¹³¹ *Id.* To access the non-content information normally only a subpoena is required, or in the case of non-content information covered under 18 U.S.C.S. § 2703(c)(1), a court order. *Id.* § 2703(c)(1)–(2).

¹³² *Id.* § 2703(a).

¹³³ *Id.* § 2703(a), (b).

¹³⁴ *Id.* § 2705.

¹³⁵ Kerr, *supra* note 117, at 1219; *see also* 18 U.S.C.S. § 2703(d).

¹³⁶ Kerr, *supra* note 117, at 1219 n.73 (citing 18 U.S.C. § 2703(d)).

¹³⁷ *Id.*

¹³⁸ *See* 18 U.S.C.S. § 2705. Under the SCA, if a process with greater procedural hurdles is used, it entitles the government to information obtainable with lesser process. SSCOECI MANUAL, *supra* note 16, at III.D.

available with a subpoena, but the government compels disclosure with a search warrant or “d” order, the SCA has been satisfied.¹³⁹

The SCA prohibits “public service providers”¹⁴⁰ from releasing information to other parties with some exceptions.¹⁴¹ A public ISP, such as AOL or Yahoo, may not voluntarily disclose any non-content or content information to a government entity unless an exception to the prohibition exists.¹⁴² The SCA is less stringent on voluntary disclosure for a nonpublic ISP.¹⁴³

A provider is not public (i.e., nonpublic) if the service is only available to those with a special relationship to the provider.¹⁴⁴ If the service provider is nonpublic, then there is no prohibition against voluntary disclosure of information.¹⁴⁵ On its face, the SCA would not apply to e-mail services provided to Soldiers via a government computer network.¹⁴⁶

Despite the Army’s status as a nonpublic ISP, the CAAF has nonetheless applied the SCA to system administrators of government networks and thereby made this statute applicable to the military.¹⁴⁷ The DOD has also applied the SCA to the Army through its own policies.¹⁴⁸ Department of Defense Directive (DODD) 5505.9 clearly indicates that the SCA applies to military law enforcement agencies.¹⁴⁹ Arguably, the Army may have converted itself into a public ISP through its own policies by providing e-mail use for those not employed by the military.

The Army provides an AKO e-mail account to not only Soldiers, but to family members, contractors, and others associated with the military.¹⁵⁰ The Army is not a “public” ISP per se, because it still requires an affiliation with the Army to obtain an account.¹⁵¹ Yet, it further demonstrates the increasing role of e-mail in modern society and the Army’s willingness

¹³⁹ SSCOECI MANUAL, *supra* note 16, at III.D (reasoning that law enforcement should exercise caution and adhere to the more onerous standards to ensure compliance); Kerr, *supra* note 117, at 1220 n.80 (arguing that obtaining a search warrant could avoid any Fourth Amendment challenges that may be raised); *see also* Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated*, 2007 U.S. App. LEXIS 23741 (Oct. 9, 2007).

¹⁴⁰ See 18 U.S.C.S. § 2702(a). Public for purposes of this article is a private entity, such as AOL or Yahoo. Nonpublic is a government agency or a business that provides services only for its employees. *See* Anderson Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998) (providing a comprehensive explanation of public and nonpublic ISPs).

¹⁴¹ See 18 U.S.C.S. § 2702.

¹⁴² *Id.* However, a public ISP may disclose non-content information to nongovernmental entities. *Id.* § 2702(c)(6). Eight exceptions allowing a public ISP to voluntarily disclose content information of a subscriber are: disclosure to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; as otherwise authorized in 18 U.S.C. § 2511(2)(a), or § 2703; with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service; to a person employed or authorized or whose facilities are used to forward such communication to its destination; as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; to the National Center for Missing and Exploited Children; to a law enforcement agency if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime; or to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. *Id.* § 2702(b). The exceptions to voluntary disclosure of non-content information of a subscriber are similar, but vary slightly. *See id.* § 2702(c).

¹⁴³ *See id.* § 2702(a)(1)–(3).

¹⁴⁴ Nonpublic is the term used in most academic research. It is counterintuitive. Public for purposes of this article is a private entity, such as AOL or Yahoo. Nonpublic is a government agency or a business that provides services only for its employees. *See* Anderson Consulting LLP, 991 F. Supp. 1041 (providing a comprehensive explanation of public and nonpublic ISPs).

¹⁴⁵ 18 U.S.C.S. § 2702. The rationale for this is not clear from the legislative history, but one reason may be that the service is for the benefit of the provider rather than the subscriber. SSCOECI MANUAL, *supra* note 16, at III.A. Additionally, a public provider offers a service in hopes of making a profit, while a nonpublic provider may offer it for a variety of reasons. Deborah M. McTigue, *Marginalizing Individual Individual Privacy on the Internet*, 5 B.U. J. SCI. & TECH. L. 5 paras. 15–17 (Spring 1999); *see infra* App. B (containing a simplified breakdown of the requirements for voluntary and compelled disclosure under the SCA).

¹⁴⁶ *See* Coacher, *supra* note 24, at 178 (concluding that the SCA is not applicable to e-mail service provided by the Air Force to its Airmen and civilian employees).

¹⁴⁷ United States v. Monroe, 52 M.J. 326, 330–31 (C.A.A.F. 2000) (applying the SCA to an Air Force computer network). *But see* Coacher, *supra* note 24, at 178 (concluding that the SCA is not applicable to e-mail service provided by the Air Force to its Airmen and civilian employees).

¹⁴⁸ U.S. DEP’T OF DEFENSE, DIR. 5505.9, INTERCEPTION OF WIRE, ELECTRONIC, AND ORAL COMMUNICATION FOR LAW ENFORCEMENT (20 Apr. 1995) [hereinafter DODD 5505.9].

¹⁴⁹ *Id.* para. 4-2.

¹⁵⁰ *See* AKO, *supra* note 73. The exhaustive list of those authorized access to a U.S. Army e-mail account is contained on this page. *Id.*

¹⁵¹ *See* Anderson Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).

to provide this technology for personal use. The SCA applies to the military through case law and policy, but this does not necessarily mean suppression for e-mail seized in violation of the SCA.

A statutory suppression remedy for a violation of the SCA does not exist, but § 2708 does leave open the possibility of suppression in the event of a constitutional violation.¹⁵² Courts have consistently ruled against finding a violation of the SCA that rises to a constitutional violation.¹⁵³ The CAAF shares this view.¹⁵⁴

While there has not been a suppression remedy for violation of the SCA, one court did enjoin the U.S. Navy from discharging a Sailor because the information attained in violation of the SCA formed the basis of the discharge.¹⁵⁵ The D.C. Circuit Court held there was a public interest in preserving privacy on the Internet and preventing the government from violating the SCA without recourse.¹⁵⁶ The holding in *McVeigh v. Cohen*¹⁵⁷ and DODD 5505.9 provide footing for suppressing information acquired in violation of the SCA, on the premise that the Army should not be rewarded for failing to adhere to DOD policy.

The SCA has come under attack for its constitutionality as well. *Warshak v. United States*, heralded as the first constitutional challenge to the SCA,¹⁵⁸ raised the possibility of Fourth Amendment protections for the content of stored electronic communications.¹⁵⁹ A Sixth Circuit panel relied on *Katz v. United States*¹⁶⁰ and *Smith v. Maryland*¹⁶¹ to determine that Mr. Warshak had a reasonable expectation of privacy in the content of his e-mail stored on the commercial ISP server.¹⁶² It held the government could only compel disclosure of a shared communication from a party who is a part of the conversation.¹⁶³ “It cannot, on the other hand, bootstrap an intermediary’s limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation).”¹⁶⁴ However, the Sixth Circuit sitting en banc vacated *Warshak*.¹⁶⁵ The holding of the Sixth Circuit panel further demonstrates that there is an objective expectation of privacy in e-mail residing on an ISP’s server under the Fourth Amendment. The Military Rules of Evidence (MRE) seem to indicate this as well.

¹⁵² 18 U.S.C.S. § 2708 (LexisNexis 2008) (“The remedies and sanctions described in this chapter [the SCA] are the only judicial remedies and sanctions for non-constitutional violations of this chapter [the SCA]”).

¹⁵³ See *United States v. Hambrick*, 225 F.3d 656 (4th Cir. 2000) (holding the issuance of a subpoena to a third party to secure information for criminal prosecution does not violate the Fourth Amendment); *United States v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000) (holding a violation of the ECPA does not violate the Fourth Amendment); *United States v. D’Andrea*, 497 F. Supp. 2d 117 (D. Mass. 2007) (holding a violation of the SCA does not require suppression of the evidence). *But see Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated*, 2007 U.S. App. LEXIS 23741; *McVeigh v. Cohen*, 983 F. Supp. 215 (D.C. Cir. 1998).

¹⁵⁴ *United States v. Allen*, 53 M.J. 402 (C.A.A.F. 2000) (holding that there was no suppression remedy under the ECPA and allowing the evidence under a theory of inevitable discovery).

¹⁵⁵ *McVeigh*, 983 F. Supp. 215. Senior Chief McVeigh was the senior enlisted member of the U.S.S. *Chicago* at the time of discovery of his homosexual orientation. *Id.* at 217.

¹⁵⁶ *Id.* at 221–22. A Navy Petty Officer at the direction of Navy Judge Advocate obtained Senior Chief McVeigh’s account information by false pretense. *Id.* at 217. Senior Chief McVeigh was allowed to retire from the Navy. See *McTigue*, *supra* note 145, para. 11 n.33 (citing Bradley Graham, *Gay Sailor Takes Navy Retirement Settlement; AOL Also Will Pay for Privacy Violation*, WASH. POST, June 13, 1998, at A3). The Department of Justice (DOJ) contends that this ruling may have been influenced by the “highly charged political atmosphere and press” coverage of this case. The DOJ contends the text of the statute makes it clear that there is not a suppression remedy for non-constitutional violations of the SCA and the holding is “somewhat perplexing.” See SSCOECI MANUAL, *supra* note 16, at III.H.

¹⁵⁷ See *McVeigh*, 983 F. Supp. 215. The DOJ believes that the court must have been mistakenly referring to constitutional rights and not the SCA. See SSCOECI MANUAL, *supra* note 16, at III.H.

¹⁵⁸ Reynolds Holding, *E-mail Privacy Gets a Win in Court*, TIME, June 21, 2007, available at <http://www.time.com/printout/0,8816,1636024.00.html>.

¹⁵⁹ *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated*, 2007 U.S. App. LEXIS 23741. The seizure of e-mail without a search warrant from an ISP’s server raises issues of a reasonable expectation of privacy, and the ability of an ISP like a telephone company to intercept the content of a transmission does not waive an expectation of privacy. *Id.* at 471.

¹⁶⁰ 389 U.S. 347 (1967).

¹⁶¹ 442 U.S. 735 (1979) (holding that the installation of a pen register was not a violation of the Fourth Amendment because it was not a search). When a person dials a telephone number and a pen register records it, he has no expectation of privacy in that information because he voluntarily turned that information to the telephone company, a third party. *Id.* at 743–44.

¹⁶² *Warshak*, 490 F.3d at 471–75, *vacated*, 2007 U.S. App. LEXIS 23741.

¹⁶³ *Id.* at 471.

¹⁶⁴ *Id.*

¹⁶⁵ *Warshak v. United States*, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007).

2. Was This an Inspection or a Workplace Search?

a. MRE 313

Monroe does not completely erode the expectation of privacy in a government e-mail account, but erases it in terms of evidence inadvertently discovered by system administrators conducting system maintenance.¹⁶⁶ The court focused on the administrator's reason for opening the e-mails: "[T]o determine the reason they were stuck in the MQUEUE directory and not for any law enforcement purpose"¹⁶⁷ The system administrators discovered the evidence pursuant to an inspection of SSgt Monroe's e-mail to ensure that the network was operating properly.

"To qualify as an inspection under MRE [Military Rule of Evidence] 313(b),¹⁶⁸ the commander's primary purpose for ordering the inspection of his or her unit must be administrative, not a search for evidence of a crime."¹⁶⁹ Military Rule of Evidence 313 allows evidence obtained from inspections and inventories conducted according to this rule to be admissible at courts-martial.¹⁷⁰ It is when the character of the inspection changes from military fitness and unit readiness to a search to uncover evidence of wrongdoing that it is no longer an inspection, but a search.¹⁷¹

To order an inspection under MRE 313, a commander does not need to have probable cause.¹⁷² The commander only needs to have a concern for the readiness of his unit. If the commander believes that evidence of crime exists before ordering an inspection, then the evidence, if found, is not admissible under MRE 313.¹⁷³

While the CAAF did not cite MRE 313, the actions of the system administrators in *United States v. Monroe*¹⁷⁴ adhered to this rule. They were acting under authority of their commanding officer to ensure that the computer network they were monitoring was "functioning properly," thereby "maintaining proper standards of readiness."¹⁷⁵ Staff Sergeant Monroe was not suspected of committing any crimes when his e-mail was inspected.¹⁷⁶ Nor was he subjected to a more stringent inspection than others who were using the network. When the system administrators discovered what they correctly surmised to be illegal pornography, they contacted law enforcement who then attained a search authorization.¹⁷⁷ The facts in *Monroe* demonstrate that the systems monitoring conducted by the system administrators complied with MRE 313.¹⁷⁸ A legitimate inspection includes monitoring to ensure that a computer network is properly functioning and that users remain within the limits of appropriate use.¹⁷⁹ The inspections contemplated under MRE 313 are similar to workplace searches for employees of government agencies.

¹⁶⁶ See *United States v. Monroe*, 52 M.J. 326 (C.A.A.F. 2000).

¹⁶⁷ *Id.* at 331.

¹⁶⁸ MCM, *supra* note 54, MIL. R. EVID. 313(b).

¹⁶⁹ Major James Herring, Jr., *What Is the "Subterfuge Rule" of MRE 313(b), After United States v. Taylor?*, ARMY LAW., Feb. 1996, at 24, 24.

¹⁷⁰ MCM, *supra* note 54, MIL. R. EVID. 313.

¹⁷¹ *United States v. Jackson*, 48 M.J. 292, 294 (1998) ("At the same time, we noted that an inspection might not be sustained if its character changed during the process or if the circumstances were unreasonable.").

¹⁷² MCM, *supra* note 54, MIL. R. EVID. 313.

¹⁷³ *Id.* MIL. R. EVID. 313(b). If the commander is searching for weapons or contraband, then he may order the inspection, but must prove by clear and convincing evidence that it was an inspection within the meaning of this rule. *Id.*

¹⁷⁴ 52 M.J. 326 (C.A.A.F. 2000).

¹⁷⁵ MCM, *supra* note 54, MIL. R. EVID. 313(b).

¹⁷⁶ *Monroe*, 52 M.J. at 328. The e-mail host administrator initially believed that SSgt Monroe received these large files as a prank, but came to realize that he was receiving these images on request. *Id.*

¹⁷⁷ *Id.* at 329–30.

¹⁷⁸ See *id.* at 326.

¹⁷⁹ See generally *id.*

b. A Workplace Search

O'Connor v. Ortega provides employees of government agencies limited Fourth Amendment protections in the workplace.¹⁸⁰ The Supreme Court held that Dr. Ortega, a physician employed by the State of California, maintained protections under the Fourth Amendment¹⁸¹ for his personal belongings in the workplace, even when the search was conducted for a civil matter.¹⁸² The realities of the workplace require a determination of what is reasonable in light of the efficient and effective requirements for the operation of the workplace.¹⁸³ “The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency’s work, and ultimately to the public interest.”¹⁸⁴ For investigations of work-related misconduct and for work-related purposes, such as retrieving a file, a standard of reasonableness judged on a case-by-case basis is required.¹⁸⁵ “Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable.”¹⁸⁶

Like civilian employers, commanders have a requirement to ensure their “workplace” operates in an efficient and effective manner.¹⁸⁷ “The . . . complicating factor in the military is that sometimes business-supervisor and law-enforcement authority merge in the person of the commander.”¹⁸⁸ The workplace search test is applicable to the military.¹⁸⁹ Military Rule of Evidence 313¹⁹⁰ provides additional guidance to the application of *O'Connor*¹⁹¹ in a military workplace. This rule provides guidance on determining whether the search for an item was for law enforcement purposes or to ensure that a workplace is operating efficiently.¹⁹² In *United States v. Muniz*,¹⁹³ decided before *O'Connor*, the Court of Military Appeals¹⁹⁴ used an “operational realities of the workplace”¹⁹⁵ concept to determine that appellant did not have a reasonable expectation of privacy in the drawers of his office credenza.

In *United States v. Muniz*, the command’s motive for searching his locked credenza drawers was to ascertain his whereabouts for accountability purposes not for a law enforcement purpose.¹⁹⁶ While the court relied on MRE 313 to determine that a search did not occur,¹⁹⁷ the rationale of *O'Connor* would have denied Captain Muniz a reasonable expectation of privacy in his credenza as well. However, *Muniz* and MRE 313 do not address the situation when government workplace practices create a reasonable expectation of privacy. *Long II* addresses this issue.¹⁹⁸

¹⁸⁰ 480 U.S. 709 (1987).

¹⁸¹ U.S. CONST. amend. IV.

¹⁸² *O'Connor*, 480 U.S. at 715. Personal property recovered during the search of his office impeached Dr. Ortega at his termination hearing. *Id.* at 736. “Dr. Ortega commenced . . . action against petitioners in Federal District Court under 42 U.S.C. § 1983, alleging that the search violated the Fourth Amendment.” *Id.* at 714.

¹⁸³ *Id.* at 721–22.

¹⁸⁴ *Id.* at 724.

¹⁸⁵ *Id.* at 725–26.

¹⁸⁶ *Id.* at 726. Justice Scalia, in a concurring opinion, believes that non-criminal government searches, which are normal in the private-employer context, do not violate the Fourth Amendment. *Id.* at 732 (Scalia, J., concurring).

¹⁸⁷ See generally *O'Connor*, 480 U.S. 709.

¹⁸⁸ *United States v. Muniz*, 23 M.J. 201, 205 (C.M.A. 1987).

¹⁸⁹ See generally *Long II*, 64 M.J. 57 (C.A.A.F. 2006); *United States v. Tanksley*, 54 M.J. 169 (C.A.A.F. 2000).

¹⁹⁰ MCM, *supra* note 54, MIL. R. EVID. 313.

¹⁹¹ *O'Connor*, 480 U.S. 709.

¹⁹² MCM, *supra* note 54, MIL. R. EVID. 313(b).

¹⁹³ *Muniz*, 23 M.J. at 205.

¹⁹⁴ On 5 October 1994, the National Defense Authorization Act for Fiscal Year 1995, Pub. L. No. 103–337, 108 Stat. 2663 (1994), changed the name of the U.S. Court of Military Appeals to the U.S. Court of Appeals for the Armed Forces. See Herring, *supra* note 169, at 24 n.5 (citing *United States v. Sanders*, 41 M.J. 485, 485 n.1 (C.A.A.F. 1995)). The same act also changed the names of the various courts of military review to the courts of criminal appeals. *Id.*

¹⁹⁵ *O'Connor*, 480 U.S. at 717.

¹⁹⁶ *Muniz*, 23 M.J. at 203.

¹⁹⁷ *Id.* at 206.

¹⁹⁸ *Long II*, 64 M.J. 57 (C.A.A.F. 2006).

VI. The Impact of *United States v. Long*

A. Background

Lance Corporal Long was convicted of wrongful use of several illicit drugs in violation of Article 112a, UCMJ.¹⁹⁹ Evidence submitted included seventeen pages of e-mail messages in which LCpl Long discussed her fear of testing positive on a urinalysis and her efforts to mask her drug use with three other Marines.²⁰⁰ Lance Corporal Long, at trial, moved to suppress these e-mails because the seizure occurred without a search authorization or her consent in violation of her Fourth Amendment rights.²⁰¹

During the course of an investigation into other misconduct allegedly committed by LCpl Long, investigators uncovered e-mails detailing her drug use.²⁰² An officer from the U.S. Marine Corps' (USMC) Inspector General, with the assistance from the network administrator for Headquarters, Marine Corps, seized LCpl Long's e-mails.²⁰³ The trial judge agreed with LCpl Long that the actions of the network administrator were a search for evidence without LCpl Long's consent and lacked a search authorization based on probable cause.²⁰⁴ However, the trial judge admitted the evidence, ruling that LCpl Long had no reasonable expectation of privacy in her government e-mail account.²⁰⁵

The Navy-Marine Corps Court of Appeals (NMCCA) held the military judge committed error by admitting the e-mail messages.²⁰⁶ The NMCCA relied on *United States v. Monroe*²⁰⁷ to outline the requirement of establishing an expectation of privacy to the content of e-mail messages sent via a government computer network.²⁰⁸ The NMCCA concluded that LCpl Long had a subjective expectation of privacy in her government e-mail account.²⁰⁹ The NMCCA also held that LCpl Long had an objectively reasonable expectation of privacy regarding her government e-mail account when law enforcement was involved in the search.²¹⁰ However, the NMCCA affirmed LCpl Long's conviction, finding the admission of the e-mails was harmless.²¹¹

The Navy Judge Advocate General certified two issues for review by the CAAF:

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

¹⁹⁹ *Long I*, 61 M.J. 539, 540 (N-M. Ct. Crim. App. 2005).

²⁰⁰ *Id.* at 541. In these e-mails, she admitted to using the illicit drugs as well. *Id.* at 542.

²⁰¹ *Id.* at 541.

²⁰² Harris Interview, *supra* note 13. Lance Corporal Long also allegedly fraternized with an officer assigned to Headquarters, U.S. Marine Corps. *Id.*

²⁰³ *Long I*, 61 M.J. at 541. Army Inspector General's investigations are for the assessment of command and not for criminal investigation, but the information may be shared with law enforcement. U.S. DEP'T OF ARMY, REG. 20-1, INSPECTOR GENERAL ACTIVITIES AND PROCEDURES para. 8-11 (1 Feb. 2007). Arguably, Army Inspector General investigations may qualify as being at the behest of law enforcement.

²⁰⁴ *Long I*, 61 M.J. at 541.

²⁰⁵ *Id.* at 541-42.

²⁰⁶ *Id.* at 542.

²⁰⁷ 52 M.J. 326 (C.A.A.F. 2000).

²⁰⁸ *Long I*, 61 M.J. at 543.

²⁰⁹ *Id.* at 544. Even though LCpl Long did not testify in her motion to suppress, the court relied on the system administrator's testimony that her password was required to access the network. *Id.* The password, like a key, excluded others from using her account and was a precautionary step to protect her privacy. *Id.*

²¹⁰ *Id.* at 546. The court, relying on *Picha v. Weiglos*, 410 F. Supp. 1214 (N.D. Ill. 1976) and *United States v. Pryba*, 502 F.2d 391 (D.C. Cir. 1974), held that "the reasonableness of an expectation of privacy turns on the degree of involvement by law enforcement." *Id.*

²¹¹ *Long I*, 61 M.J. at 546-49. The NMCCA held the error harmless because there was sufficient evidence based on government witnesses that LCpl Long would have been convicted without the admission of the e-mail transcript. *Id.*

received via the government network server.²¹²

Lance Corporal Long filed a cross petition arguing that the Fourth Amendment violation was not harmless beyond a reasonable doubt.²¹³ The CAAF focused on whether LCpl Long had a reasonable expectation of privacy in her e-mail communications sent over a government network.²¹⁴ Based on the particular facts of this case, the CAAF held that LCpl Long did have a subjective expectation of privacy in her e-mails, that her expectation of privacy was objectively reasonable, and that the error in admitting these e-mails was not harmless.²¹⁵ The CAAF looked at several factors to reach this conclusion.

B. Analysis of *United States v. Long*

1. Personal Use

Both the NMCCA and the CAAF held that LCpl Long could use her government e-mail account for personal use; this was persuasive in determining that she had a reasonable expectation of privacy.²¹⁶ Mr. Assessor, the senior network administrator, testified that LCpl Long could use her government e-mail account as long as it did not interfere with official business.²¹⁷ This coincides with current version of the *Joint Ethics Regulation (JER)*.²¹⁸

The *JER* enforces the DOD policy on the use and subsequent monitoring of government computer networks. Section 2–301(a) informs service members and DOD civilian employees that government communications are for “official and authorized purposes only.”²¹⁹ The *JER* expressly prohibits chain letters, pornography, and unofficial advertising, but permits limited personal use.²²⁰ The *JER* specifically allows employees to use their e-mail to send “directions to visiting relatives,” to check on house repairs, or to inform family members of changes in travel plans.²²¹ Each of the services has further refined the *JER* provisions and each varies slightly on what is permissible, but allows personal use of government e-mail.²²²

The Army has adopted the *JER* guidance on use of e-mail communications for personal matters.²²³ Army regulations published after decision in *Long II* still maintain the *JER* standard. The permissible use of a government network, even encouraged in some instances,²²⁴ indicates that the Army is promoting a reasonable expectation of privacy in those personal e-mails if the Soldier abides by the *JER*.

²¹² *Long II*, 64 M.J. 57, 58 (C.A.A.F. 2006).

²¹³ *Id.*

²¹⁴ *Id.* at 62.

²¹⁵ *Id.* at 59.

²¹⁶ *Id.* at 64; *Long I*, 61 M.J. at 541.

²¹⁷ *Long I*, 61 M.J. at 541. Judge Crawford, in her dissent, criticizes the majority’s reliance on the system administrator’s testimony. See *Long II*, 64 M.J. at 67 (Crawford, J., dissenting). She found that his perceptions of the Department of Defense (DOD) policy on computer use should not be “binding on the Department itself.” *Id.* However, she could offer no evidence to demonstrate that the system administrator’s perception was incorrect.

²¹⁸ See *JER*, *supra* note 27. The *JER* adopts the standards of ethical conduct for the Executive branch and ensures that all members of the military understand that “Public Service is a public trust.” *Id.* § 2-301; Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.101(a) (2008).

²¹⁹ *JER*, *supra* note 27. “Federal Government communications systems and equipment (including Government owned telephones, facsimile machines, electronic mail, Internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only.” *Id.* § 2-301(a).

²²⁰ *Id.* § 2-301(a)(2)(d).

²²¹ *Id.* § 2-301(a).

²²² Conrad, *supra* note 28, at 25 n.207. The baselines of personal use include limits on frequency, no additional costs to DOD, and not reflecting adversely on DOD. See *JER*, *supra* note 27, § 2-301(a). Failures to adhere to the standards of use set forth by the *JER* are criminal offenses for Soldiers. *Id.* Promulgating letter, para. (B)(2)(a). “The prohibitions and requirements printed in bold italics in [this] reference are general orders and apply to all military members without further implementation.” *Id.*

²²³ See AR 25-1, *supra* note 3, para. 6-1e; AR 25-2, *supra* note 3, para. 4-5r(6).

²²⁴ Army Knowledge Online, <https://www.us.army.mil> (follow “Inside AKO” hyperlink, then follow “AKO Video Messaging” hyperlink) (last visited Oct. 9, 2008).

As previously discussed in Section II of this article, the Army has legitimate reasons for monitoring a computer network. However, the Army wants to respect the rights of those who use government networks for personal use.²²⁵ Army Regulation (AR) 380-53, *Information Systems Security Monitoring*, stresses that system administrators must conduct monitoring in the least obtrusive manner possible.²²⁶ The system administrators will, to the maximum extent possible, respect “the privacy and civil liberties of individuals whose telecommunications are subject to monitoring.”²²⁷ Additionally, when evidence of criminal misconduct does occur, unless it requires additional monitoring to prevent death, serious bodily injury, or sabotage, administrators must stop systems monitoring and report the misconduct to law enforcement for investigation.²²⁸ The Army’s own longstanding policy to respect privacy and civil liberties demonstrates that the Army had provided an expectation of privacy vis-à-vis law enforcement prior to *Long II*.

Finally, AR 380-53 provides guidance to ensure that system administrators do not monitor privileged communications.²²⁹ The Army published AR 380-53 before *Long II* and subsequent changes to the warning banner for all government computer networks. However, all of the senior uniformed Judge Advocates agree that communications between clients and attorneys remain privileged when sent over a government computer network despite valid reasons for systems monitoring.²³⁰ Brigadier General James Walker²³¹ stated, “The key aspect of the revision is to make certain that we maintain the protections of privileged communications . . . within . . . the Department of Defense.”²³² The American Bar Association has even opined that attorneys do not violate an ethical duty by communicating with clients via e-mail.²³³ In its willingness to recognize privilege in addition to allowing personal use after *Long II*, the Army has implicitly strengthened the argument that Soldiers have a reasonable expectation of privacy in their government e-mail for Fourth Amendment purposes.

While the CAAF relied on the personal use policy to determine LCpl Long had a reasonable expectation of privacy, it examined other factors as well.²³⁴ A policy permitting personal use does not, on its own, create a reasonable expectation of privacy. The CAAF looked at factors, such as the user’s ability to exclude others from reading e-mail, to determine if government practices had created a reasonable expectation of privacy.²³⁵

2. The Use of a Password

The CAAF looked at MRE 314(d)²³⁶ to determine if LCpl Long’s e-mail was military property not requiring probable cause for a search.²³⁷ The court relied on the holding in *O’Connor v. Ortega*,²³⁸ which is consistent with MRE 314(d) allowing searches of government property without a search authorization unless facts demonstrate that the person had a

²²⁵ AR 25-2, *supra* note 3, para. 4-5s(4). System administrators will not engage in blanket monitoring of communications. *Id.*

²²⁶ AR 380-53, *supra* note 3, para. 2-6c.

²²⁷ *Id.* para. 2-1b.

²²⁸ *Id.* para. 2-9c.

²²⁹ *Id.* para. 2-10i. Army Regulation 380-53 does not provide any rules that forbid disclosure if inadvertently discovered nor does it provide any means for a system administrator to recognize what is a privileged communication under the Military Rules of Evidence. *Id.* See *infra* App. C for a more detailed discussion on ethical responsibilities of Judge Advocates in relation to communicating with clients on a monitored network.

²³⁰ Teri Figueroa, *Pentagon Revising Computer-Snooping Policy*, N. COUNTY TIMES, Jan. 7, 2008, http://www.nctimes.com/articles/2008/01/07/news/top_stories/15_50_901_6_08.txt (relying on statements from the Staff Judge Advocate to the Commandant, U.S. Marine Corps); Telephonic Interview with Richard Aldrich, Contractor, Dep’t of Defense Chief Info. Officer, in Charlottesville, Va. (Jan. 2, 2008) [hereinafter Aldrich Interview]; see also e-mail from Lieutenant Colonel Thomas J. Herthel, U.S. Air Force, Administrative Law Division Office of the Judge Advocate General, to Lieutenant Colonel Thomas Wand, U.S. Air Force, Chief, Joint Service Policy and Legislation (Jan. 11, 2008, 10:27 EST) [hereinafter Herthel e-Mail] (on file with author).

²³¹ Staff Judge Advocate to the Commandant, U.S. Marine Corps.

²³² Figueroa, *supra* note 230 (referring to Memorandum from Dep’t of Def. Chief Info. Officer to Secretaries of the Military Dep’ts, et al., subject: Policy on Department of Defense Information Systems—Standard Consent Banner and User Agreement (2 Nov. 2007) [hereinafter CIO Memo I]). This policy is on temporary hold. Memorandum from Dep’t of Def. Chief Info. Officer to Secretaries of the Military Dep’ts, et al., subject: Temporary Hold on Implementation of New Banner and User Agreement (7 Dec. 2007) [hereinafter CIO Memo II] (on file with author).

²³³ See ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 99-413 (1999).

²³⁴ *Long II*, 64 M.J. 57, 64 (C.A.A.F. 2006).

²³⁵ *Id.* at 63.

²³⁶ MCM, *supra* note 54, MIL. R. EVID. 314(d).

²³⁷ *Long II*, 64 M.J. at 64.

²³⁸ 480 U.S. 709 (1987).

reasonable expectation of privacy in that property.²³⁹ Relying on *Ortega*, the CAAF looked at the privacy expectations in terms of the office practices, procedures, and regulations in effect at Headquarters, USMC.²⁴⁰ One of the office practices, the use of a password, was particularly persuasive.

The CAAF determined that the use of a password, known only to LCpl Long, was indicative in establishing an expectation of privacy.²⁴¹ “In fact, CAAF viewed the password requirements for e-mail as not only indicative of Long’s privacy expectations, but as a business practice that reinforces this expectation.”²⁴² Lance Corporal Long had a reasonable expectation of privacy because the ability to access her account relied on a password that only she knew.²⁴³ In *City of Reno v. Bohach*, the Federal District Court of Nevada held that the appellant had no reasonable expectation of privacy in the content of his text pages stored on a police department computer.²⁴⁴ In *Bohach*, anyone with access to the police department network could retrieve these messages.²⁴⁵ In contrast, Lance Corporal Long (LCpl) had the ability to prevent everyone except the system administrator from accessing her e-mail account.²⁴⁶ Lance Corporal Long’s password to her e-mail account was the equivalent to the key for the lock on her wall locker.

Even though a master key existed for LCpl Long’s e-mail account, the ability to secure an area demonstrates that a person has acquired a subjective expectation of privacy.²⁴⁷ The CAAF has looked to the ability of a servicemember to secure government property to the exclusion of others to determine if an individual could establish a subjective expectation of privacy.²⁴⁸ Chief Judge Everett, in a concurring opinion from *United States v. Muniz*, stated that there are circumstances, such as being able to secure the drawer to a credenza, that provide a service member a reasonable expectation of privacy in government-issued property.²⁴⁹ Although the ability to exclude others from a desk or from accessing an e-mail account establishes an expectation of privacy, it does not prevent the command from inspecting or monitoring a Soldier’s use of government equipment.²⁵⁰ *Long II* reinforces that law enforcement cannot search government-owned property when a reasonable expectation of privacy has been established without a search authorization, yet a commander may still inspect that property.

The Army and DOD are attempting to circumvent *Long II* with new policies. The proposed DOD consent banner places users on notice that the password that a Soldier creates to access his e-mail is for the benefit of the government and not the Soldier.²⁵¹ No Army regulation states this. The approved consent banner issued by the Army does not state this.²⁵² Training that all Soldiers are required to complete before obtaining access to a government network stresses the importance of keeping individual passwords secured.²⁵³ A Soldier may not share his password with other Soldiers, including supervisors, because

²³⁹ *Long II*, 64 M.J. at 64–65.

²⁴⁰ *Id.* at 64.

²⁴¹ *Id.* at 63.

²⁴² Stewart, *supra* note 14, at 12.

²⁴³ *Long II*, 64 M.J. at 63. Even though the password may have served some governmental interest, it did not diminish her subjective expectation of privacy. *Id.*

²⁴⁴ 932 F. Supp. 1232 (D. Nev. 1996) (finding no expectation of privacy in text messages sent over the police department network). Bohach, a police officer, had sought an injunction to prevent the Internal Affairs Unit of the Reno Police Department from obtaining the text of pager messages based on Fourth Amendment and ECPA claim. *Id.* at 1233. The paging system allowed any user of the police department to send a text message from any police department computer using a program that would transmit the message to the department pager for a particular officer. *Id.* at 1233–34.

²⁴⁵ *Id.* at 1235.

²⁴⁶ *Long I*, 61 M.J. 539, 541 (N-M. Ct. Crim. App. 2005) (noting that system administrator did not even know LCpl Long’s password and had to lock her out of the system to access her e-mail account).

²⁴⁷ *But see* *United States v. Geter*, 2003 CCA LEXIS 134 (N-M. Ct. Crim. App. May 30, 2003). The court determined that the appellant did not demonstrate a subjective expectation of privacy because the password was for security of the system. *Id.* at *12. This argument is not persuasive. Soldiers store their government-issued TA-50 in a wall locker, so under this rationale Soldiers would have no reasonable expectation of privacy in their wall locker.

²⁴⁸ *United States v. Craig*, 32 M.J. 614, 615 (C.M.A. 1992) (holding that there was no expectation of privacy when appellant was told by his commander to leave the desk unlocked so that others may access it).

²⁴⁹ *United States v. Muniz*, 23 M.J. 201, 208 (C.M.A. 1987) (Everett, C.J., concurring).

²⁵⁰ *Id.* at 203.

²⁵¹ CIO Memo I, *supra* note 232. This policy is on temporary hold. CIO Memo II, *supra* note 232.

²⁵² AR 25-2, *supra* note 3, para. 4-5m.

²⁵³ U.S. Army Info. Assurance Training Ctr., Department of Defense Information Assurance Awareness Training, <https://ia.gordon.army.mil/dodiaa/default.asp> (last visited Oct. 9, 2008).

he is responsible for the use of that account.²⁵⁴ All Soldiers still have the ability to exclude others, with the exception of the system administrators, from viewing the content e-mail messages even with implementation of the new DOD consent banner. The ability to exclude others from a government e-mail account demonstrates both a subjective and an objective expectation of privacy. While the stated intent of the password is for the benefit of the government,²⁵⁵ in reality it provides the Soldier the ability to exclude others from accessing his assigned e-mail. Regardless, consent to monitoring may erase the reasonable expectation of privacy established by the presence of a password.

3. Consent

Because of *O'Connor*, a user's consent to monitor his government e-mail creates the largest hurdle to finding a reasonable expectation of privacy in government e-mail.²⁵⁶ Nevertheless, *Long II* demonstrated that this is not an insurmountable task.²⁵⁷ The NMCCA and the CAAF looked at the "Notice and Consent to Monitoring" banner to determine if LCpl Long had a reasonable expectation of privacy.²⁵⁸ The banner put LCpl Long on notice that her e-mails were subject to monitoring by a system administrator, but did not mention that law enforcement could view the e-mails for reasons other than unauthorized use.²⁵⁹ The NMCCA held that LCpl Long had a subjective expectation of privacy as to all others except for the network administrator based on the language of the banner.²⁶⁰

The CAAF, like the NMCCA, distinguished between systems monitoring and law enforcement.²⁶¹ "Simply put, in light of all the facts and circumstance in this case, the 'monitoring' function detailed in the log-on banner did not indicate to LCpl Long that she had no reasonable expectation of privacy in her e-mail."²⁶² The CAAF distinguished this case from *Monroe*,²⁶³ the inspection of the e-mail was in accordance with the consent to monitoring to which SSgt Monroe had agreed.²⁶⁴ Lance Corporal Long never consented to a search by law enforcement and therefore a search authorization was required.²⁶⁵ The CAAF did not discuss the issue of voluntary consent.

"To be valid, consent must be given voluntarily."²⁶⁶ The ability to use a government computer system relies on agreeing to consent to monitoring.²⁶⁷ This provides for no real choice in some circumstances. Lance Corporal Long, stationed in

²⁵⁴ *Id.*; see also AR 25-2, *supra* note 3, para. 4-5a(8).

²⁵⁵ See CIO Memo I, *supra* note 232.

²⁵⁶ Conrad, *supra* note 28, at 2.

²⁵⁷ *Long II*, 64 M.J. 57, 65 (C.A.A.F. 2006).

²⁵⁸ *Long I*, 61 M.J. 539, 541 (N-M. Ct. Crim. App. 2005).

This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Id.

²⁵⁹ *Id.* at 541. This may have oversimplified the situation. Evidence discovered during systems monitoring generally fits into the exceptions of *O'Connor v. Ortega*, 480 U.S. 709 (1987). It is when the search is purely for law enforcement that the two prongs of *Ortega* are not satisfied. See *O'Connor v. Ortega*, 480 U.S. 709 (1987).

²⁶⁰ See *Long I*, 61 M.J. at 544 (holding the military judge made no explicit finding on this); *Long II*, 64 M.J. at 65.

²⁶¹ *Long II*, 64 M.J. at 65.

²⁶² *Id.*

²⁶³ 52 M.J. 326 (C.A.A.F. 2000).

²⁶⁴ *Long II*, 64 M.J. at 64.

²⁶⁵ *Long I*, 61 M.J. at 541.

²⁶⁶ MCM, *supra* note 54, MIL. R. EVID. 314(e)(4).

²⁶⁷ See AR 25-2, *supra* note 3, para. 4-5m.

Washington, D.C., had the ability to use a personal computer after duty hours to conduct personal business. For the Soldier deployed to an isolated location, he may have to choose between waiving his expectation of privacy in his government e-mail and communicating with family. This subtle difference is enough to make the consent involuntary.²⁶⁸ Consenting to have your communications monitored by clicking on the log-in banner is a virtual “acquiescence to authority” that requires the suppression of the evidence.²⁶⁹ The Army complicates this matter by offering e-mail accounts to spouses and encouraging personal use.²⁷⁰ This practice erodes the consent to monitor personal e-mail.²⁷¹ Additionally, by consenting to monitoring when a Soldier has no other choice but to use a government e-mail account, a Soldier’s ability to communicate freely and openly is restricted.

The Supreme Court has held that the government may not deny a benefit to a person on the basis that it infringes on a constitutionally protected area.²⁷² The Supreme Court was particularly concerned in cases involving free speech interests.²⁷³ In terms of monitoring e-mail, Soldiers may unknowingly fail to consider that consenting to monitoring of e-mail may be eroding their privacy interests. This is especially troubling when the purpose of the monitoring is to gather evidence and bypass the Fourth Amendment.

VII. The Army’s Reaction

Prior to the decision in *Long II*, Army policy regarding computer monitoring²⁷⁴ was designed to ensure that government computers networks were functioning properly and not to serve as a law enforcement tool.²⁷⁵ Since then, the focus has moved to a policy that enables unfettered law enforcement access to a Soldier’s e-mail account under the premise of systems monitoring.²⁷⁶ Discovering evidence of misuse or other illegal activity is a by-product of ensuring that the network is properly operating, not the primary focus.²⁷⁷ The current focus in systems monitoring is to allow law enforcement unfettered access to any communication passed over government network. Allowing law enforcement to encroach upon systems monitoring invalidates the new policy. Comparing the Army policies in light of DOD policies before and after the decision in *Long II*²⁷⁸ demonstrates this point.

²⁶⁸ *United States v. White*, 27 M.J. 264, 266 (C.M.A. 1988) (citing *Schneekloth v. Bustamonte*, 412 U.S. 218, 228 (1973)) (“For, no matter how subtly the coercion was applied, the resulting ‘consent’ would be no more than a pretext for the unjustified police intrusion against which the Fourth Amendment is directed.”).

²⁶⁹ *See United States v. Radvansky*, 45 M.J. 226, 230 (C.A.A.F. 1996) (citing *United States v. McClain*, 31 M.J. 130, 133 (C.M.A. 1990), *United States v. White*, 27 M.J. 264, 266 (C.M.A. 1988)). Professor Friewald argues that the government cannot deny constitutional protection merely because the government has taken that protection away. Friewald, *supra* note 62, para. 31 (relying on *Smith v. Maryland*, 442 U.S. 735, 739 n.5 (1979)) (“To do otherwise would place constitutional rights at the mercy of the executive branch, an entity which the Fourth Amendment was specifically designed to constrain.”).

²⁷⁰ Army Knowledge Online, <https://www.us.army.mil> (follow “Inside AKO” hyperlink, then follow “AKO Video Messaging” hyperlink) (last visited Oct. 9, 2008); AKO, *supra* note 73.

²⁷¹ Memorandum from Dep’t of the Air Force, Office of the Gen. Counsel (National Security & Military Affairs), to Air Force Office of Special Investigations Judge Advocate, subject: Computer Privacy (14 Dec. 2006) [hereinafter Air Force Gen. Counsel Memo] (on file with author). A log-in banner generally precludes as reasonable expectation of privacy “except where local practice has eroded consent.” *Id.*

²⁷² *Perry v. Sindermann*, 408 U.S. 593 (1972).

²⁷³ *Id.* at 597 (holding that the government may not deny benefits to its citizen based upon exercise their right of free speech). The CAAF has not addressed the constitutionality of consent to monitoring in any of the cases involving digital media from the aspect of the First Amendment. Lance Corporal Long’s defense attorney did not raise any freedom of speech concerns in his appellate answer to CAAF. *See Appellee’s Answer, Long II*, 64 M.J. 57 (C.A.A.F. 2006) (No. 05–5002/MC). If LCpl Long has been in Iraq and her only access was to a government network, the basis for her appeal may have taken on a different light.

²⁷⁴ 64 M.J. 57 (C.A.A.F. 2006).

²⁷⁵ Thomas King, Attorney, Office of the Staff Judge Advocate, U.S. Army Network Enterprise Technology Command, Legal Issues and Information Systems Operations (Sept. 16, 2002) (unpublished Power Point presentation citing guidance provided by the Deputy, Army Chief of Staff for Intelligence) (on file with author). Computer monitoring is not to be used to further internal unit investigations by targeting individual Soldiers. *Id.*

²⁷⁶ *See AR 25-2, supra* note 3.

²⁷⁷ The misuse of a government computer network discovered during monitoring is an offense punishable under the UCMJ as a *JER* violation. *See JER, supra* note 27, Promulgating letter, para. (B)(2)(a) (“The prohibitions and requirements printed in bold italics in [this] reference are general orders and apply to all military members without further implementation.”). This does not mean that when a system administrator discovers misconduct that criminal prosecution was the primary purpose of the systems monitoring. *See infra* notes 298–301 and accompanying text.

²⁷⁸ *See Long II*, 64 M.J. 57 (2006).

In the context of systems protection monitoring, DODD 8500.01E, *Information Assurance*, provides guidance on what monitoring entails.²⁷⁹ The purpose of monitoring is to “detect, react, and isolate” threats to the government network, including threats of internal misuse.²⁸⁰ It does not provide for systems monitoring to be a tool for law enforcement. This is consistent with policies in effect prior to the decision in *Long II*.

In 1998, the Assistant Secretary of Defense (Command, Controls, Communication, and Intelligence) provided guidance on computer monitoring.²⁸¹ Monitoring is for “purposes of systems management and protection, protection against improper or authorized use or access, and verification of applicable security features or procedures; . . . use of the system constitutes monitoring.”²⁸² Neither this guidance nor DODD 8500.01E equates this to consenting to law enforcement monitoring.²⁸³ However, in response to *Long II*²⁸⁴ on 2 November 2007 the DOD Chief Information Officer supplemented this guidance to include consent to monitoring for law enforcement purposes.²⁸⁵ This new log-in banner has been on hold since 7 December 2007.²⁸⁶ However, the Army has adopted new log-in banner language and updated AR 25-2 to permit law enforcement encroachment upon systems monitoring.²⁸⁷

Army Regulation 25-2, paragraph 4-5m adopts the requirements for the consent for monitoring provided by the Assistant Secretary of Defense (Command, Controls, Communication, and Intelligence) in 1998, but has additional information as to the scope of the consent.²⁸⁸ The prior log-in banner reflected the language required by the 1998 Assistant Secretary of Defense (Command, Controls, Communication, and Intelligence) policy.²⁸⁹ The new language informs the user that he expressly consents to monitoring for law enforcement purposes and that there is no expectation of privacy in his government e-mail account.²⁹⁰ This change is a direct response to *Long II*.²⁹¹ Prior to the publication of the 24 October 2007 version of AR 25-2, users maintained an expectation of privacy in systems monitoring with respect to law enforcement.²⁹²

The Army has reserved the right to view any communication whenever it desires in its new version of AR 25-2.²⁹³ Paragraph 4-5s²⁹⁴ provides that system administrators may retrieve, recover or intercept an e-mail only with the consent of a

²⁷⁹ U.S. DEP’T OF DEFENSE, DIR. 8500.01E, INFORMATION ASSURANCE (24 Oct. 2002) (C1, 23 Apr. 2007) [hereinafter DODD 8500.01E]. The *JER* also places Soldiers on notice that their use of a government computer system is subject to monitoring. *JER*, *supra* note 27, § 2-301(a)(3). The *JER* does not define monitoring, but refers the reader to two now-rescinded DOD directives. *Id.* (citing U.S. DEP’T OF DEFENSE, DIR. 4640.6, COMMUNICATIONS SECURITY TELEPHONE MONITORING AND RECORDING (26 June 1981) (rescinded 9 Oct. 2007); U.S. DEP’T OF DEFENSE, DIR. 4640.1, TELEPHONE MONITORING AND RECORDING (15 Jan. 1980) (rescinded 9 July 1990)). Lieutenant Colonel Coacher compared this guidance to placing a size “2007” foot into a “1980” shoe, which is difficult to do and requires a lot of “wiggling” to accomplish. *See* Coacher, *supra* note 25, at 189.

²⁸⁰ DODD 8500.01E, *supra* note 279, para. 4-20.

²⁸¹ ASOD (C4I) Memo, *supra* note 6.

²⁸² *Id.*

²⁸³ U.S. DEP’T OF DEFENSE, INSTR. 8560.01, COMMUNICATION SECURITY (COMSEC) MONITORING AND INFORMATION ASSURANCE (IA) READINESS TESTING para. 4-5 (9 Oct. 2007). Criminal misconduct discovered during COMSEC monitoring may not be used for prosecution without approval of the general counsel of the department who conducted the monitoring. *Id.*

²⁸⁴ 57 M.J. 64 (C.A.A.F. 2006).

²⁸⁵ CIO Memo II, *supra* note 232. The change to the standard consent banner was in response to *Long II*, 64 M.J. 57 (C.A.A.F. 2006). Aldrich Interview, *supra* note 230; *see also* Figueroa, *supra* note 230 (citing Major Patrick Ryder, a spokesman for the DOD) (“In general terms, the main difference in the two user consent banners is that the updated version seeks to make it clearer to users what they are consenting to when they use a DoD computer.”).

²⁸⁶ CIO Memo I, *supra* note 232. Retracted because of concerns by the Air Force TJAG, Major General Rives, over the failure to explicitly recognize privileges under the new policy, in particular the attorney client privilege. Herthel e-mail, *supra* note 230. New DOD policy mentions that privileges were not negated by the new banner, but raises the issue if they even existed. CIO Memo I, *supra* note 232.

²⁸⁷ *See* AR 25-2, *supra* note 3. On 3 August 2007, the Army released a major revision of AR 25-2 to replace the previous version dated 14 November 2003. AR 25-2 (2003), *supra* note 6. The 3 August 2007 version of AR 25-2 was replaced by the current version and corrected typographical errors and put in place the current log-in banner. *See* AR 25-2, *supra* note 3, Summary of Changes.

²⁸⁸ *See* AR 25-2, *supra* note 3, para. 4-5m.

²⁸⁹ *See* AR 25-2 (2003), *supra* note 6.

²⁹⁰ AR 25-2, *supra* note 3, para. 4-5m. Prior to the change in AR 25-2, FORSCOM had adopted a banner that informed users that law enforcement officials for the purpose of “investigating and prosecuting criminal misconduct” might monitor computer systems. FORSCOM Memo, *supra* note 6.

²⁹¹ *Long II*, 64 M.J. 57 (C.A.A.F. 2006); Aldrich Interview, *supra* note 230.

²⁹² AR 25-2 (2003), *supra* note 6, para. 4-5r (“Users will be advised that there is no expectation of privacy while using Army ISs [information systems] or accessing Army resources except with respect to LE/CI [Law Enforcement/Counter-Intelligence] activities.”).

²⁹³ AR 25-2, *supra* note 3, para. 4-5s(4).

party to the communication, in response to the inspector general, in response to properly authorized law enforcement investigation, in response to an informal investigation under AR 15-6,²⁹⁵ a preliminary inquiry under AR 380-5,²⁹⁶ or a commander's inquiry under Rule for Courts-Martial 303.²⁹⁷ There is an additional method for the release under paragraph 4-5t, a management search in the absence of an employee.²⁹⁸ The Army allows liberal access to view a Soldier's e-mail on a government server. The ability to view a Soldier's e-mail on a government server ranges from systems monitoring, to administrative requests, or in response to investigations with an eye toward prosecution. The new Army policy, while trying to erase the reasonable expectation of privacy created by *Long II*, is at odds with Supreme Court precedent.²⁹⁹

The Army's policy for systems monitoring has transformed from an inspection to ensure readiness of its computer networks to a search to uncover wrongdoing for criminal prosecution. In *United States v. Burger*, the Supreme Court held that administrative inspections of a highly regulated industry are constitutional, in part to lower expectations of privacy due to the state's interest in regulation.³⁰⁰ However, in *Ferguson v. City of Charleston*, the Supreme Court held that a Fourth Amendment violation occurs when a government policy exists for the primary purpose of collecting evidence for criminal prosecution, even if the policy has secondary non-criminal justification.³⁰¹ Army Regulation 25-2 has warped from something akin to an inspection envisioned by MRE 313 to a policy designed to allow law enforcement to seize e-mail without probable cause.³⁰² It is no longer monitoring to ensure that the network remains viable, but an attempt to bypass the Fourth Amendment by allowing law enforcement to access e-mail without acquiring a search authorization.³⁰³

VIII. Analysis

The CAAF, the SCA, and the MRE do not prohibit the monitoring of government computer networks to ensure that the system is operating properly and used for only authorized purposes.³⁰⁴ However, the CAAF has held that a servicemember has a reasonable expectation of privacy vis-à-vis law enforcement in their government e-mail account.³⁰⁵ The involvement of law enforcement shifts the purpose from systems protection to evidence collection, and thus requires probable cause and a search authorization.³⁰⁶

²⁹⁴ *Id.* para. 4-5s(10). The consent of the party to monitoring for this paragraph appears separate and distinct from the consent to monitor the user agrees to when he access a government information system.

²⁹⁵ U.S. DEP'T OF ARMY, REG. 15-6, PROCEDURES FOR INVESTIGATING OFFICERS AND BOARDS OF OFFICERS (2 Oct. 2006).

²⁹⁶ U.S. DEP'T OF ARMY, REG. 380-5, DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM (29 Sept. 2000).

²⁹⁷ MCM, *supra* note 54, R.C.M. 303. Arguably, investigations conducted under the provisions of AR 15-6, an Inspector General's Request, or AR 380-5 may not qualify as law enforcement investigations. However, if initiated with an eye towards prosecution they would qualify. This would require a careful examination of the facts in each situation.

²⁹⁸ AR 25-2, *supra* note 3, para. 4-5t. For example, if a trial counsel, on emergency leave, has witness contact information on an e-mail stored on a government server, the Chief of Justice would be able to access it under this paragraph.

²⁹⁹ See generally *O'Connor v. Ortega*, 480 U.S. 709 (1987) (holding that government employees have limited Fourth Amendment protections in the workplace).

³⁰⁰ 482 U.S. 691 (1987) (upholding a New York statute that permitted warrantless inspections of junkyards for the primary purpose of deterring auto theft). The Court determined that New York had a substantial interest in deterring auto theft, that regulating the "vehicle dismantling" industry helps deter auto theft, the statute provides a constitutionally adequate substitute for a warrant, and finally the statute limits the "time, place, and scope" of the inspection. See *id.* at 708-13.

³⁰¹ 532 U.S. 67 (2001). A state-run hospital in South Carolina required all expectant mothers to receive a urinalysis. *Id.* Law enforcement received information on positive test results. *Id.* The hospital policy's ultimate goal was to ensure that the expectant mothers obtained drug counseling; its immediate goal was to provide information for prosecution. See *id.* The Supreme Court distinguished this case from *United States v. Burger*, 482 U.S. 691 (1987), where the discovery of criminal violations was incidental to an administrative search; in *Ferguson*, the policy "was specifically designed to gather evidence of violations of penal laws." *Ferguson*, 532 U.S. at 84 n.21.

³⁰² See *United States v. Battles*, 25 M.J. 58, 60 (C.M.A. 1987).

Whether such government action might be considered constitutional as a legitimate administrative inspection in light of the holding of the Supreme Court in *New York v. Burger*, need not be decided today. Moreover, whether Mil. R. Evid. 313(b) is constitutional in light of the particular requirements of that decision is also a question for a later time.

Id. (citation omitted).

³⁰³ "Monitoring is the observation of a resource for the purpose of ascertaining its status or operational state." See AR 25-2, *supra* note 3, glossary.

³⁰⁴ See generally Dolak & Dolak, *supra* note 26; Conrad, *supra* note 28; Coacher, *supra* note 24.

³⁰⁵ *Long II*, 64 M.J. 57 (C.A.A.F. 2006).

³⁰⁶ Coacher, *supra* note 24, at 192-93.

The SCA³⁰⁷ is applicable to the military by its own policies not by the terms of the statute. Under DODD 5505.9,³⁰⁸ law enforcement are directed to adhere to the provisions of the ECPA.³⁰⁹ The SCA is a sub-part of the ECPA.³¹⁰ Under the SCA, a system administrator may turn over evidence discovered while rendering services or in protecting the property of the provider.³¹¹ If law enforcement wants to view the content of e-mail stored on a server, they are required to attain a subpoena or court order.³¹² There is no per se suppression remedy for violating the terms of the SCA,³¹³ but DOD has solidified a Soldier's reasonable expectation of privacy in his government e-mail account by holding itself accountable to the provisions of the SCA.³¹⁴

The Army and DOD further reinforce a Soldier's expectation of privacy in government e-mail by allowing personal use.³¹⁵ Soldiers use their government e-mail for personal use with permission from the government. The Army has even touted AKO as a means for Soldiers to communicate with their families by offering spouses e-mail addresses and informing Soldiers how to send video messages with their e-mail accounts.³¹⁶ The Army and the other services recognize the need to protect privileged communications contained in government e-mail as well.³¹⁷ A reasonable Soldier could believe he has an expectation of privacy in his government e-mail because the government allows him to use his government e-mail for personal communications, gives his spouse a government e-mail account, and then allows him to maintain privilege in protected communications. The innocuous log-in banner, even if one assume this is a valid consent to monitoring, loses its effectiveness in waiving any expectation of privacy by promoting policies that run counter to it.

Prior to the decision in *Long II*, the Army specifically ensured that Soldiers had a reasonable expectation of privacy from law enforcement during systems monitoring.³¹⁸ The monitoring policy was consistent with an inspection under MRE 313; an inspection directed at everyone using the network and subjecting everyone to the same level of scrutiny. Since the decision in *Long II*, the Army has focused the monitoring policy on gathering evidence against an individual instead of protecting the network. By changing its policy, the Army is now violating the holding in *O'Connor v. Ortega*³¹⁹ and *Ferguson v. City of Charleston*.³²⁰ The Army's computer monitoring policy has now become a tool for law enforcement instead of a legitimate inspection to ensure the health of the computer network.

A system administrator should have considerable discretion to monitor a computer network to ensure it is operating properly. However, the involvement of law enforcement in computer monitoring raises Fourth Amendment issues.³²¹ The simplest solution is to prohibit any personal use of government computer systems and not recognize any privilege for material sent over government computer networks. This will likely not happen. Often e-mail is the only means of communications for deployed Soldiers. Additionally, it is not practical to forbid e-mail for personal use as it is the predominant means of communication, especially with younger Soldiers.³²² By permitting the personal use of a government

³⁰⁷ See Stored Wired and Electronic Communications and Transactional Records Access, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701-2712).

³⁰⁸ DODD 5505.9, *supra* note 148.

³⁰⁹ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

³¹⁰ See *supra* note 117 and accompanying text.

³¹¹ See 18 U.S.C.S. § 2702(b) (LexisNexis 2008).

³¹² See *supra* notes 125-39 and accompanying text for a more detailed discussion.

³¹³ 18 U.S.C.S. § 2708; see also *United States v. Allen*, 53 M.J. 402 (C.A.A.F. 2000) (holding that the SCA does not provide for a suppression remedy). *But see McVeigh v. Cohen*, 983 F. Supp. 215 (D.C. Cir. 1998).

³¹⁴ *McVeigh*, 983 F. Supp. 215 (enjoining the discharge of a homosexual Sailor because the information on which the discharge was based was obtained in violation of the SCA).

³¹⁵ See *JER*, *supra* note 27, § 2-301; AR 25-1, *supra* note 3, para. 6-1e.

³¹⁶ Army Knowledge Online, <https://www.us.army.mil> (follow "Inside AKO" hyperlink, then follow "AKO Video Messaging" hyperlink) (last visited Oct. 9, 2008).

³¹⁷ See *Herthel e-mail*, *supra* note 230; *Figueroa*, *supra* note 230.

³¹⁸ AR 25-2 (2003), *supra* note 6, para. 4-5r(2).

³¹⁹ 480 U.S. 709 (1987).

³²⁰ 532 U.S. 67 (2001).

³²¹ See *Coacher*, *supra* note 24, at 156. See generally *Long II*, 64 M.J. 57 (C.A.A.F. 2006) (holding that there is a reasonable expectation of privacy in a government e-mail account).

³²² See *Freiwald & Bellia*, *supra* note 65, at 568.

e-mail account, issues involving a reasonable expectation of privacy will always exist. The best course of action might be to revert to a systems monitoring policy that relies on the holding of *O'Connor v. Ortega*³²³ and MRE 313 to ensure that evidence acquired during monitoring is admissible at trial.³²⁴

Until a new systems monitoring policy is developed, the best practice for criminal cases is to obtain a search authorization before viewing information residing on a government e-mail server.³²⁵ A search authorization only requires probable cause.³²⁶ In *United States v. Leedy*, the CAAF held that probable cause requires more than just a bare suspicion, but less than a preponderance of the evidence.³²⁷ With such a low threshold, a good practice would be to attain a search authorization if law enforcement believes that evidence of criminal conduct exists in a Soldier's e-mail messages. In addition to preventing the suppression of evidence, this practice demonstrates that the military justice system is fair.³²⁸ The prudent law enforcement agent will proceed only with a search authorization, despite the new e-mail monitoring policy, prior to viewing e-mail on a government server.

IX. Conclusion

It is uncertain whether the CAAF will continue to recognize a reasonable expectation of privacy in a government e-mail account or limit the impact of *Long II* to its facts. The CAAF has recently affirmed two cases from the Air Force Court of Appeals³²⁹ that on their face seem to conflict with *Long II*.³³⁰ Both cases are distinguishable from *Long II*. Neither case dealt with e-mail seized from a government server nor enforced workplace practices that created a reasonable expectation of privacy as they did in *Long II*.³³¹ As e-mail use continues to expand, the number of criminal cases involving evidence acquired from a government computer network will increase. The recognition of a reasonable expectation of privacy in electronic communications will continue to be a contested issue.

Even though decided on a very specific set of facts, the decision in *Long II* creates new privacy rights by recognizing a reasonable expectation of privacy in government e-mail. The Army has reacted by creating policies that try to erase the privacy rights created by the CAAF's decision in *Long II*. The Army's attempt to remove any expectation of privacy has transformed a legitimate computer network monitoring program into a law enforcement tool. Once the CAAF recognized a reasonable expectation of privacy in e-mail stored on a government server, policies and regulations denying the existence of this privacy expectation have missed the mark.

³²³ 480 U.S. 709 (1987).

³²⁴ This could be accomplished by rescinding the current version of AR 25-2 and adopting the policies put in place under the 2003 version of AR 25-2.

³²⁵ This is recommended by both the Navy and Air Force. See e-mail from Deputy Assistant Judge Advocate Gen. (Criminal Law) to All Navy and Marine Corps Judge Advocates, subject: Search Authorizations for Computer Files in Light of *United States v. Long*, 64 M.J. 57 (2006), Part II (1 June 2007) (on file with author); General Counsel of the Air Force, *Expectation of Privacy in Computer Systems: Follow-Up*, GEN. COUNSEL'S Q., Apr. 2007; see also Lieutenant Colonel John T. Soma et al., *Computer Crime: Substantive Statutes & Technical & Legal Search Considerations*, 39 A.F. L. REV. 225, 225-26 (1996).

³²⁶ MCM, *supra* note 54, MIL. R. EVID. 315(a).

³²⁷ 65 M.J. 208, 213 (C.A.A.F. 2007) (holding that there is no specific probability required to establish probable cause, but it is based on common sense that a crime has occurred). The current Air Force policy only requires "individualized suspicion" that a user engaged in criminal behavior. Air Force Gen. Counsel Memo, *supra* note 271. To search the user's e-mail account requires permission from someone authorized to issue a search authorization. *Id.* (citing U.S. DEP'T OF AIR FORCE, INSTR. 33-129, WEB MANAGEMENT AND INTERNET USE (3 Feb. 2005)). While not a search authorization, it is the practical equivalent.

³²⁸ President Lyndon Johnson believed that the top priority of the military justice system was to ensure a perception of fairness. Walter T. Cox III, *The Army, the Courts, and the Constitution: The Evolution of Military Justice*, 118 MIL. L. REV. 1, 19 (1987) (referencing comments made by President Johnson on the enactment of the Military Justice Act of 1968, Pub. L. No. 90-632, 82 Stat. 1335).

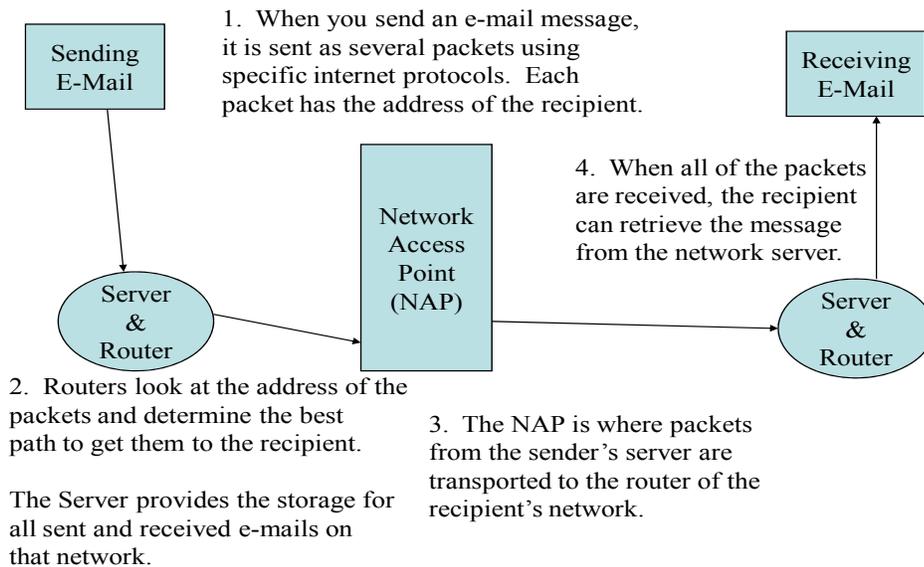
³²⁹ See *United States v. Larson*, 64 M.J. 559 (A.F. Ct. Crim. App. 2007) (finding the appellant had no reasonable expectation in privacy in data stored computer when he knew that computer would be turned over to another officer upon his return from deployment); *United States v. Rutherford*, 2007 CCA LEXIS 262 (A.F. Ct. Crim. App. June 19, 2007) (affirming the military judge's ruling that the appellant lacked a subjective expectation of privacy in e-mails stored on his government computer and holding that the e-mails would have been admissible under the theory of inevitable discovery).

³³⁰ *United States v. Larson*, 66 M.J. 212 (C.A.A.F. 2008); *United States v. Rutherford*, 2008 CAAF LEXIS 639 (May 27, 2008).

³³¹ *Larson*, 66 M.J. at 215-16 (holding that Appellant's activity was illegal, he was put on notice, he had consented to monitoring of activities that were illegal, and Appellant's commander could log onto the computer to access the seized material); *United States v. Rutherford*, 2007 CCA LEXIS 262 (finding that the e-mails were stored on the hard drive and were viewed by an Airman performing maintenance on the computer).

Appendix A

How E-mail is Delivered³³²



Electronic mail allows for an exchange of information between computers using telephone and cable lines.³³³ Packet switching allows this to occur.³³⁴ Data is broken into smaller pieces, i.e., packets, and sent out to its destination.³³⁵ It is not necessary for each of these packets to travel the same route.³³⁶ This allows computers to talk with one another without a direct connection.³³⁷ This electronic communication occurs in various forms such as e-mails, web surfing, chat rooms, and bulletin boards. Electronic mail messages routed through and stored on an ISP's server until the recipient to collect them.³³⁸ However, the e-mail, even after delivery, remains on the ISP's server as a back up.³³⁹

³³² PRESTON GRALLA, THE INTERNET WORKS 11, 89-90 (1999).

³³³ David T. Cox, *Litigating Child Pornography and Obscenity Cases in the Internet Age*, 4 J. TECH. L. & POL'Y 1 para. 83 (Summer 1999).

³³⁴ *Id.* para. 84.

³³⁵ *Id.* para. 83.

³³⁶ *Id.* para. 85.

³³⁷ *Id.*

³³⁸ *Id.*

³³⁹ Mulligan, *supra* note 59, at 1562-63.

Appendix B

The Stored Communications Act³⁴⁰

Status	Voluntary Disclosure Public ISP	Voluntary Disclosure Nonpublic ISP	Compelled Disclosure Public ISP	Compelled Disclosure Nonpublic ISP
Unopened e-mail in storage for less than 180 days	No unless § 2702(b) Applies	Yes § 2702(a)(1) Applies	Search Warrant § 2703(a)	Search Warrant § 2703(a)
Unopened e-mail in storage for 180 days or more	No unless § 2702(b) Applies	Yes § 2702(a)(1) Applies	Subpoena with notice, § 2703(d) order, search warrant	Subpoena with notice, § 2703(d) order, search warrant
Opened e-mail or other content	No unless § 2702(b) Applies	Yes § 2702(a)(2) Applies	Subpoena with notice, § 2703(d) order, search warrant	SCA does not apply § 2711(2)
Most Non-content Records	No unless § 2702(c) Applies	Yes § 2702(a)(3) Applies	§ 2703(d) order, search warrant	§ 2703(d) order, search warrant
Basic session logs, subscriber information	No unless § 2702(c) Applies	Yes § 2702(a)(3) Applies	Subpoena, § 2703(d) order, search warrant	Subpoena, § 2703(d) order, search warrant

³⁴⁰ KERR, *supra* note 116, at 507.

Appendix C

Attorney-Client Privilege

“System protection monitoring also raises policy issues when the system is used to transmit protected communications.”³⁴¹ The *Manual for Courts-Martial* provides that communications between certain parties are privileged in nature and not admissible at courts-martial.³⁴² These communications are inadmissible as long as they remain confidential.³⁴³ Army Regulation 27–26, *Rules of Professional Conduct for Lawyers*, also imposes an ethical duty on an attorney to maintain confidentiality in communications between him and his client.³⁴⁴ The use of e-mail to communicate with a client and the monitoring of government networks may possibly violate an attorney’s ethical duty to provide confidential communications with his client.

Electronic mail has become an increasingly preferred method for attorneys to communicate with clients; because of this, several state bar associations have issued ethics opinions that address this issue.³⁴⁵ The Army Rules for Professional Conduct give limited guidance on communications over e-mail.³⁴⁶ The discussion to Rule 1.6 cautions Judge Advocates to “strive to avoid” unauthorized persons from overhearing conversations and to scrutinize access by others to automation equipment.³⁴⁷ The American Bar Association (ABA) has concluded that confidentiality will be maintained if the lawyer communicates with a client through e-mail.³⁴⁸ The ABA has concluded that from a technological and legal standpoint, e-mail has progressed as a means of communication that has a reasonable expectation of privacy.³⁴⁹ While e-mail is subject to intercept or retrieval by a third party, this does not diminish its confidentiality because every form of communication is subject to interception.³⁵⁰

Unsettled is the issue with electronic communications over a government network where the user has consented to monitoring of his e-mail.³⁵¹ The discussion to Army Rule 1.6 raises this issue, but provides no guidance.³⁵² This issue exists in the ongoing trial of LCpl Tatum in a motion to prevent the USMC from monitoring e-mails between the attorneys and the accused.³⁵³ Lance Corporal Tatum’s civilian defense attorney claims that communicating with the client by e-mail violates the attorneys’ ethical duties under Navy Professional Rules of Conduct and their State Bar rules.³⁵⁴ Lieutenant Colonel Colby Vokey³⁵⁵ stated that “by using the computer, you are almost violating the state and military ethics rules on confidentiality.”³⁵⁶ The claims by LCpl Tatum’s defense team center on the fact that the Marine Corps has unfettered access to e-mail communications between attorney and client, and the accused and his attorneys would be unaware if the government were to view their e-mails.³⁵⁷ Army Regulation 380-53 instructs system administrators to avoid monitoring communications protected by privilege.³⁵⁸ Lance Corporal Tatum’s defense team also cites the USMCs’ policy³⁵⁹ that

³⁴¹ Coacher, *supra* note 24, at 183.

³⁴² MCM, *supra* note 54, MIL. R. EVID. 501–04, 513.

³⁴³ *Id.* There are exceptions to each of these privileges. *Id.*

³⁴⁴ U.S. DEP’T OF ARMY, REG. 27-26, RULES OF PROFESSIONAL CONDUCT FOR LAWYERS R. 1.6 (1 May 1992) [hereinafter AR 27-26].

³⁴⁵ Matthew J. Boettcher & Eric G. Tucciarone, *Concerns over Attorney-Client Communication Through E-Mail: Is the Sky Really Falling?*, 2002 L. REV. M.S.U.-D.C.L. 127, 138 (Spring 2002).

³⁴⁶ AR 27-26, *supra* note 344, R. 1.6 discussion.

³⁴⁷ *Id.*

³⁴⁸ See Am. Bar Ass’n Comm. on Ethics and Prof’l Responsibility, Formal Op. 99–413 (1999).

³⁴⁹ *Id.*

³⁵⁰ See *id.*

³⁵¹ Boettcher & Tucciarone, *supra* note 345, at 140 n.70 (citing Conn. Bar Ass’n, Op. 99–52 (1999)).

³⁵² AR 27-26, *supra* note 344, R. 1.6 discussion.

³⁵³ Teri Figueroa, *Lawyers Fret Over Military Computer Snooping*, N. COUNTY TIMES, Dec. 31, 2007, http://www.nctimes.com/articles/2008/01/01/news/top_stories/21_42_7312_31_07.prt.

³⁵⁴ Motion for Appropriate Relief (For Injunctive Relief from Warrantless Intrusion into Attorney-Client Privileged Information on Computer of Defense Counsel), *United States v. Tatum* (Western Jud. Cir. N-M. Trial Judiciary Dec. 14, 2007) [hereinafter Tatum Motion].

³⁵⁵ United States Marine Corps, Regional Defense Counsel, Western Region.

³⁵⁶ Figueroa, *supra* note 353.

³⁵⁷ Tatum Motion, *supra* note 354.

³⁵⁸ AR 380-53, *supra* note 3, para. 2-10i.

implements the DOD Chief Information Operations new policy on scope of consent to systems monitoring.³⁶⁰ However, they fail to mention that this policy states that it will have no effect on a privilege recognized by law.³⁶¹ Although this issue has not been settled by the Army Rules of Professional Conduct or by a formal opinion from the Office of the Standards of Conduct, an Army defense counsel is likely not violating his ethical duty by communicating with his client via a government e-mail account.

The MRE recognize several forms of protected communication that arise to a testimonial privilege.³⁶² These include communications to clergy,³⁶³ husband-wife privilege,³⁶⁴ psychotherapist-patient privilege,³⁶⁵ and attorney-client privilege.³⁶⁶ To invoke the attorney-client privilege recognized under MRE 502, the communication must be confidential and made for the purpose of seeking legal advice.³⁶⁷ The intended recipient of the communication must be the attorney, client, or an agent of the attorney.³⁶⁸ The CAAF has held if there is any doubt that the intent of the communication was to be confidential, it should be resolved in favor of the accused.³⁶⁹ This is consistent with the decision in *United States v. Noriega*.³⁷⁰ Manuel Noriega, the former President of Panama, made several calls to his attorney on the phone outside of his cell where he was detained pending trial.³⁷¹ The court held Noriega had a reasonable expectation of privacy in his conversations with his attorneys due the confusion surrounding the scope of the monitoring of telephone calls.³⁷² This could be applicable to the guidance provided by the Army and DOD.

The scarce references to the recognition of privilege by Army regulation and DOD guidance may save the day for maintaining any privilege for information passed over a government computer network. Brigadier General James Walker³⁷³ stated, ““The key aspect of the revision is to make certain that we maintain the protections of privileged communications . . . ? within . . . the Department of Defense.”³⁷⁴ Additionally, even if the system administrator does view privileged information during his monitoring function, this would not defeat the claim of confidentiality.³⁷⁵

A military attorney does not violate his ethical duties nor does a client waive his attorney-client privilege by communicating via a government e-mail account. There are steps a military attorney can do to protect himself from ever having to defend this issue. The attorney must familiarize himself with his licensing state. While governed by the Army Rules of Professional Conduct, he also has a duty not to violate the rules of the state in which he admitted to practice.³⁷⁶ It would behoove the attorney to get consent to communicate via e-mail after explaining the possibility to his client that his e-

³⁵⁹ Tatum Motion, *supra* note 354 (citing Message, 060014Z Dec 07, Commandant Marine Corps, subject: Mandatory Requirement to Use Standard Department of Defense Information Systems (IS) Consent Banner and User Agreement).

³⁶⁰ CIO Memo I, *supra* note 232. This policy is on temporary hold. CIO Memo II, *supra* note 232.

³⁶¹ Tatum Motion, *supra* note 354; *see also* CIO Memo I, *supra* note 232.

³⁶² MCM, *supra* note 54, MIL. R. EVID. 501–04, 513.

³⁶³ *Id.* MIL. R. EVID. 503.

³⁶⁴ *Id.* MIL. R. EVID. 504.

³⁶⁵ *Id.* MIL. R. EVID. 513.

³⁶⁶ *Id.* MIL. R. EVID. 502.

³⁶⁷ *Id.* MIL. R. EVID. 502(a). “(1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client . . .” are protected as part of the attorney-client relationship. *United States v. Spriggs*, 48 M.J. 692, 695 (A. Ct. Crim. App. 1998) (quoting *United States v. McCluskey*, 20 C.M.R. 261, 267 (C.M.A. 1955) (citation omitted)).

³⁶⁸ MCM, *supra* note 54, MIL. R. EVID. 502.

³⁶⁹ *United States v. Rust*, 41 M.J. 472, 479 (C.A.A.F. 1995) (citing *United States v. Gandy*, 26 C.M.R. 135, 141 (A.B.R. 1958)).

³⁷⁰ 764 F. Supp. 1480 (S.D. Fla. 1991).

³⁷¹ *Id.* at 1482–83. Contrary to prison policy, prison officials advised Noriega that calls to his attorneys were not monitored. *Id.* at 1482–87.

³⁷² *Noriega*, 764 F. Supp. at 1487. The court warned that there would have been no expectation of privacy had Noriega been aware that his calls to his attorneys were monitored. *Id.* at 1487–89.

³⁷³ Staff Judge Advocate to the Commandant, U.S. Marine Corps.

³⁷⁴ Figueroa, *supra* note 230 (referring to Memorandum from Dep’t of Def. Chief Info. Officer to Secretaries of the Military Dep’ts et. al., subject: Policy on Department of Defense Information Systems—Standard Consent Banner and User Agreement (2 Nov. 2007)). This policy is on temporary hold. CIO Memo II, *supra* note 232.

³⁷⁵ Coacher, *supra* note 24, at 185 n.182 (citing *United States v. Noriega*, 917 F.2d 1543, 1551 n.10 (11th Cir. 1990)).

³⁷⁶ AR 27-26, *supra* note 344, para. 4a(3).

mail might be subject to monitoring and the alternative means of communications. “Such a process not only keeps the client reasonably informed to make the decision to use e-mail, but protects the attorney” from violating his ethical duties.³⁷⁷ The attorney could also place the words “Attorney-Client Privilege” in the subject line of any e-mail containing privileged material.³⁷⁸ This should put the system administrator on notice of the privilege and even if turned over to law enforcement it would put them on notice as well.³⁷⁹ The defense attorney could also work with the system administrator to ensure that he understands the reasons not to disclose the defense attorney’s e-mail. These proactive steps will help prevent the cat from ever getting out of the bag.

³⁷⁷ Boettcher & Tucciarone, *supra* note 345, at 146–47.

³⁷⁸ Alternatively, you could place this warning in the body of the e-mail:

ATTENTION: This transmission may contain attorney work-product or information protected under the attorney-client privilege, which is protected from disclosure under 5 USC § 552. Do not release outside of DoD channels without prior authorization from the sender. If you have received this message in error, please notify the sender immediately by telephone and delete this message. Thank you.

³⁷⁹ Coacher, *supra* note 24, at 188 n.195.

It might be advisable for attorneys and their clients who use e-mail to communicate to clearly label any messages containing confidences. For example, most e-mail programs allow for a subject line. Similar to labels placed on most legal office FAX cover sheets, a smart attorney will use this subject line to label a confidential message as "Attorney-Client Information." This would put a system administrator on notice that the information contained in the message is protected and should not be further monitored or released.

Id.