COMMUNICATIONS PRIVACY IN THE MILITARY

Justin Holbrook[†]

TABLE OF CONTENTS

---

† Associate Professor of Law and Director of Veterans Law Clinic, Widener University School of Law. J.D. Harvard Law School (2001); B.A.L.S Georgetown University (1998). The author wishes to thank Grant Wahlquist and Drew Brown for their invaluable assistance with this article.

I. INTRODUCTION

> The warrant is to seize all the plaintiff's books and papers without exception, and carry them before Lord Halifax; what? Has a Secretary of State a right to see all a man's private letters of correspondence, family concerns, trade and business? This would be monstrous indeed; and if it were lawful, no man could endure to live in this country.[1]

It is axiomatic that subjective expectations of privacy must be objectively reasonable to warrant constitutional protections under the Fourth Amendment.[2] When it comes to computers in the workplace, proponents of robust privacy expectations face difficult battles on both the subjective and objective fronts. As a question of fact, at least three (and probably many more) factors diminish subjective privacy expectations in workplace electronic communications[3]: the public nature of work environments, the technical oversight of network administrators, and the ubiquity of employee notices in handbooks, user agreements, and logon banners. As a question of law, the operational realities of the workplace and the need for employer oversight further encumber objectively reasonable privacy expectations.[4]

In the context of the federal workplace, such subjectively held and objectively reasonable privacy expectations in electronic communications

1. Entick v. Carrington, 95 Eng. Rep. 807 (K.B. 1765) (recounting plaintiff's response to defendants' arguments).

2. *See* Minnesota v. Olson, 495 U.S. 91, 95 (1990); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

3. For purposes of this Article, the term "communications" specifically refers to electronic communications, including e-mail, chat, and instant messaging.

4. *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (quoting Tri-State Steel Constr., Inc. v. Occupational Safety & Health Review, 26 F.3d 173, 176 (D.C. Cir. 1994)) (observing subjective expectations of privacy are questions of fact reviewed under clearly erroneous standard while objective expectations of privacy are questions of law subject to de novo review).

appear even more incredible, especially if that federal workplace happens to be within the U.S. military. That constitutional protections are colored by the nature of military service is well-settled law.[5] What service member, therefore, could honestly and reasonably believe that a government computer issued for official use by the military provides even a sliver of privacy expectation?

As it turns out, the issue is one of deceptive simplicity. Like courts elsewhere, military courts have struggled to find an articulable standard with which to analyze Fourth Amendment electronic privacy issues. This difficulty is partly due to the factual differences between electronic privacy cases which, when painted with the broadest of brushes, appear factually similar, but whose technological distinctions justify different subjective and objective privacy expectations. It is partly due to the ferment engendered by courts applying Fourth Amendment jurisprudence to evolving technologies. And it is also partly due to the unique legal standards applied to the military by virtue of its history, customs, and statutory authority to both supervise and self-police its members.

Weaving these concerns into a coherent analytical model is no easy task. At issue is a straightforward question cloaked in complexity: Do service members have a legitimate expectation of privacy in their workplace electronic communications? Following from this question are others. If privacy expectations are justified, how much privacy? Would the acknowledgment of some measure of privacy degrade the military's operational effectiveness? What about its ability to self-police remotely deployed members who commit criminal misconduct using government information systems?

In exploring these questions, I draw on a line of cases issued by the Court of Appeals for the Armed Forces (CAAF)[6] grappling with service members' communications privacy expectations, including *United States v.*

---

5. For a discussion of the applicability of the Bill of Rights to military service members, see *infra* Section II.B.

6. The United States Court of Appeals for the Armed Forces (CAAF), an Article I court created by Congress, functions as "the supreme court of the military judicial system." United States v. Rorie, 58 M.J. 399, 403 (C.A.A.F. 2003) (quoting McPhail v. United States, 1 M.J. 457, 462 (C.M.A. 1976)). The court is composed of five civilian judges appointed for 15-year terms by the President with the Senate's advice and consent. *Id.* Prior to its current designation, the CAAF was known as the Court of Military Appeals (1950–1968) and the United States Court of Military Appeals (1968–1994). THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES (2006), *available at* http://www.armfor.uscourts.gov/CAAFBooklet2006.pdf; *see also* Karen A. Ruzic, Note and Comment, *Military Justice and the Supreme Court's Outdated Standard of Deference: Weiss v. United States*, 70 CHI.-KENT L. REV. 265, 276–77 (1994) (discussing congressional motivation behind changing the CAAF's name).

Long[7] and *United States v. Larson*,[8] two cases that have caused widespread concern throughout the Department of Defense (DoD).[9] I also reflect on the possibility that the nature of military service itself warrants both subjective and objective expectations of privacy in workplace communications. On the one hand, the unique realities of military service justify diminished privacy expectations in everything from garrison barracks to government e-mail accounts.[10] On the other hand, the dislocation of military members from friends and family by virtue of their military service arguably creates an inescapable user reliance on military resources to communicate with the outside world. This reliance forces the military to acknowledge that government information systems may, in fact, be used for more than official use, which could create both a subjective and objective expectation of privacy in any personal use.[11]

This Article's argument proceeds in three steps. First, the Article considers Fourth Amendment jurisprudence and how it applies to military members in the workplace. Several principles are distilled from this jurisprudence to mark the contours of communications privacy in the

7. 64 M.J. 57 (C.A.A.F. 2006).

8. 66 M.J. 212 (C.A.A.F. 2008).

9. *See, e.g.*, Lawrence A. Edell, *A Reasonable Expectation of Privacy: Is a Government E-mail Account the Equivalent of a Wall Locker in a Barracks Room?*, 2008 ARMY LAW. 1, 2 (2008) (observing that the CAAF's decision in *Long* created DoD concern regarding "the ability to monitor its computer networks"); Jamie L. Mendelson, *Government Computers and Email—Get the Search Authorization!*, 3 JAJG PERSP. 9 (2008) (discussing post-*Larson* search authorization for service members' workplace e-mails and computers); U.S. DEP'T OF AIR FORCE, INSTRUCTION 51-201, ADMINISTRATION OF MILITARY JUSTICE § 13.13.2.2 (2010) [hereinafter AFI 51-201] (noting the unsettled nature of electronic privacy law after *Long* and *Larson* and encouraging officials to "consider obtaining search authorization for cases involving alleged criminal activity").

10. For a discussion of the applicability of the service members' privacy expectations under the Fourth Amendment, see *infra* Section II.E.

11. Because of the nature of military service, and in accordance with the Joint Ethics Regulation (JER), military service regulations allow limited personal use of official information systems. *See* U.S. DEP'T OF DEFENSE, DIR. 5500.7R, JOINT ETHICS REGULATION § 2-301 (Nov. 29, 2007); U.S. DEP'T OF AIR FORCE, INSTRUCTION 33-129, WEB MANAGEMENT AND INTERNET USE § 2-1 (2005) ("Appropriate officials may authorize personal uses . . . ."); U.S. DEP'T OF ARMY, ARMY REG. 25-1, ARMY KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY para. 6-1.d(5) (2008) ("Official use includes health, morale, and welfare (HMW) communications by military members and DoD employees who are deployed in remote or isolated locations for extended periods of time on official DoD business."); Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DoD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 184–88 (2009) (discussing JER and noting it authorizes commanders "to permit DoD personnel at a normal workplace to conduct brief internet searches beyond matters involving official business or family communications").

military. Second, the Article considers Fourth Amendment protections in the context of electronic communications, working through the seminal Supreme Court decisions, the congressional enactment of the Stored Communications Act, and the CAAF's communications privacy cases. Finally, the Article reviews the DoD's response to the CAAF's communications privacy cases and explore how a normative inquiry could assist the CAAF in situating service members' communications privacy rights in the context of traditional Fourth Amendment jurisprudence. The Article concludes by suggesting that military courts adopt an analytical framework that explicitly distinguishes between work-related and law enforcement searches in determining the degree of communications privacy properly afforded service members.

II. FIRST PRINCIPLES OF PRIVACY IN THE MILITARY WORKPLACE

This Part reviews Fourth Amendment jurisprudence and discusses how that jurisprudence has been applied in the public workplace generally and the military workplace specifically. This Part addresses the relevant portions of the Military Rules of Evidence (MRE), which distinguish between searches for work-related and law enforcement purposes, and analyzes federal workplace case law, which similarly distinguishes between work-related and law enforcement searches. Distilled from this discussion are several principles of military workplace privacy which, when considered in light of electronic communications, provide critical guidance in determining what level of electronic communications privacy service members should receive.

A. THE TOUCHSTONE OF FOURTH AMENDMENT ANALYSIS

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[12] Warrants must issue upon "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."[13] For purposes of the Fourth Amendment, a "search" is conducted when the government, acting on its own or through an authorized agent, intrudes into a person's "constitutionally protected reasonable expectation of privacy."[14] The

12. U.S. CONST. amend. IV.

13. *Id.*

14. California v. Ciraolo, 476 U.S. 207, 211 (1986) (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)); *see also* Soldal v. Cook County, 506 U.S. 56, 63 (1992) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)) ("A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."); United States v. Daniels, 60 M.J. 69, 71 (C.A.A.F. 2004) ("The Supreme Court defines a

Supreme Court highlighted this emphasis on privacy rights, as opposed to property rights, in Fourth Amendment analysis as early as 1967 when it observed in *Warden v. Hayden* that "[w]e have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property . . . . This shift in emphasis from property to privacy has come about through a subtle interplay of substantive and procedural reform."[15] An individual's reasonable expectation of privacy now serves as the "touchstone" of Fourth Amendment inquiry.[16]

To determine whether an individual's privacy expectations are constitutionally protected, courts generally apply a two-part test, first articulated by Justice Harlan in his concurring opinion in *Katz v. United States*, a case involving the expectation of privacy in telephone calls.[17] Observing that "the Fourth Amendment protects people, not places," Justice Harlan conceived a sliding scale of protections, in which the appropriate level of protection is determined by inquiring (1) whether the person involved has a subjective (actual) expectation of privacy, and (2) whether that expectation is objectively reasonable.[18] A privacy expectation is objectively reasonable if it is "one that society is prepared to recognize as 'reasonable.' "[19] The first query is a question of fact, while the second is a matter of law.[20]

Importantly, situations exist in which the two-part *Katz* inquiry may be inadequate. Writing for the majority in *Smith v. Maryland*, Justice Blackmun commented:

> [f]or example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. . . . In such circumstances, where an

---

Fourth Amendment 'search' as a government intrusion into an individual's reasonable expectation of privacy.").

15. 387 U.S. 294, 304 (1967) (internal citations omitted); *cf. Soldal*, 506 U.S. at 64 (observing that, although protection of privacy is "principal" object of contemporary Fourth Amendment jurisprudence, protection of property remains integral).

16. *Ciraolo*, 476 U.S. at 211.

17. 389 U.S. at 361.

18. *Id.*; *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) (discussing *Katz* and noting that a subjective expectation exists when an individual "seeks to preserve [something] as private" and an objective expectation exists when, "viewed objectively, [it] is 'justifiable' under the circumstances" (internal quotation marks omitted) (citations omitted)).

19. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also* Minnesota v. Olson, 495 U.S. 91, 95–96 (1990).

20. United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (quoting Tri-State Steel Construction Inc. v. Occupational Safety & Health Review Comm'n, 26 F.3d 173, 176 (D.C. Cir. 1994)).

> individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[21]

Justice Blackmun's comment underscores the importance of basing Fourth Amendment protections on normative valuations of what should be protected rather than simply what is protected, especially when the government may have sought to perform an end-run around Fourth Amendment privacy expectations by issuing blanket pronouncements of prescribed intrusions.[22] Even in Katz, in which the facts supported the Court's two-pronged inquiry, the core holding rested on a normative judgment that an individual placing a telephone call "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[23] Such normative judgments, as discussed in Section IV.C below, continue to play a critical role in evaluating society's expanding reliance on communications technologies.[24]

---

21. 442 U.S. at 741 n.5. In *Smith*, the Supreme Court held that using a "pen register" to record a dialed phone number did not violate the Fourth Amendment because individuals "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. For an excellent discussion of how *Smith* applies to electronic communications, see Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2110 (2009) ("Perhaps the most practically significant of these unresolved questions is whether novel categories of Internet communications data, such as e-mail subject lines, website Uniform Resource Locators (URLs), and website IP addresses should be protected as the contents of electronic communications, or whether they should be treated as noncontent 'envelope' information."). In *Larson*, it was precisely this "novel" internet information which law enforcement agents seized and which the trial court admitted. *See infra* Section III.C.4.

22. Professor Susan Freiwald has observed that one of the Framers' motivations for the Fourth Amendment was their concern about the government issuing blanket pronouncements in the form of general warrants. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 59 (2007); *see also* Berger v. New York, 388 U.S. 41, 64 (1967) (striking down New York's wiretapping statute as violating the Fourth Amendment's particularity requirement similar to a general warrant); *infra* Section IV.B.1 (discussing how the DoD's mandatory logon banner functions like a general warrant).

23. *Katz*, 389 U.S. at 352.

24. *See infra* Section IV.C; *see also* Freiwald, *supra* note 22, at 29 (discussing *Katz* court's normative acknowledgment of "vital role that the public telephone has come to play in private communications" and comparing it with vital role of e-mail in contemporary society).

B. THE MILITARY AND CONSTITUTIONAL PROTECTIONS

Constitutional protections "take on a different complexion" when applied to members of the military.[25] As the Supreme Court observed in *Parker v. Levy*, "the different character of the military community and of the military mission requires a different application of those protections. The fundamental necessity for obedience, and the consequent necessity for imposition of discipline, may render permissible within the military that which would be constitutionally impermissible outside of it."[26] Courts have observed this alternate constitutional complexion in the context of the First Amendment,[27] Fifth Amendment,[28] Sixth Amendment,[29] Seventh Amendment,[30] and, as discussed in this Article, the Fourth Amendment.[31]

---

25. *See* United States v. Allen, No. ACM 32727, 1999 CCA LEXIS 116, at *11 (A.F. Ct. Crim. App. Apr. 22, 1999). Jurists have long recognized the distinctive nature of military service. *See, e.g.*, *In re* Grimley, 137 U.S. 147, 153 (1890) ("An army is not a deliberative body. It is the executive arm. Its law is that of obedience. No question can be left open as to the right to command in the officer, or the duty of obedience in the soldier."). This distinction implicates the color and scope of constitutional protections. *See* Solorio v. United States, 483 U.S. 435, 447–48 (1987) (discussing constitutional protections for military members); Parker v. Levy, 417 U.S. 733, 758 (1974) (same).

26. 417 U.S. at 758.

27. *See, e.g.*, *id.* at 761 (holding speech of commissioned officer urging enlisted personnel to refuse to obey orders not protected under First Amendment); United States v. Forney, 67 M.J. 271, 274–75 (C.A.A.F. 2009) (holding virtual child pornography not protected under military law even if protected under First Amendment in civilian society); *see also* John A. Carr, *Free Speech in the Military Community: Striking a Balance Between Personal Rights and Military Necessity*, 45 A.F. L. REV. 303 (1998); Katherine C. Den Bleyker, *The First Amendment versus Operational Security: Where Should the Milblogging Balance Lie?*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 401 (2007); David E. Fitzkee & Linell A. Letendre, *Religion in the Military: Navigating the Channel Between the Religion Clauses*, 59 A.F. L. REV. 1 (2007).

28. *See, e.g.*, Weiss v. United States, 510 U.S. 163, 177 (1994) (holding due process under Fifth Amendment differs in military); *Ex parte* Quirin, 317 U.S. 1, 40 (1942) (noting Fifth Amendment explicitly excepts "cases arising in the land or naval forces"); United States v. Culp, 14 C.M.A. 199, 205 (C.M.A. 1963) ("[N]either has the Supreme Court held that all of the rights covered by the Fifth and Sixth Amendments apply to those in the military.").

29. *See, e.g.*, *Quirin*, 317 U.S. at 40 (noting Sixth Amendment exempts by implication "cases arising in the land or naval forces"); United States v. Witham, 47 M.J. 297, 301 (C.A.A.F. 1997) (noting "a military accused has no Sixth Amendment right to trial by jury").

30. *See Culp*, 14 U.S.C.M.A. at 208 (observing Seventh Amendment right to trial by jury is limited to suits at common law, which does not include "suits in equity or proceedings in admiralty").

31. *See, e.g.*, Comm. for GI Rights v. Callaway, 518 F.2d 466, 476–77 (D.C. Cir. 1975) (holding warrantless inspections for drug abuse not violative of Fourth Amendment); United States v. McCarthy, 38 M.J. 398, 401 (C.M.A. 1993) ("Fourth Amendment requirement that a warrant be supported by oath or affirmation does not apply to searches and seizures by military authorities" (citation omitted)); United States v. Stuckey, 10 M.J. 347, 360–61 (C.M.A. 1981) (noting military commander, though not magistrate for Fourth Amendment

These provisional limitations flow from judicial recognition that Congress retains a plenary role "over rights, duties, and responsibilities in the framework of the Military Establishment, including regulations, procedures, and remedies related to military discipline[.]"[32] It is for this reason that the Supreme Court acknowledged that "[j]udicial deference . . . is at its apogee when reviewing congressional decisionmaking in this area."[33] In modern jurisprudence, it is settled law that the military is a "separate community" subject to congressional regulation with limited oversight by the federal judiciary.[34]

While military law limits certain rights, others are expanded beyond constitutional minimums by federal statutes, executive orders, federal case law, executive orders, or service regulations.[35] Two common examples include the right to counsel before special and general courts martial, regardless of the indigent circumstances of the accused,[36] and the requirement to administer warnings against self-incrimination, regardless of

---

purposes, may authorize searches).

32. Chappell v. Wallace, 462 U.S. 296, 301 (1983). As set forth in Art. I, § 8, the legislature has broad responsibility for both maintaining and directing the military:

> Congress shall have Power . . . To make Rules for the Government and Regulation of the land and naval Forces [and] to provide for organizing, arming, and disciplining, the Militia, and for governing such Part of them as may be employed in the Service of the United States . . . .

U.S. CONST. art. I, § 8; *see also* Solorio v. United States, 483 U.S. 435, 447–48 (1987) ("Congress has primary responsibility for the delicate task of balancing the rights of servicemen against the needs of the military. . . . [W]e have adhered to this principle of deference in a variety of contexts where, as here, the constitutional rights of servicemen were implicated.").

33. *Weiss*, 510 U.S. at 177 (citation omitted) (internal quotation marks omitted).

34. *See* Parker v. Levy, 417 U.S. 733, 743 (1974). The Court noted

> [t]his Court has long recognized that the military is, by necessity, a specialized society separate from civilian society. . . . The differences between the military and civilian communities result from the fact that "it is the primary business of armies and navies to fight or be ready to fight wars should the occasion arise."

Id. (quoting United States *ex rel.* Toth v. Quarles, 350 U.S. 11, 17 (1955)). For an insightful discussion of the "separate community" doctrine, see James M. Hirschhorn, *The Separate Community: Military Uniqueness and Servicemen's Constitutional Rights*, 62 N.C. L. REV. 177 (1984).

35. *See generally* Francis A. Gilligan, *The Bill of Rights and Service Members*, 1987 ARMY LAW. 3 (1987) (discussing Bill of Rights as applied to service members and arguing service members sometimes enjoy rights broader than those required by Constitution).

36. 10 U.S.C. § 838(b)(1) (2006) (providing that an "accused has the right to be represented in his defense before a general or special court-martial or at an investigation under [Article 32]" while implementing procedures for detailing defense counsel). Military defense counsel are provided without expense to the accused. *See, e.g.*, United States v. Culp, 14 U.S.C.M.A. 199, 202 (C.M.A. 1963) ("[N]o service man appears before a court-martial alone and there are no 'indigents' before courts-martial. Inevitably, by law, the accused before a court-martial appears with appointed counsel and no funds are required.").

the custodial nature of the interrogation.[37] The basis for this rights expansion is often that, although both visible and understandable within the canopy of contemporary legal society, the roots of American military jurisprudence predate the Constitution, the Articles of Confederation, and the American Revolution itself, finding their origin in Roman and British military tradition.[38] Military jurisprudence thus exists distinct and separate from the law governing Article III courts.[39]

---

37. Article 31(b) of the Uniform Code of Military Justice (UCMJ) provides that:

> [n]o person subject to this chapter may interrogate, or request any statement from, an accused or a person suspected of an offense without first informing him of the nature of the accusation and advising him that he does not have to make any statement regarding the offense of which he is accused or suspected and that any statement made by him may be used as evidence against him in a trial by court-martial.

10 U.S.C. § 831(b) (2006); *see also Culp*, 14 U.S.C.M.A. at 206 (discussing protections afforded service members under Bill of Rights and noting "[h]e cannot be compelled to be a witness against himself and that provision of the Fifth Amendment is preserved and expanded" (citations omitted)). Service members also have broader rights under the Eighth Amendment. *See* United States v. Matthews, 16 M.J. 354, 368 (C.M.A. 1983) ("[W]e have held that, in enacting Article 55, Congress 'intended to grant protection covering even wider limits' than 'that afforded by the Eighth Amendment.' " (quoting United States v. Wappler, 2 U.S.C.M.A. 393, 396 (C.M.A. 1953))).

38. *See Culp*, 14 U.S.C.M.A. at 205. For an introduction to the historical roots of the U.S. military legal system, see Ruzic, *supra* note 6, at 266–70.

39. *See generally* Note, *Military Justice and Article III*, 103 HARV. L. REV. 1909 (1990) (discussing military courts and their relationship to Article III courts). In *Burns v. Wilson*, 346 U.S. 137, 140 (1953), the Supreme Court rejected two applications for writs of habeas corpus from petitioners who had been convicted at court-martial of murder and rape and sentenced to death. In reviewing a civil court's power to review a military court-martial's judgment, the Supreme Court commented on the distinctive nature of military law:

> [m]ilitary law, like state law, is a jurisprudence which exists separate and apart from the law which governs in our federal judicial establishment. This Court has played no role in its development; we have exerted no supervisory power over the courts which enforce it; the rights of men in the armed forces must perforce be conditioned to meet certain overriding demands of discipline and duty, and the civil courts are not the agencies which must determine the precise balance to be struck in this adjustment. The Framers expressly entrusted that task to Congress.

Id. at 140 (internal citations omitted). The Supreme Court's reasoning echoed sentiments expressed nearly a century earlier in *Dynes v. Hoover*, 61 U.S. 65 (1857):

> [t]hese provisions show that Congress has the power to provide for the trial and punishment of military and naval offences in the manner then and now practiced by civilized nations; and that the power to do so is given without any connection between it and the 3d article of the Constitution defining the judicial power of the United States; indeed, that the two powers are entirely independent of each other.

Id. at 79; *cf. In re* Grimley, 137 U.S. 147, 150 (1890) ("[I]t is equally clear that by habeas corpus the civil courts exercise no supervisory or correcting power over the proceedings of a

Despite being a "separate community," service members are not outside the umbrella of constitutional protections. Quoting Blackstone, the Court of Military Appeals explained in *United States v. Culp*, "he puts not off the citizen when he enters the camp; but it is because he is a citizen, and would wish to continue so, that he makes himself for a while a soldier."[40] Courts thus apply the Bill of Rights to service members provision-by-provision, similar to the manner in which the Bill of Rights applies to the states.[41]

C. THE FOURTH AMENDMENT AS APPLIED TO THE MILITARY

Within the context of the Fourth Amendment, "[t]he 'expectation of privacy' is different in the military than it is in civilian life."[42] The foundation for this jurisprudential distinction lies in both necessity and custom. The responsibilities of a military commander extend to the welfare and combat readiness of his troops, investigation of their alleged misconduct, and the safety of the installation on which they live.[43] As a result of these responsibilities, which often are carried out in foreign, remote locations, military commanders necessarily require the power to inspect, search, and seize both persons and property under their command.[44] The breadth of such powers is supported by military custom, which "has long granted military commanders broad powers of search and seizure,"[45] and is now expressly provided for in the MRE.[46]

---

court[-]martial; and that no mere errors in their proceedings are open to consideration. The single inquiry, the test, is jurisdiction.").

40. 14 C.M.A. at 206 (quoting WILLIAM BLACKSTONE, COMMENTARIES *408 (Wendell ed.)) (internal quotation marks omitted).

41. *See* United States v. Stuckey, 10 M.J. 347, 349 (C.M.A. 1981). The court noted

> [t]he time is long past when scholars disputed the applicability of the Bill of Rights to service personnel. Instead, our premise must be that the Bill of Rights applies with full force to men and women in the military service unless any given protection is, expressly or by necessary implication, inapplicable.

Id. (internal quotation marks and citation omitted).

42. Comm. for GI Rights v. Callaway, 518 F.2d 466, 477 (D.C. Cir. 1975) (internal citations omitted).

43. *Stuckey*, 10 M.J. at 359.

44. *Id.*

45. *Id.* at 360 (citing United States v. Middleton, 10 M.J. 123, 126 (C.M.A. 1981)).

46. *See* MIL. R. EVID. 312–317. Although memorialized in Military Rule of Evidence (MRE) 315, which addresses a commander's power to authorize searches based on probable cause, the basis for search authority is rooted in the nature of command itself. As the *Stuckey* court noted, "the commander's long-recognized power to authorize searches within the area of his command is generally viewed as derived from and correlative with his position and responsibilities in the military community—which, of course, is 'a specialized society separate from civilian society.' " 10 M.J. at 360 (quoting Parker v. Levy, 417 U.S. 733, 743 (1974)). Of course, a commander's power to authorize probable cause searches is subject to

The Military Rules of Evidence (MRE) recognize several intrusions into potential zones of privacy, only some of which require a prior probable cause determination. MRE 312, for example, outlines the procedures for consensual and non-consensual visual examinations of the body, body cavity intrusions, extraction of body fluids (i.e., blood and urine), and intrusions for medical necessity. All of these, with the exception of intrusions for medical necessity, must be based on consent or must be conducted as either a lawful inspection or as a search and seizure pursuant to probable cause.[47]

MRE 313 provides for the admissibility of evidence obtained from inspections and inventories.[48] An "inspection" is an examination of a unit, installation, vessel, aircraft, or vehicle conducted by a command "to determine and to ensure the security, military fitness, or good order and discipline."[49] The primary purpose of the inspection cannot be to obtain evidence of criminal wrongdoing.[50] Similarly, an "inventory," which must be conducted for a legitimate administrative purpose, cannot be used as a ruse to obtain evidence of criminal wrongdoing.[51]

MRE 314, drawing on well-established case law, identifies ten searches not requiring probable cause: (1) border searches; (2) searches upon entry to or exit from a U.S. installation, aircraft, or vessel abroad; (3) searches of government property; (4) consent searches; (5) searches incident to a lawful stop; (6) searches incident to a lawful apprehension; (7) searches within jails and confinement facilities; (8) emergency searches to save life; (9) searches of open fields or woodlands; and (10) other searches not requiring probable cause "under the Constitution of the United States as applied to members of the armed forces."[52] Even within these ten areas, however, searches may be unlawful if the primary purpose of the search is to obtain evidence of

---

scrutiny. *See* 10 U.S.C. § 898 (2006) (addressing noncompliance with procedural rules); 10 U.S.C. § 938 (2006) (addressing complaints of wrongs).

47. MIL. R. EVID. 312.

48. MIL. R. EVID. 313.

49. MIL. R. EVID. 313(b).

50. *Id.* One commentator has suggested that the military's authority to monitor its information systems stems from its authority to conduct inspections pursuant to MRE 313. *See* Edell, *supra* note 9, at 23. Because MRE 313 expressly prohibits inspections for law enforcement purposes, it cannot serve as a basis for the military to search workplace communications systems for "any" purpose. *See infra* text accompanying notes 307–10 (discussing DoD's new logon banner, which permits inspections for any purpose). As a result, the military must look elsewhere for its authority to conduct warrantless searches into protected zones of privacy. *See* Edell, *supra* note 9, at 23 (arguing Army policy allowing computer monitoring for law enforcement purposes violates Supreme Court precedent).

51. MIL. R. EVID. 313(c).

52. MIL. R. EVID. 314.

criminal wrongdoing or if the search is conducted contrary to an individual's reasonable expectation of privacy.[53] If a reasonable expectation of privacy exists, an impartial commander or military judge must give search authorization based on probable cause.[54]

With respect to searches not requiring probable cause, military courts have adopted the Supreme Court's two-part *Katz* inquiry to analyze the reasonableness of service members' privacy expectations.[55] In *United States v. Daniels*, the CAAF considered whether a service member appellant's Fourth Amendment rights were violated when his barracks roommate seized a vial of cocaine from his bedside nightstand at the direction of a ranking military member. After finding that the appellant had a reasonable expectation of privacy in his nightstand and that the roommate was acting as an agent of the government, the court held the warrantless search of the nightstand unlawful.[56] *Daniels* holds that service members, like civilians, receive Fourth Amendment protections when they have a subjective expectation of privacy that is objectively reasonable.[57] Also, *Daniels* holds that in the military, as elsewhere, private actors may become agents of the government when their actions are "encouraged, endorsed, and participated in" by government officials acting in a law enforcement capacity.[58]

Perhaps the most fundamental difference in the Fourth Amendment as applied to military members lies not in the prohibition against unreasonable searches, but in the requirement to obtain a search warrant supported by an oath.[59] MRE 315 distinguishes between a search warrant, which is issued by a

53. For example, the primary purpose of searches conducted upon entrance to or exit from an installation cannot be to "obtain[] evidence for use in a trial by court-martial or other disciplinary proceeding . . . ." MIL. R. EVID. 314(c). Also, searches of government property are not permissible if "the person to whom the property is issued or assigned has a reasonable expectation of privacy" depending on "the facts and circumstances at the time of the search." MIL. R. EVID. 314(d).

54. MIL. R. EVID. 315(d). That the privacy expectation of service members may be intruded upon in certain circumstances without issuance of a warrant is another example of the provision-by-provision application of the Bill of Rights to the armed forces. For a discussion of the distinction between search warrants and search authorization, see *infra* text accompanying notes 59–62. For a discussion of the provisional application of the Bill of Rights to service members, see *supra* Section II.B.

55. *See, e.g.*, United States v. Daniels, 60 M.J. 69, 71 (C.A.A.F. 2004); United States v. Portt, 21 M.J. 333, 334–35 (C.M.A. 1986).

56. *Daniels*, 60 M.J. at 71–72.

57. *Id.* at 71.

58. *Id.*; *see also* Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 614 (1989) ("Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities.").

59. *See* Gilligan, *supra* note 35, at 4 ("In at least one area the courts have applied

competent civilian authority pursuant to the Fourth Amendment's "warrant" clause, and search authorization, which is issued by a competent military authority pursuant to military law.[60] This distinction was challenged in *United States v. Chapman*, in which a service member who was the subject of a civilian prosecution urged the Seventh Circuit Court of Appeals to suppress evidence obtained from the service member's barracks room pursuant to a military commander's search authorization.[61] Holding that the military search authorization complied with the Fourth Amendment's prohibition against unreasonable searches, the court stated:

> It is too late in the day to suggest that the Fourth Amendment's basic protection against unreasonable searches and seizures does not apply to members of the armed forces. Nevertheless, the military implementation of that guarantee is different from that employed in civilian matters. In civilian cases, the warrant requirement has been abrogated by judicial decision only in certain carefully described situations. In the military situation, Congress "has primary responsibility for the delicate task of balancing the rights of servicemen against the needs of the military."[62]

The holding in *Chapman* captures the essence of Fourth Amendment privacy protections for service members. While the procedural "complexion" of military privacy rights may differ from their civilian counterparts, the underlying constitutional protection against "unreasonable searches and seizures" remains. As with civilians, the challenge is to determine what privacy protections are reasonable.

D. PRIVACY IN THE PUBLIC WORKPLACE

Although the military workplace differs from the civilian workplace, the judicially recognized privacy interests of public employees are instructive in determining the boundaries of service members' workplace privacy interests. With respect to public employees, courts have held that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the

---

separate standards. That is in the area of the oath. The information given to the judge or the commander need not be under oath, although an oath is preferred.").

60. MIL. R. EVID. 315(b)(2), (d). In the U.S. Air Force, the competent military authority is usually an installation "magistrate" appointed by an installation commander to conduct probable cause search inquiries for on-base searches. AFI 51-201, *supra* note 9, § 3.1. The U.S. Army also has a magistrate program for probable cause search authorizations, although it differs in some respects. U.S. DEP'T OF ARMY, ARMY REG. 27-10, MILITARY JUSTICE (2005).

61. 954 F.2d 1352 (7th Cir. 1992).

62. *Id.* at 1367 (quoting Solorio v. United States, 483 U.S. 435, 447 (1987)).

government instead of a private employer."[63] Rather, public employees enjoy a limited expectation of privacy in their workplace, like those in the private sector, to the extent that the expectation is reasonable under all the circumstances.[64] In reviewing reasonableness, the context of the employment relationship is determinative. Intrusion by a supervisor is more reasonable than intrusion by law enforcement.[65] Office practices and procedures may reduce employees' expectations of privacy in their offices, desks, file cabinets, and computers.[66] Even then, however, some constitutional protections may remain.[67]

In *O'Connor v. Ortega*, the Supreme Court considered the scope of a public employee's privacy expectations in his workplace office.[68] Noting that public employers have wide latitude in entering employees' private workspaces for "the efficient and proper operation of the workplace," the Court drew clear lines between employer intrusion for work-related and law enforcement purposes.[69] For example, an employer may invade an employee's private workspace to retrieve a file. An employer may even invade an employee's workspace in furtherance of a work-related investigation. When the employer becomes an agent of law enforcement, however, and acts within the shadow of a criminal investigation, the employer's legitimate, work-related purposes end, and an intrusion of an altogether different kind begins.[70]

---

63. O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion).

64. *Id.*

65. *Id.*; *see also* Mancusi v. DeForte, 392 U.S. 364 (1968). In the context of military searches, the contrast is even more stark, because the military is both employer and police. *See infra* text accompanying notes 80–81.

66. *O'Connor*, 480 U.S. at 723.

67. In his concurring opinion in *O'Connor*, Justice Scalia criticizes the plurality's methodology for pinning the expectation of privacy a public employee has in his office to the frequency of office visitors:

> in my view, one's personal office is constitutionally protected against warrantless intrusions by the police, even though employer and co-workers are not excluded. . . . Constitutional protection against *unreasonable* searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer.

Id. at 730–31 (Scalia, J., concurring).

68. *Id.* at 709 (majority opinion).

69. *Id.* at 721, 723 ("While police, and even administrative enforcement personnel, conduct searches for the primary purpose of obtaining evidence for use in criminal or other enforcement proceedings, employers most frequently need to enter the offices and desks of their employees for legitimate work-related reasons wholly unrelated to illegal conduct.").

70. *Id.* at 722 ("In contrast to other circumstances in which we have required warrants, supervisors in offices such as at the Hospital are hardly in the business of investigating the violation of criminal laws."). In this sense, the civilian workplace is distinguishable from the military workplace, where the roles of supervisor, criminal investigator, and, at times,

The Supreme Court established a standard of reasonableness in the context of legitimate, work-related intrusions. As the Supreme Court held in *O'Connor*, "public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."[71] In practice, the test is simply whether the intrusion was "justified at its inception" and, as actually conducted, whether it was "reasonably related in scope to the circumstances which justified the interference in the first place."[72]

When a public employer's search is carried out for criminal, rather than work-related, purposes, the reasonableness standard gives way to the probable cause standard, which generally requires a search warrant. Surveying applicable case law in *O'Connor*, the Supreme Court observed, "[t]he only cases to imply that a warrant should be required involve searches that are not work related, or searches for evidence of criminal misconduct . . . ."[73]

The distinction between work-related and law enforcement searches is important. In *United States v. Kahan*, which the Supreme Court cited in *O'Connor*, the defendant, an employee of what then was the Immigration and Naturalization Service (INS), moved to suppress documentary evidence of criminal misconduct taken by INS agents from a desk-side wastebasket used exclusively by the defendant.[74] INS agents had been routinely searching the defendant's wastebasket as part of a criminal investigation into his official duties. In discussing whether searching the wastebasket constituted a "search" for purposes of the Fourth Amendment, the district court noted (1) the sole purpose of the intrusion was to obtain criminal evidence; (2) the case was distinguishable from those in which a supervisor or co-worker chances upon criminal evidence while looking through an employee's desk or wastebasket; and (3) the case did not involve a supervisor engaged in a work-related inspection.[75] The court acknowledged that the government, like private employers, "should be able to manage its . . . offices effectively and without undue restrictions on the supervision of its employees."[76] The court

enforcer of criminal law are merged. *See infra* text accompanying notes 80–81.

71. 480 U.S. at 725–26.

72. *Id.* at 726 (quoting Terry v. Ohio, 392 U.S. 1, 20 (1968)).

73. *Id.* at 721.

74. 350 F. Supp. 784, 789–90 (S.D.N.Y. 1972).

75. *Id.* at 791.

76. *Id.*

placed special emphasis, however, on the distinction between private and public employers when employee criminal misconduct is suspected:

> If a private employer suspects misconduct on the part of an employee, he will not ordinarily conduct an investigation to substantiate criminal charges against him. Rather, he will simply fire that employee. . . . In contrast, when a government supervisor begins an investigation of suspected criminal activities of an employee in the course of his work, the supervisor's role is no longer that of a manager of an office, but that of a criminal investigator for the government. The purpose of the supervisor's surveillance is no longer simply to preserve efficiency in the office. It is specifically designed to prepare a criminal prosecution against the employee. In that case, searches and seizures by the supervisor or by other government agents are governed by the Fourth Amendment admonition that a warrant be obtained in the absence of exigent circumstances.[77]

Finding the search constituted a Fourth Amendment search, the district court then turned to whether the defendant had a reasonable expectation of privacy in the wastebasket contents.[78] The court concluded (1) government employees, like their private sector counterparts, have an expectation of privacy in their workspace from government criminal investigators; (2) government supervisors may not provide third-party consent to the search of office areas "reserved for the exclusive use of a particular employee"; and (3) by throwing his documents into his wastebasket, the defendant had not abandoned them.[79] The contested evidence, having been obtained in violation of the Fourth Amendment, was suppressed.[80]

E. PRIVACY IN THE MILITARY WORKPLACE

The standard for workplace searches is similar in both the military and non-military context. However, in a military workplace the lines between work-related and law enforcement searches are less defined because the roles

---

77. *Id.*

78. *Id.* at 791–92.

79. *See id.* at 795–96. With respect to "abandonment," the district court noted the analysis does not consider whether defendant relinquished possessory interest, but whether he relinquished his privacy interest. The district court adopted

> the defense counsel's analogy, offered in oral argument, that a wastebasket should be likened to a paper shredder in that whatever a person throws in, he expects to be destroyed. Once destroyed, the contents and appearance of the papers disposed of are solely within the knowledge of that person and, hence, absolutely private.

Id. at 796 n.8. The parallels to electronic documents and e-mails which are deleted by the user but nevertheless retained on the hard drive are obvious.

80. *Id.* at 797.

of supervisor, criminal investigator, and law enforcement agent merge in the form of the commander. As one military court noted,

> [w]e must note that the military workplace is not the usual workplace envisioned by the Supreme Court in *O'Connor*. . . . Military commanders have authority and powers not possessed by civilian employers. Military commanders, for example, can authorize searches of their personnel, order them confined, and bring criminal charges against them.[81]

Additionally, actions that may constitute simple workplace misconduct for civilians may constitute criminal offenses for service members.[82] If anything, this would seem to heighten the need for probable cause search authorization prior to conducting searches for wrongdoing, a fact not lost on military courts.

In *United States v. Muniz*, decided just before *O'Connor*, the United States Court of Military Appeals considered whether a service member had a legitimate expectation of privacy in the government-issued credenza inside his government office.[83] While Captain Muniz was on leave for a secret tryst with a female service member, members of his command entered his office, opened his locked credenza, and copied an address from an envelope they thought might identify his location.[84] Their motivation in doing so was to notify Captain Muniz of a medical emergency involving his daughter; only later did they discover he had, among other things, falsified his leave address to disguise his clandestine affair.[85] In canvassing the constitutional landscape of workplace searches, the military court noted Captain Muniz maintained a separate office, the office could be locked, staff members occasionally entered each other's work areas even when the primary occupant was absent, the locked credenza (though government property) was used only by Captain Muniz, and Captain Muniz had the credenza's only key.[86] Comparing military searches to civilian workplaces searches, the military court then observed, "[t]he only seemingly complicating factor in the military is that sometimes business-supervisor and law-enforcement authority merge in the person of

81. *Long*, 64 M.J. at 62 (citations omitted).

82. For example, failing to properly perform assigned duties, feigning illness in order to miss work, and being late for work can all result in criminal charges under the UCMJ. *See* 10 U.S.C. §§ 886, 892, 915 (2006). For additional discussion of the merger of workplace and criminal misconduct in the military, see *infra* text accompanying note 365.

83. 23 M.J. 201, 204 (C.M.A. 1987).

84. *Id.* at 203–04.

85. *Id.* at 202–04.

86. *Id.* at 204–05.

the commander."[87] Without fully resolving this "complicating factor," the court concluded it was the reasonableness of the appellant's privacy expectation claim, rather than "which hat the commander happens to be wearing that day," which controlled, and determined Captain Muniz did not have a legitimate expectation of privacy in his credenza from a search to discover his whereabouts, a non-criminal purpose.[88]

In a case the following year, *United States v. Breseman*, the United States Court of Military Appeals briefly addressed, but did not have occasion to resolve, the issue of a government search authorized by a commander acting in his law enforcement (as opposed to supervisory) capacity.[89] In *Breseman*, a military commander provided probable cause search authorization to a Coast Guard Intelligence agent who wanted to search the defendant's government-owned desk. After interviewing the agent and reviewing the supporting affidavit and evidence, the commander authorized the search pursuant to MRE 315.[90] Without deciding whether the defendant had a reasonable expectation of privacy in his desk, the court held the commander adequately safeguarded the defendant's rights by complying with MRE 315.[91] Under *Breseman*, even if there is a reasonable expectation of privacy, if the search is related to law enforcement, obtaining military search authorization is sufficient to protect a service member's Fourth Amendment rights.

Neither *Muniz* nor *Breseman* definitively answer the question of whether a service member's reasonable workplace privacy interest can be searched for criminal evidence without probable cause search authorization.[92] Applying

87. *Id.* at 205.

88. *Id.* at 205–06. Though dated, for a thorough discussion of military case law regarding military members' right to privacy in their government desks, see David P. Arcuri, *Muniz, Breseman, Craig, and the Right to Privacy in a Government-Owned Desk*, 1992 ARMY LAW. 26, 28 (1992) (discussing the Military Court of Appeals' express rejection of "a bright-line rule that a service member never may have a reasonable expectation of privacy in a government-owned desk"). The court's holding in *Breseman* also underscores the protections afforded service members under MRE 314, which requires probable cause if a reasonable privacy interest exists and the primary purpose of the search is to obtain evidence of criminal wrongdoing. *See* MIL. R. EVID. 314(d).

89. 26 M.J. 398 (C.M.A. 1988). The Court of Military Appeals first applied *O'Connor* to the military workplace in *United States v. Battles*, in which the court noted "the scope of the expectation of privacy depends in part on the demands of the workplace and its openness to employees and the public." United States v. Craig, 32 M.J. 614, 615 (A.C.M.R. 1991) (citing United States v. Battles, 5 M.J. 58, 60 (C.M.A. 1987)).

90. United States v. Breseman, 26 M.J. 398, 399 (C.M.A. 1988).

91. *Id.* at 400. In his concurring opinion, Chief Judge Everett phrased the holding in a slightly different manner: "I conclude that the commanding officer had probable cause to authorize a search of appellant's desk . . . and that he authorized a search in compliance with the Military Rules of Evidence and the Fourth Amendment." *Id.* (Everett, J., concurring).

92. In *United States v. Craig*, decided in 1991, the U.S. Army Court of Military Review

the reasoning in *Kahan*, however, one would expect military courts to conclude that government searches conducted for law enforcement purposes "are governed by the Fourth Amendment admonition that a warrant be obtained in the absence of exigent circumstances."[93] This was precisely the issue confronted and decided by the CAAF in *United States v. Long*,[94] discussed in Section III.C.3 below.[95] There, the CAAF held that service members may have a reasonable expectation of privacy from law enforcement searches in their workplace e-mail,[96] a reflection of Justice Warren's comment that "our citizens in uniform may not be stripped of basic rights simply because they have doffed their civilian clothes."[97]

F. FIRST PRINCIPLES OF MILITARY WORKPLACE PRIVACY

From the preceding discussion, several principles of privacy in the military generally, and the military workplace specifically, emerge. First, the Bill of Rights applies to service members. This includes the Fourth Amendment's protections against unreasonable searches and seizures. Although guaranteed by procedural safeguards that sometimes differ from those in the civilian sector, service members' reasonable expectations of privacy are constitutionally protected. Second, the Fourth Amendment's privacy protections extend into the federal workplace. This includes the military workplace. If, based on all of the circumstances, service members can demonstrate a subjectively held and objectively reasonable expectation of privacy, warrantless searches and seizures are unreasonable absent exigent circumstances. Third, although necessity, custom, and law merge the roles of

---

found that a defendant had no expectation of privacy against his military supervisor's search of his government desk. 32 M.J. 614, 615 (A.C.M.R. 1991). In that case, the supervisor's search occurred only after the defendant's wife told the supervisor about defendant's criminal misconduct and the supervisor consulted with Army investigators about searching the defendant's desk. *Id.* Unfortunately, the court did not explore whether the supervisor's search was for a law-enforcement or work-related purpose and how that determination would impact its Fourth Amendment analysis.

93. United States v. Kahan, 350 F. Supp. 784, 791 (S.D.N.Y. 1972).

94. 64 M.J. 57 (C.A.A.F. 2006).

95. For a discussion of *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006), see *infra* Section III.C.3. For a discussion of privacy expectations in workplace e-mail, see *infra* Section II.B.

96. *Long*, 64 M.J. at 65.

97. Arcuri, *supra* note 88, at 30 n.45 (quoting Earl Warren, *The Bill of Rights and the Military*, 37 N.Y.U. L. REV. 181, 188 (1962)). In his article, Captain Arcuri argues that military commanders searching for criminal evidence are acting as law-enforcement agents rather than supervisors. Turning the language of *Muniz* on its head, he posits that in such cases "the service member, not the commander, should be in 'no worse position than his civilian counterpart.' " *Id.* at 30.

supervisor and law enforcement agent in the person of the commander, military officials may not use their roles as supervisors to cloak their actions as law enforcement agents. If an inspection, inventory, or routine workplace intrusion into a constitutionally protected area is related to a criminal investigation, both Fourth Amendment protections and the MRE first require search authorization based on probable cause. As discussed in Part III below, an appreciation for these principles is vital in casting both military communications privacy cases and the DoD's response to those cases in their proper light.

III. THE FOURTH AMENDMENT AND MILITARY E-MAIL

The Supreme Court has long recognized the need for Fourth Amendment protections to apply to electronic intrusions. In his concurring opinion in *Katz v. United States*, Justice Harlan noted that prior case law upholding the constitutionality of electronic surveillance without physical intrusion was "bad physics as well as bad law."[98] Whether accompanied by physical intrusion or not, "[e]lectronic surveillance is a search for and seizure of words" subject to Fourth Amendment safeguards.[99]

In 1968, the year after the Supreme Court outlined the requisite procedural safeguards for law enforcement agents seeking to conduct electronic surveillance, Congress incorporated the Supreme Court's heightened standards into the Wiretap Act.[100] These provisions were brought into the modern age of electronic communications by the Electronic Communications Privacy Act of 1986 (ECPA), which included the Stored Communications Act (SCA).[101] Unfortunately, as numerous commentators have noted, they have not been meaningfully updated since then to reflect the technological and social evolution of electronic communication.[102] As a

98. 389 U.S. 347, 362 (1967) (Harlan, J., concurring) (discussing Goldman v. United States, 316 U.S. 129 (1942)).

99. United States v. Stuckey, 10 M.J. 347, 349 (C.M.A. 1981) (citing Katz v. United States, 389 U.S. 347 (1967)).

100. *See* Freiwald, *supra* note 22, at 50–53.

101. 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 Stored Communications Act (SCA) safeguards electronic communications by prohibiting unauthorized access, restricting disclosure, and permitting a "governmental entity" to compel disclosure of certain electronic communications. Warshak v. United States (*Warshak II*), 532 F.3d 521, 523 (6th Cir. 2008). For a discussion of the SCA, see *infra* Section III.A.3.

102. *See, e.g.*, Freiwald, *supra* note 22, at 15–17 (noting the SCA was passed when "networked computing was in its infancy"); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 814 (2003) (discussing ECPA and noting that although amended repeatedly, "all subsequent changes have merely nibbled around the edges of the law that Congress passed with

result, stored electronic communications are protected, at most, by a warrant based on probable cause, rather than the heightened protections of in-transit communication contemplated by *Katz* and the original Wiretap Act.[103]

This Part, following discussion of the first principles of military privacy in Part II, examines precisely how courts—especially military courts—have applied the Fourth Amendment to the "search for and seizure of words" in electronic communications.[104] To lay the necessary foundation, this Part begins with the procedural safeguards outlined in *Katz*. It then moves to brief considerations of the Wiretap Act and the SCA. Finally, this Part reviews the four guidepost communications privacy cases considered thus far by the CAAF and explores whether and under what circumstances service members enjoy the limited workplace privacy expectations outlined by the Supreme Court in *O'Connor*. Particular emphasis is placed on *United States v. Larson*, the most recent computer privacy case decided by the CAAF. This Part argues that it is both factually and analytically distinguishable from prior communications privacy case law.

A. THE FOURTH AMENDMENT AND THE FEDERAL STATUTORY SCHEME FOR ELECTRONIC COMMUNICATIONS PRIVACY

1. Katz v. United States

In *Katz v. United States*, the Supreme Court considered whether the Fourth Amendment protects a person's privacy interest in telephone calls made from a public telephone booth.[105] The petitioner, Mr. Katz, was convicted at trial of communicating wagering information over a telephone in violation of a federal statute. Part of the evidence introduced against him

---

tremendous foresight back in 1986"); Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1045–46 (2008) (arguing the 180-day distinction in the SCA, which requires probable cause for e-mails stored on third-party servers less than 180 days but not for e-mails stored longer than 180 days, reflects twenty-year-old technology in which e-mails were downloaded to personal computers rather than maintained online).

103. Oza, *supra* note 102, at 1045–46. The argument that stored electronic communications should receive the same heightened safeguards as intercepted telephone calls is based on the normative valuation that electronic communications are as "vital" to private communications today as the telephone was in 1967 when the Supreme Court decided *Katz*. 389 U.S. at 348. Unlike telephone calls, however, electronic communications are generally stored during transmission. Given the normative parity of telephonic and electronic communications, it is difficult to understand why technological distinctions should warrant different statutory protections.

104. United States v. Stuckey, 10 M.J. 347, 349 (C.M.A. 1981) (citing Katz v. United States, 389 U.S. 347 (1967)).

105. 389 U.S. at 348.

included telephone calls recorded by FBI agents with a device surreptitiously placed on the outside of the telephone booth Mr. Katz used. At trial, Mr. Katz unsuccessfully moved to suppress these telephone call recordings, arguing they constituted a violation of his Fourth Amendment privacy expectations.[106] On appeal, the Supreme Court discussed the "vital role that the public telephone has come to play in private communication" and found that Mr. Katz' expectation of privacy in his telephone calls was reasonable.[107] The Court held that the government, which had not sought a search warrant, failed to adhere to appropriate procedural safeguards prior to monitoring Mr. Katz' call:

> They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized.[108]

Importantly, the safeguards outlined by the Court in *Katz* included not only an antecedent probable cause review by a detached magistrate, which would be required for any Fourth Amendment search, but also an articulation of the "precise limits" of the search in a "specific court order," as well as a detailed, post-search notification to the magistrate of "all that had been seized."[109] These heightened safeguards having been ignored, the Court overturned Mr. Katz' conviction.[110]

2. The Wiretap Act

Congress responded to *Katz* the following year by passing the Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968.[111] As Congress noted, a primary purpose of the Wiretap Act was the protection of individual privacy.[112] To achieve that end, Congress determined that that non-consensual interception of wire or oral communications "should be allowed only when authorized by a court of competent jurisdiction and

106. *Id.*
107. *Id.* at 352.
108. *Id.* at 356.
109. *Id.* The foundation for these standards had been laid in a case issued earlier during the 1967 term, *Berger v. New York*, 388 U.S. 41 (1967). For a discussion of *Berge*r and its implications for military communications privacy, see *infra* text accompanying notes 309–14.
110. *Katz*, 389 U.S. at 359.
111. 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).
112. *Id.* § 801(d), 82 Stat. at 211.

should remain under the control and supervision of the authorizing court."[113] Congress specifically recognized that communications carriers would occasionally need to intercept communications for work-related purposes, but prohibited common carriers from "service observing or random monitoring except for mechanical or service quality control checks."[114] The importance of this prohibition is that it acknowledges an individual privacy interest even when that interest is occasionally invaded for routine, work-related purposes. Put another way, in the Wiretap Act, Congress determined, just as the Supreme Court had in *Katz*, that an individual making a telephone call retains a reasonable privacy expectation in that call despite knowing it may be intercepted by the communications carrier for non-law enforcement purposes, which is a foundational principle of judicial decision-making in later communications privacy cases.[115]

To protect an individual's privacy interest, Congress incorporated into the Wiretap Act the prescriptive guidelines articulated by the Supreme Court in *Katz*, including: (1) an antecedent court order based on probable cause and supported by a detailed oath or affirmation; (2) a description in the order of the person to be surveilled, the communications technology involved, the probable offenses, the identity of the agency and agent, and the period of time (no longer than thirty days) authorized for surveillance; and (3) based on judicial discretion, subsequent reports to the issuing judge regarding the progress and fruits of the surveillance.[116] In exigent circumstances, Congress declared immediate surveillance permissible, provided law enforcement agents seek and obtain a warrant within forty-eight hours.[117] Congress also provided a statutory exclusionary remedy for communications obtained in violation of the Wiretap Act.[118]

---

113. *Id.*

114. 18 U.S.C. § 2511(2)(a) (2006).

115. Recent case law also recognizes that a third-party provider's ability to access private content does not per se destroy a reasonable expectation of privacy. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905–06 (9th Cir. 2008) (holding that plaintiff had Fourth Amendment expectation of privacy in text messages even though service provider "may have been able to access the contents of the messages for its own purposes"). Still, some degree of uncertainty regarding a user's ability to maintain privacy expectations in electronic information disclosed to third-party service providers remains. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1211 (2004) (discussing judicial application of "disclosure" doctrine to information maintained for users by Internet Service Providers (ISPs)); *see also infra* text accompanying notes 135–36.

116. 18 U.S.C. §§ 2511–2522 (2006).

117. 18 U.S.C. § 2518 (2006).

118. 18 U.S.C. §§ 2511–2522.

3. The Electronic Communications Privacy Act and Stored Communications Act

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) to extend federal statutory protections to "electronic communications."[119] Among other things, the ECPA added the term "electronic communications" to the Wiretap Act, imposing the same heightened warrant requirements for surveillance of real-time, in-transit electronic communications as for traditional telephone calls.[120] As part of the ECPA, Congress also enacted the SCA, which establishes a two-tiered system for government access to electronic communications stored by third parties based on the duration of storage.[121] When an electronic communication has been stored 180 days or less, the government must seek a warrant based on probable cause.[122] When an electronic communication has been stored more than 180 days, the government may (a) provide notice to the user and then obtain the communication pursuant to a subpoena or court order, or (b) elect not to provide notice to the user and obtain the communications pursuant to a warrant based on probable cause.[123] Unlike the original Wiretap Act, Congress did not include a statutory exclusionary remedy for in-transit or stored electronic communications obtained in violation of the ECPA.[124]

---

119. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of U.S.C.). For in-depth treatment of the ECPA and Fourth Amendment privacy expectations, see Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004). The statutory scheme the ECPA amended is composed of three statutes: the Wiretap Act, 18 U.S.C. §§ 2511–2522, the Pen Register Statute, 18 U.S.C. §§ 3121–3127, and the Stored Communications Act, 18 U.S.C. §§ 2701–2711. Kerr, *supra* note 102, at 815.

120. 18 U.S.C. §§ 2511–2522 (2006); *see* Freiwald, *supra* note 22, at 13 ("With a few exceptions, the ECPA merely added the word 'electronic communication' to every instance of 'wire communication' in the statute."). Unfortunately, these heightened protections did not include stored communications. *See infra* note 125 and accompanying text.

121. 18 U.S.C. §§ 2701–2711 (2006).

122. 18 U.S.C. § 2703(a).

123. 18 U.S.C. § 2703(b).

124. *Compare* 18 U.S.C. § 2518(10) (2006) ("Any aggrieved person . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter."), *with* 18 U.S.C. § 2708 (2006) ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."). Although violators are subject to civil and criminal penalties, the failure to include a statutory exclusionary remedy means that evidence obtained in violation of the SCA may still be used against a defendant at trial absent a constitutional violation. *See* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000). The court noted that:

> [t]he statute specifically allows for civil damages and criminal punishment for violations of the ECPA, but speaks nothing about the suppression of information in a court proceeding. Instead, Congress clearly intended for

Because of the ECPA's distinction between in-transit and stored communications, electronic communications occurring in real time receive (with the exception of the suppression remedy) the heightened statutory protections provided in the original Wiretap Act, while those which are stored for more than 180 days do not.[125] As applied to e-mail, this distinction can have the perverse effect of making it more difficult for law enforcement authorities to surveil and seize a single in-transit e-mail than thousands of stored e-mails, particularly those maintained in electronic storage more than 180 days, for which a probable cause warrant is not required.[126] As a result of this deficiency, some commentators have characterized the SCA's protections as "anemic."[127] They argue that the SCA, written more than twenty years ago, fails to recognize the reliance contemporary computer users place on networked access to e-mails, documents, and photographs stored on third-party servers.[128] When the SCA was enacted, most computer users downloaded e-mails and any attached files directly to their personal

---

> suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of the ECPA.

Id.; *see also* Kerr, *supra* note 115, at 824–25 (discussing *Kennedy* and arguing for a statutory exclusionary remedy for Internet surveillance).

125. *See* United States v. Monroe, 52 M.J. 326, 330–31 (C.A.A.F. 2000) ("Congress has differentiated between the treatment of the intercept of electronic communications, which is governed by the stringent requirements of 18 USC §§ 2511–2521 (1999), and the access to stored electronic communications, which is governed by the less restrictive provisions of 18 USC §§ 2701–2707 (1999)."") (citing David B. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 3–12 (1999)). Kerr observes that "as a communication travels across the Internet, different laws apply to it at different times. For example, an e-mail message will be protected by the Wiretap Act when in transit, but by the SCA when it is stored." Kerr, *supra* note 115, at 1231 ("While the SCA protects the privacy of stored Internet communications, the Wiretap Act and Pen Register statute protect the privacy of Internet communications in transit.").

126. Unlike traditional telephone calls, which occur synchronously and generally are not recorded between private parties, e-mails are exchanged asynchronously and, by design, are stored until purposefully or routinely deleted. Even then, copies of an e-mail may be maintained on the computer of the sender or recipient, on the network of a third-party intermediary, or as a hidden file on the computer of the person who deleted the e-mail. *See* Freiwald, *supra* note 22, at 14 (2007); *see also* Kerr, *supra* note 115, at 1232 ("Because the Wiretap Act requires the government to obtain a 'super' search warrant rather than the usual warrant required by the SCA, law enforcement agents have an incentive to try to do prospective surveillance normally undertaken under the Wiretap Act using the retrospective authority of the SCA." (citation omitted)).

127. James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 85–89 (1997); Freiwald, *supra* note 22, at 16; *see also* Mulligan, *supra* note 119, at 1571–76; Oza, *supra* note 102, at 1045–46.

128. *See, e.g.*, David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009) (discussing ECPA's failure to protect communications exchanged via cloud computing).

computers, leaving little, if any, stored communications on third-party servers.[129] Today, however, users frequently rely on third-party services such as Gmail, Yahoo!, Hotmail, and MobileMe to store and retrieve their electronic communications. In such a world, it makes little sense for in-transit e-mails to receive heightened statutory protections, downloaded e-mails stored on a home computer to receive basic Fourth Amendment protections, and web-based e-mails stored on a third-party server to receive less than probable cause statutory protections, especially when the method of communication (e-mail) invokes similar expectations of individual privacy.[130] The Supreme Court's normative conclusion that reasonable privacy expectations are those that "society is prepared to recognize as 'reasonable' "[131] calls for Congress to amend the ECPA and for courts to consider seriously Fourth Amendment privacy rights in stored e-mail.[132]

4. Fourth Amendment Challenges to the SCA

Arguably, the competing standards for seizure of substantively similar electronic communications and the absence of a statutory exclusionary remedy should have encouraged, rather than discouraged, both statutory and constitutional challenges. Given that more than twenty years have passed since enactment of the ECPA, one would be justified in assuming the courts have developed a set of analytical tools for reviewing both the federal statutory scheme and its Fourth Amendment implications. As both courts and commentators have repeatedly noted, however, the tool chest remains

129. Oza, *supra* note 102, at 1045, 1052–54 (discussing the varying protections afforded e-mail based on the manner in which it is received, including Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and web-based e-mail).

130. Under the federal statutory scheme, telephone calls and real-time electronic communications retain the heightened protections of the original Wiretap Act, while e-mails stored on third-party servers receive probable cause protection or less depending on the duration of storage. E-mails downloaded to a user's personal computer and deleted from the third-party service provider's server are, like other items of personal possession, subject to routine Fourth Amendment analysis. *See* Kerr, *supra* note 115, at 1232; Mulligan, *supra* note 119, at 1571–72.

131. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

132. *See* Freiwald, *supra* note 22, at 16 (2007) (arguing for abandonment of *Katz* inquiry as analytical model in e-mail privacy cases in favor of Fourth Amendment values espoused in silent video surveillance cases); Kerr, *supra* note 115, at 1233–42 (proposing numerous changes to SCA); Oza, *supra* note 102, at 1045, 1069–70 (proposing removal of the 180-day distinction in the ECPA); Katherine A. Oyama, Note, *E-Mail Privacy After* United States v. Councilman*: Legislative Options for Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 516–25 (2006) (recommending that Congress reconsider the relationship between ECPA's two-tier framework and modern expectations of e-mail privacy); Scott A. Sundstrom, Note, *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, 2102 (1998) (urging the courts to apply the Fourth Amendment to e-mail communications).

relatively bare.[133] As a result, communications surveillance case law is famously unsettled, both regarding the constitutionality of the SCA and the privacy interests computer users have in e-mail stored on third-party servers.

A recent Sixth Circuit case, *Warshak v. United States*, illustrates this phenomenon.[134] In *Warshak*, the plaintiff sought declaratory and injunctive relief from the government after he discovered the government had seized personal e-mails from his Yahoo! and local ISP accounts pursuant to the SCA, alleging a violation of his Fourth Amendment rights.[135] On appeal from a district court opinion which held the SCA unconstitutional because it provided for disclosure on less than probable cause, the Sixth Circuit initially ruled that Mr. Warshak retained a reasonable expectation of privacy in his e-mails, even in light of the fact that Mr. Warshak's ISP could, if it chose to do so, review the content of his e-mails.[136]

On rehearing en banc, the Sixth Circuit vacated its earlier decision on grounds of ripeness and standing, holding that Mr. Warshak's request required an inappropriate facial determination of the SCA's constitutionality.[137] The court left open the door to a later constitutional challenge, however, noting that "Mr. Warshak still retains the right to challenge the district court's resolution of his motion to suppress through an appeal of his criminal conviction."[138] While declining to resolve the constitutional issue, the court did foreshadow the complexity of the SCA's constitutional landscape by discussing the difficulty in determining which e-

133. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) ("The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored."); Freiwald, *supra* note 22, at 15 (arguing dearth of case law applying Fourth Amendment to ECPA arises from difficulty in applying *Katz* two-part inquiry to electronic communication); Kerr, *supra* note 102, at 824 (arguing lack of case law interpreting federal surveillance scheme stems from Congress' failure to provide suppression remedy, which in turn discourages criminal defendants from raising challenges).

134. 532 F.3d 521 (6th Cir. 2008).

135. *Id.* at 524.

136. Warshak v. United States (*Warshak I*), 490 F.3d 455, 473 (6th Cir. 2007) ("[I]ndividuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user 'seeks to preserve as private,' and therefore 'may be constitutionally protected.' " (quoting Katz v. United States, 389 U.S. 347, 351 (1967))). The court's decision in *Warshak I* parallels Congress' determination in the original Wiretap Act that telephone users retain an expectation of privacy despite monitoring for "mechanical or service quality checks." 18 U.S.C. § 2511(2)(a)(i) (1968); *see supra* text accompanying note 123.

137. *Warshak*, 532 F.3d at 526.

138. *Id.* at 534.

mails fell within the SCA's 180-day time period, the varying privacy expectations computer users may have based on their ISP service agreements, and the as-of-yet-unanswered question of how much privacy society is prepared to recognize in computer users' e-mail.[139]

Other courts have applied Fourth Amendment analysis to e-mails stored on third-party servers without specifically confronting the constitutionality of the SCA. In *United States v. Hart*, the Western District of Kentucky considered the defendant's constitutional argument to suppress e-mails obtained by the government from Yahoo! without full compliance with the SCA.[140] Applying the two-part *Katz* inquiry, the district court found that the defendant had agreed to the Yahoo! Terms of Service, which authorized disclosure of "content" as required by law, and therefore "did not show that he sought to preserve . . . his 'Content' as private."[141] Citing *Warshak*, the district court equated "content" with e-mail "messages" and declined to find a constitutional violation. However, the district court limited its holding to the facts of the case, stating "[w]hether or not society is prepared to recognize as reasonable an expectation of privacy in all e-mail communications, the evidence in the record does not show that the defendant sought to preserve as private that which the plaintiff now seeks to introduce into evidence."[142]

Courts elsewhere have issued a range of opinions about e-mail privacy, declining in some cases to find a reasonable expectation of privacy in Internet subscriber information, IP addresses, and to/from address information,[143] while finding in other cases a reasonable expectation of

139. *Id.*

140. United States v. Hart, No. 08-109-C, 2009 U.S. Dist. LEXIS 72473 (W.D. Ky. Aug. 17, 2009). The government failed to provide proper notice to the defendant as required by the SCA under certain circumstances. *See supra* text accompanying note 121.

141. *Hart*, 2009 U.S. Dist. LEXIS 72473, at *7. Other courts have relied on contract law to find support for a user's reasonable expectations of privacy in stored e-mail. *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 2006) (finding "[American Online's] contractual obligations with appellant insured him privacy"); *see also* Stephen R. Stewart, *Katy Bar the Door—2006 New Developments in Fourth Amendment Search and Seizure Law*, 2007 ARMY LAW. 1, 13 (2007).

142. *Hart*, 2009 U.S. Dist. LEXIS 72473, at *7–*8.

143. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (finding "users have no expectation of privacy in to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information"); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (finding no reasonable expectation of privacy in Internet "subscriber" information provided by ISP to law enforcement agents pursuant to SCA); United States v. Ohnesorge, 60 M.J. 946, 949 (N-M. Ct. Crim. App. 2005) (finding no reasonable privacy expectation in internet "subscriber" information on government computer).

privacy in pager text messages and e-mails.[144] None have yet held the SCA itself unconstitutional.[145]

B. E-MAIL PRIVACY IN THE PUBLIC WORKPLACE

Like e-mail privacy generally, e-mail privacy in the public workplace remains an unsettled area of the law, with courts disagreeing about the extent to which employees can retain a reasonable expectation of privacy in e-mails sent over communications systems provided by the government for conducting official business.[146] Two approaches are immediately obvious. First, one might argue that the government provides communications systems for official use only. Because all communications sent over the network are, at least notionally, for official use, users lose any reasonable expectation of privacy.[147] Second, one might argue that the provision of a communications system is no different than the provision of a government desk. It is the actual practice of the government, rather than its general policy of official use, which supports or weakens a limited expectation of privacy. In fact, this latter argument would accord most closely with the Supreme Court's holding in *O'Connor*, which stands for the proposition that employees may possess limited Fourth Amendment privacy rights in the workplace based "on all the circumstances."[148]

Certainly legitimate reasons exist for the government, like other employers, to monitor the online activity of its employees.[149] Public

144. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903, 909 (9th Cir. 2008) (finding civil violation of both SCA and Fourth Amendment as pertaining to text messages stored by third-party service provider and obtained by plaintiff's public employer); United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996) (finding expectation of privacy in e-mails stored on AOL server).

145. *See* Warshak v. United States, 532 F.3d 521, 531 ("The Stored Communications Act has been in existence since 1986 and to our knowledge has not been the subject of any successful Fourth Amendment challenges . . . .").

146. For a recent and thorough discussion of online privacy in the workplace generally, see Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83 (2008); *see also* Micah Echols, *Striking a Balance Between Employer Business Interests and Employee Privacy: Using Respondeat Superior to Justify the Monitoring of Web-Based, Personal Electronic Mail Accounts of Employees in the Workplace*, 7 COMP. L. REV. & TECH. J. 273 (2003); Justin Conforti, Comment, *Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the Ortega Test in* Quon v. Arch Wireless, 5 SETON HALL CIR. REV. 461 (2009); Sundstrom, *supra* note 132, at 2102; DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (3d ed.).

147. Even then the slope is slippery, since, in the military at least, "official" and "authorized" use includes limited personal use. *See supra* text accompanying note 11.

148. O'Connor v. Ortega, 480 U.S. 709, 726 (1987) (plurality opinion).

149. In the private sector, seventy-seven percent of major U.S. employers reportedly

employers have an interest in ensuring employee productivity, data security, patent and trademark protection, and quality customer relations.[150] They also have an interest in preserving evidence for potential litigation, minimizing behavior that may create a hostile work environment, and ensuring their communications systems are secure, stable, and free of harmful viruses and programs.[151] Finally, with respect to certain computer systems, government agencies must take precautions to ensure their networks are protected from internal and external attacks that would endanger local, state, or national security.[152]

Rather than justifying a blanket exception to Fourth Amendment workplace privacy rights, however, such reasons appear to be yet another variety of the "efficient and proper operation of the workplace" needs the Supreme Court held in *O'Connor* to justify warrantless work-related searches.[153] If so, employees do not have a reasonable expectation of privacy against monitoring for work-related, non-investigatory purposes. Neither do they have a reasonable expectation of privacy against searches related to the investigation of work-related misconduct, provided the search is both "justified at its inception" and "reasonably related in scope."[154] Whether they

---

monitor employee communications. Echols, *supra* note 146, at 278; *see also* Press Release, Am. Mgmt. Inst., 2007 Electronic Monitoring & Surveillance Survey: Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse (Feb. 28, 2008), http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/ (last visited Sept. 1, 2009) (finding 66% of employers monitor internet connections, 65% use internet blocking software, and 43% monitor e-mail).

150. *See* Edell, *supra* note 9, at 2 (discussing justifications for employer monitoring); Sprague, *supra* note 146, at 111 (same).

151. These concerns are no different than those expressed by private employers. *See* Echols, *supra* note 146, at 278 (listing legal liability, company security, and productivity as three top reasons employers monitor employee communications).

152. *See* LeEllen Coacher, *Permitting Systems Monitoring: When the Government Can Look and What It Can See*, 46 A.F. L. REV. 155, 155–56 (1999) (discussing monitoring for operational security, law enforcement, and systems protection); Edell, *supra* note 9, at 2–3 (discussing protection of national security assets as a justification for monitoring); Kastenberg, *supra* note 11, at 181 (discussing actions by state and non-state actors to exfiltrate data from government information systems); Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. Rev. 43, 45–50 (2009) (discussing emergence of cyber warfare); *see* Erik Holmes, *Even Routine Work Poses Cyber Threat*, AIR FORCE TIMES, May 11, 2009, at 18 (discussing attacks against DoD computer systems and stolen data regarding F-35 Joint Strike Fighter); William H. McMichael & Bruce Rolfsen, *Despite Network Virus—Avoid Thumb Drives*, AIR FORCE TIMES, Dec. 8, 2008, at 13 (reporting on Air Force directives ordering computer users from using thumb drives due to virus concerns).

153. O'Connor v. Ortega, 480 U.S. 709, 723 (1987) (plurality opinion).

154. *Id.* at 726.

have an expectation of privacy for investigations related to criminal misconduct, however, remains largely undecided.[155]

In *United States v. Simons*, the Fourth Circuit considered whether an employee of the Foreign Bureau of Information Services (FBIS), a division of the Central Intelligence Agency (CIA), held a reasonable expectation of privacy in his workplace online activity and workplace computer.[156] During routine systems monitoring for inappropriate uses, it was discovered that Mr. Simons had downloaded child pornography to his workplace computer, which was located in his private office. [157] FBIS remotely examined and copied the contents of Mr. Simons' computer. After the files were viewed by representatives from the CIA Office of Inspector General (OIG), "one of whom was a criminal investigator," FBIS personnel entered Mr. Simons office, removed his hard drive, and replaced it with a copy.[158] Evidence from the hard drive then was used to obtain a search warrant, which eventually led to two searches of Mr. Simons' office and his subsequent arrest.[159]

Following his conviction, Mr. Simons argued on appeal the FBIS had violated his Fourth Amendment privacy rights.[160] The circuit court first concluded that "the remote searches of Simons' computer did not violate his *Fourth Amendment* rights because, in light of the [FBIS] Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet."[161] The FBIS internet policy specifically notified FBIS employees that "FBIS would 'audit, inspect, and/or monitor' employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages."[162] Thus, even if Mr. Simons held a subjective belief in the privacy of his online activity, his belief was not reasonable. The circuit court then turned to the initial warrantless entry into Mr. Simons' office. Finding Mr. Simons did have a reasonable expectation of privacy in his office, the court concluded the search fell within the *O'Connor* "work-related" exception.[163] In reaching that conclusion, the court assumed the "dominant purposes of the

155. *Compare* Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (holding state agency employee had reasonable expectation of privacy in workplace computer based on employer's infrequent access), *with* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding federal employee had no reasonable expectation of privacy in files downloaded from Internet when employer had published monitoring policy).

156. 206 F.3d 392 (4th Cir. 2000).

157. *Id.* at 396.

158. *Id.*

159. *Id.* at 395–97.

160. *Id.* at 398.

161. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

162. *Id.*

163. *Id.* at 400.

warrantless search . . . was to acquire evidence of criminal activity."[164] Nevertheless, "FBIS did not lose its special need for 'the efficient and proper operation of the workplace' " simply because a dual purpose of the search was criminal.[165] Thus, the court found the warrantless entry, which was reasonable in its inception and scope, did not violate Mr. Simons' Fourth Amendment privacy rights.[166]

In *United States v. Angevine*, the Tenth Circuit reached a similar conclusion when it determined a professor at a public university did not have a reasonable expectation of privacy in his university computer from local law enforcement officials.[167] In that case, law enforcement officers obtained a search warrant to seize a work computer belonging to Professor Angevine, who was suspected of possessing child pornography.[168] Numerous images of child pornography were found. At trial, Professor Angevine requested a hearing pursuant to *Franks v. Delaware*[169] to challenge the search warrant.[170] Both the trial and appellate courts denied Professor Angevine's motion because the university's computer policy and logon banner prevented finding a reasonable expectation of privacy, thereby making the search warrant unnecessary.[171] Although the circuit court did not expressly discuss the distinction between work-related and law enforcement searches, the court did note the University policy "reserved the right to randomly audit Internet use and to monitor specific individuals suspected of misusing University computers [and] . . . explicitly warned employees that legal action would result from violations of federal law."[172] The court also found significant the fact that the logon "splash screen" warned users of " 'criminal penalties' for misuse . . . ."[173]

As discussed below, military case law in these areas is still developing. Were courts to apply *Simons* and *Angevine* to the military workplace, however, both could have substantive implications. For military commanders, who are authorized to simultaneously act as supervisors and law enforcement agents, *Simons* could be relied upon to argue that military authorities may conduct a warrantless search of an otherwise protected workplace area if the purpose of the search—which may primarily be criminal in nature—is at least *partly*

164. *Id.*
165. *Id.*
166. *Id.* at 401.
167. 281 F.3d 1130 (10th Cir. 2002).
168. *Id.* at 1132.
169. 438 U.S. 154 (1978).
170. 281 F.3d at 1130.
171. *Id.* at 1135.
172. *Id.* at 1134.
173. *Id.*

work-related. For military criminal investigators, *Angevine* could be relied upon to argue that warrantless law enforcement searches of government computers are permissible as long as users receive notice of such searches through an agency-wide policy or logon banner. Unfortunately, as pertaining to searches of government e-mail accounts, neither case is precisely on point. In *Simons*, the initial electronic evidence implicating Mr. Simons was discovered as the result of routine systems monitoring, not a criminal investigation,[174] and in *Angevine* e-mail was not at issue.[175]

C. E-MAIL PRIVACY IN THE MILITARY WORKPLACE

Considering the unsettled state of civilian case law, one might reasonably expect military cases to reflect a similar schizophrenia. One might also expect, given the skepticism some critics have for the military's protection of individual service members' liberties, that military courts confronting communications privacy in the context of the Fourth Amendment would have approached the issue cautiously, erring on the side of the military's need to ensure "the efficient and proper operation of the workplace"[176] and only reluctantly finding Fourth Amendment protections for individual service members. On both points, one would be wrong.

In general, military courts have been forward leaning in both considering and finding Fourth Amendment privacy expectations in electronic communications, including those maintained privately and in the workplace. In fact, well before any Article III court addressed stored e-mail in the context of the Fourth Amendment, military courts had already ruled on the matter twice.[177] In both cases, which involved law enforcement searches, the CAAF found that service members possessed a reasonable expectation of privacy in their e-mail, and the government had violated service members' Fourth Amendment rights by intruding without a warrant.[178]

The reasons military courts outpaced Article III courts in first addressing privacy protections for stored e-mail may not be immediately apparent, but

174. United States v. Simons, 206 F.3d 392, 396 (4th Cir. 2000).

175. *Angevine*, 281 F.3d at 1132.

176. O'Connor v. Ortega, 480 U.S. 709, 723 (1987) (plurality opinion).

177. *See* United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996); United States v. Long, 64 M.J. 57 (C.A.A.F. 2006); *see also* Freiwald, *supra* note 22, at 3-4, 4 n.9 (noting in 2007 that "[n]o Article III court has yet established when or even whether users entertain a reasonable expectation of privacy in their e-mails" but that "two military courts have found a reasonable expectation of privacy in stored e-mail and imposed a warrant requirement on government access to it").

178. For a discussion of *Maxwell*, see *infra* Section III.C.1. For a discussion of *Long*, see *infra* Section III.C.3.

several possibilities present themselves. First, as observed earlier, the government assigns qualified counsel without cost to every military defendant in a special or general court-martial, regardless of the indigent circumstances of the accused.[179] Each of these attorneys is licensed to practice law in at least one state, is a graduate of both an American Bar Association (ABA) accredited law school[180] and a service-specific Judge Advocate training course,[181] and is the recipient of extensive and continuing training in trial tactics, trial procedures, and changes in law.[182] Rather than having the enormous caseload commonly carried by public defenders, military defense counsel typically have only a handful of cases, enabling them to spend more time on each case. Additionally, for serious and complex cases, the government may assign military defendants an additional defense attorney free of charge, as well as relevant forensic experts in psychology, pathology, medicine, or computer science, to name a few fields of expertise.[183] The effect of bringing all of these resources to bear in a given case may be that military defense counsel have both the ability and availability to explore and, if warranted, raise novel issues of fact and law for the benefit of their client, a luxury their civilian counterparts may not always enjoy.[184]

---

179. *See supra* text accompanying note 36.

180. The requirement under 10 U.S.C. § 827(b)(1) (2006), is that counsel "must be a judge advocate who is a graduate of an accredited law school or is a member of the bar of a Federal court or of the highest court of a State; or must be a member of the bar of a Federal court or of the highest court of a State." In the Air Force, for example, the relevant service regulation requires judge advocates to graduate from an ABA accredited law school and "[b]e in good standing and admitted to practice before a Federal court or the highest court of a U.S. state, territory, or the District of Columbia." U.S. DEP'T OF AIR FORCE, AIR FORCE INSTRUCTION 51-103, DESIGNATION AND CERTIFICATION OF JUDGE ADVOCATES para. 1.1 (2004) [hereinafter AFI 51-103]. The U.S. Army has similar requirements. *See* U.S. DEP'T OF ARMY, ARMY REG. 27-1, JUDGE ADVOCATE LEGAL SERVICES para. 13-2 (1996) [hereinafter ARMY REG. 27-1] (establishing requirements for entry into U.S. Army JAG Corps). The service secretaries have statutory authority to implement the requirements for designation as judge advocates. *See, e.g.*, 10 U.S.C. § 8067(g) (2006) ("Judge advocate functions in the Air Force shall be performed by commissioned officers of the Air Force who are qualified under regulations prescribed by the Secretary, and who are designated as judge advocates.").

181. For example, the Air Force requires judge advocates to graduate from the Judge Advocate Staff Officer Course prior to being certified as a judge advocate. AFI 51-103, *supra* note 180, at para. 3.1.

182. The Army, Air Force, and Navy each maintain a judge advocate school, which provides accession training, specialty training, and continuing legal education. *See, e.g.*, ARMY REG. 27-1, at para. 10-2 (1996) (discussing the responsibilities of the Commandant of The Judge Advocate General's School, U.S. Army).

183. Regarding experts, military regulations specifically provide for their employment and payment at government expense. *See, e.g.*, AFI 51-201, *supra* note 9, at para. 6.2.5 (discussing provision of urinalysis experts).

184. The American Bar Association has commented on public defenders' excessive

Second, civilian law enforcement officials seeking to access a suspect's workplace communications must coordinate with the suspect's employer in accordance with the federal statutory scheme. However, even if disclosure of such communications were to violate the SCA, the lack of a statutory suppression remedy provides little incentive for defense counsel to raise the issue at trial.[185] In the military, however, commanders may search service members' electronic communications without the need to coordinate with, or seek authorization from, a third party.[186] That military commanders act as both supervisors and criminal investigators heightens the possibility that the fruits of their searches will find their way to trial and, as a result, into a motion to suppress. Because such communications may have been seized pursuant to command authority rather than the SCA, defense counsel are free to raise Fourth Amendment concerns without first having to wade through the SCA's omission of statutory suppression.

Third, every defendant convicted at court martial who receives an approved sentence of death, dismissal, dishonorable discharge, bad-conduct discharge, or confinement for more than one year receives an automatic right of appeal, which includes appellate defense counsel and plenary de novo review, all of which are provided at government expense.[187] From the initial

---

caseloads. *See* Eight Guidelines of Public Defense Related to Excessive Workloads, American Bar Association (2009), *available at* http://www.abanet.org/legalservices/sclaid/defender/downloads/eight_guidelines_of_public_defense.pdf. Although employed by the military, military defense counsel (MDC) are charged with ethically and vigorously defending their clients regardless of the effect of that representation on the military. The "Fundamental Principles" of the Air Force Military Defense Counsel Charter states:

> An MDC's primary responsibility is to his or her client. Constrained only by ethical limits, MDCs are authorized by law to enter into attorney–client relationships and to oppose the government of the United States, in order to promote the individual interests of service members they represent without regard to how their actions might otherwise affect the Air Force as an institution.

AFLSA/JAJD, OPERATING INSTRUCTION 1, AIR FORCE MILITARY DEFENSE COUNSEL CHARTER (2005).

185. *See, e.g.*, United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (concluding "Congress clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of the ECPA"); *see also* Kerr, *supra* note 102, at 824 (arguing the lack of case law interpreting the federal surveillance scheme stems from Congress' failure to provide a suppression remedy, which in turn discourages criminal defendants from raising challenges).

186. For a discussion of military commanders' search authority, see *supra* text accompanying notes 44–54. Although a "third party" is not involved, commanders must still ensure their searches comply with the SCA, which prohibits access of stored communications without authorization. *See infra* note 233.

187. *See* 10 U.S.C. § 866(b)–(c) (2006); *see also* United States v. Roach, 66 M.J. 410, 412–13 (C.A.A.F. 2008) (discussing three main differences between civilian and military criminal

appellate level, cases also may be appealed to the Court of Appeals for the Armed Forces[188] and ultimately to the Supreme Court.[189] Assigned appellate attorneys—not defense trial counsel—normally represent the defendant on appeal, increasing the likelihood they will catch errors made at trial and raise issues of ineffective assistance of counsel.[190]

The extent to which these factors laid the groundwork for military courts' early entrance into the field of Fourth Amendment communications privacy is open for discussion. What is clear, however, is that military case law, though evolving, has already marked the boundaries for analyzing and determining Fourth Amendment privacy claims in electronic communications in a way that civilian federal courts have not. As discussed below, the guidepost cases are *United States v. Maxwell*,[191] *United States v. Monroe*,[192] *United States v. Long*,[193] and *United States v. Larson*.[194]

1. United States v. Maxwell—*The Fourth Amendment and Commercial E-Mail*

The CAAF first crossed the threshold of Fourth Amendment Internet law in *United States v. Maxwell*, where it addressed whether a U.S. service member possessed a reasonable expectation of privacy in his commercial America Online (AOL) e-mail account.[195] Decided in 1996, the CAAF treated the issue as one of first impression in military law. Reasoning that e-mail transmissions were analogous to traditional communications like mail and telephone calls, the CAAF held a reasonable expectation of privacy in e-mail existed.[196]

Contrary to Colonel Maxwell's pleas, the court martial convicted him of two counts of indecent language, one specification of distributing obscene materials, and one specification of transporting or receiving child pornography in violation of Article 134, UCMJ.[197] The indecent language

---

proceedings: (1) mandatory review; (2) government provided appellate counsel; and (3) de novo review of findings and sentence). Additionally, cases which do not merit mandatory appeal must be reviewed by the office of the Judge Advocate General of the relevant service, who may modify the findings and sentence, refer the case to the appellate courts, or order a rehearing. *See* 10 U.S.C. § 869 (2006).

188. 10 U.S.C. § 867 (2006).
189. 10 U.S.C. § 867(a).
190. *See* Gilligan, *supra* note 35, at 5.
191. 45 M.J. 406 (C.A.A.F. 1996).
192. 52 M.J. 326 (C.A.A.F. 2000).
193. 64 M.J. 57 (C.A.A.F. 2006).
194. 66 M.J. 212 (C.A.A.F. 2008).
195. 45 M.J. at 416.
196. *Id.* at 410, 417–19.
197. *Id.* at 410.

specifications alleged violations of clauses 1 and 2 of Article 134,[198] which generally prohibit "disorders and neglects to the prejudice of good order and discipline in the armed forces" and "conduct of a nature to bring discredit upon the armed forces," respectively.[199] The specifications for distributing obscene materials and transporting or receiving child pornography alleged violations of clause 3 of Article 134,[200] which prohibits "crimes and offenses not capital."[201]

The bases for conviction under Article 134 rested heavily on computer evidence. The conviction of indecent language was principally based on evidence the Air Force Office of Special Investigations (AFOSI) obtained from the Federal Bureau of Investigation (FBI) following execution of a search warrant on AOL. The search, which was directed at Colonel Maxwell's AOL account "Redde1," also included e-mails from Colonel Maxwell's secondary AOL account, "Zirlock."[202] Among the "Zirlock" e-mails were communications from Colonel Maxwell to another Air Force officer in which Colonel Maxwell discussed his sexual orientation, desires, and preferences. It was these e-mails that led to the conviction for indecent language.[203] Similarly, the conviction for child pornography resulted from seizure of Colonel Maxwell's on-base personal computer by AFOSI agents, who properly obtained a search warrant from the base military magistrate. The agents found three images depicting minor children, which became the basis for the child pornography conviction.[204]

198. *Id.*

199. 10 U.S.C. § 934 (2006). The sweeping language of Article 134 has been upheld despite constitutional criticisms of being "void for vagueness." *See* Parker v. Levy, 417 U.S. 733, 752–57 (1974) (rejecting "vagueness" claim in light of judicial construction which has "narrow[ed] the . . . literal language of the articles, and at the same time supplying considerable specificity by way of examples of the conduct that they cover").

200. United States v. Maxwell, 45 M.J. 406, 410 (C.A.A.F. 1996).

201. 10 U.S.C. § 934. Although the literal language of Clause 3 is obscure, its meaning in practice is clear. Service members may be punished under Clause 3 for violating federal crimes of unlimited application, such as counterfeiting or various frauds, and crimes of local application, which includes both federal crimes and state crimes adopted as part of the Federal Assimilative Crimes Act (18 U.S.C. § 13). *See* 10 U.S.C. § 934.

202. *Maxwell*, 45 M.J. at 414. In the search warrant, Colonel Maxwell's AOL account was erroneously listed as "REDDEL" rather than "Redde1" (pronounced "Ready One"), and his alternate account "Zirlock" was not listed at all. AOL collected records for both "Redde1" and "Zirlock," however, because they belonged to the user. Colonel Maxwell challenged both searches, but was unsuccessful as concerning "Redde1," which the CAAF held was a minor scrivener's error. *Id.* at 413, 420.

203. *Id.* at 414.

204. *Id.*

On appeal, defense counsel raised numerous issues of error, ranging from the constitutionality of the applicable federal statutory scheme to the validity of both the AOL and on-base search warrants.[205] Before reaching these issues, however, the CAAF explored as an initial matter whether appellant's expectation of privacy in his AOL e-mail account was reasonable.[206] The CAAF relied heavily on the testimony of AOL's vice president of marketing, who stated that "AOL's policy was not to read or disclose subscribers' e-mail to anyone except authorized users" and "[i]t was AOL's practice to guard these 'private communications' and only disclose them to third parties if given a court order . . . ."[207] From these statements, the CAAF concluded that the "appellant possessed a reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL."[208]

The CAAF then took an interesting and important turn in its analysis. Acknowledging the varying degrees of Fourth Amendment privacy expectations, the CAAF distinguished between privacy interests in the computer itself and the messages sent or e-mailed from that computer:

> We are satisfied that the Constitution requires that the FBI and other police agencies establish probable cause to enter into a personal and private computer. However, when an individual sends or mails letters, messages, or other information on the computer, the Fourth Amendment expectation of privacy diminishes incrementally. Moreover, the more open the method of transmission, such as the 'chat room,' the less privacy one can reasonably expect. This case alone presents a spectrum of privacy expectations . . . .[209]

After acknowledging the "spectrum of privacy expectations," the CAAF analogized to existing technologies. The court noted that in making an initial transmission over e-mail, first class mail, or telephone, a sender has a

---

205. *Id.* at 416.

206. *Id.*

207. *Id.* at 417. In *United States v. Long*, the CAAF similarly relied on network administrator testimony in determining whether the network provider had, through its policies and actions, created a reasonable expectation of privacy in its computers. 64 M.J. 57 (C.A.A.F. 2006); *see also infra* text accompanying note 234.

208. *Maxwell*, 45 M.J. at 417. The CAAF also observed the AOL's system differed from "less secure" e-mail systems on the Internet. *Id.* (citing American Civil Liberties Union v. Reno, 929 F. Supp. 824, 830–44 (E.D. Pa. 1996)). Whether the technical differences that led CAAF to draw this distinction still exist is questionable, especially given the evolution from proprietary platforms to web-based e-mail applications. *See generally* Couillard, *supra* note 128, at 2205 (discussing application of Fourth Amendment privacy expectations to electronic communications stored on Internet cloud).

209. *Maxwell*, 45 M.J. at 417.

reasonable expectation of privacy from unauthorized interceptions by law enforcement authorities. This expectation, however, does not extend to secondary and tertiary transmissions over which the original sender has no control.[210] Having found parallels in other mediums of communication, the CAAF had little difficulty in finding that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[211] Accordingly, the CAAF held that the "Zirlock" e-mail messages supporting the indecent language specifications were beyond the scope of the search warrant (which included only "Redde1" e-mails) and thus had to be suppressed.[212]

Although *Maxwell* addressed e-mails sent over commercial, as opposed to government networks, it provides a helpful backdrop in identifying the first principles underscoring the CAAF's subsequent privacy expectation decisions in *Monroe* and *Long*—decisions which, at first blush, appear to reach opposite conclusions concerning Fourth Amendment privacy expectations in government e-mail. The strength of the CAAF's approach in *Maxwell*, which the court drew upon in subsequent cases, lies in its willingness to base its privacy expectation analysis on the vital nature of the technology at issue, the methods of storage, retrieval, and transmission, and the distinction between non-law enforcement and law enforcement searches. As the CAAF concluded in *Maxwell*, "[e]xpectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient."[213] These distinctions would define the outcomes of later CAAF decisions.

2. United States v. Monroe—*The Fourth Amendment and Government E-Mail Monitoring*

In *United States v. Monroe*, the CAAF's next milestone communications privacy case, the court considered whether e-mails transmitted over a government network warranted protection from systems monitoring.[214] By drawing a line between routine systems monitoring and purposeful law enforcement activity, the CAAF held the e-mails at issue did not qualify for Fourth Amendment protection.[215]

---

210. *Id.* at 417–18.

211. *Id.* at 418. The possibility of unauthorized interceptions by others, such as hackers, "does not diminish the legitimate expectation of privacy in any way." *Id.*

212. *Id.* at 424.

213. *Id.* at 418–19.

214. 52 M.J. 326, 330 (C.A.A.F. 2000).

215. *Id.* at 329–31.

In late 1995, during the course of routine systems maintenance, two Air Force systems administrators at Osan Air Base, Korea discovered the local government e-mail server had fifty-nine undeliverable messages addressed to Staff Sergeant Monroe.[216] To learn why the files had not been routed correctly, the e-mails were copied to another computer and opened by the systems administrators, who discovered multiple sexually explicit images.[217] The systems administrators then opened Staff Sergeant Monroe's e-mail account "to find out whether this material had been requested or whether Monroe had been the victim of a prank."[218] After finding an e-mail from Staff Sergeant Monroe requesting a file from the sender of the pornographic images, the systems administrators turned the material over to AFOSI agents, who consulted with the local judge advocate and base military magistrate to obtain probable cause search authorization.[219] AFOSI agents then searched Staff Sergeant Monroe's on-base dormitory room, seized his personal computer, and found several images of child pornography.[220]

At trial, Staff Sergeant Monroe argued his Fourth Amendment rights had been violated and moved to suppress both the initial evidence found by the systems administrators and the evidence the AFOSI later seized.[221] The trial court denied his motion, and Staff Sergeant Monroe entered a conditional guilty plea to preserve the suppression issue on appeal.[222] He was convicted by a general court-martial of violating a general order, possessing child pornography, and transmitting and receiving obscene writings and computer graphics.[223]

On appeal, the CAAF began by comparing the facts at issue in *Monroe* to those at issue in *Maxwell*.[224] The court noted that in *Maxwell* the e-mails were

---

216. *Id.* at 328–29.

217. *Id.*

218. *Id.*

219. *Id.* at 326–29.

220. *Id.* at 329. Although not explicitly stated in the court's opinion, it appears the e-mails had been sent to and from Staff Sergeant Monroe's government e-mail account, which he accessed using his personal computer in his dormitory room. Staff Sergeant Monroe did not have access to government computers at his workplace capable of sending or receiving e-mail. *Id.*

221. *Id.*

222. *Id.*

223. *Id.*

224. *Id.* at 330. At the intermediate appellate level, the Air Force Court of Criminal Appeals had affirmed the military judge's denial of the motion to suppress, finding Staff Sergeant Monroe had no reasonable expectation of privacy in his e-mails "at least as regards his superiors and the [systems] administrator and his/her superiors." *Id.* at 329 (quoting United States v. Monroe, 50 M.J. 550, 559 (A.F. Ct. Crim. App. 1999)) (internal quotation marks omitted). The Air Force appellate court also sustained the probable cause search authorization issued by the base magistrate. *Id.*

located on a privately owned AOL server and that AOL had contractually agreed to provide limited subscriber privacy.[225] By contrast, the e-mails in *Monroe* were located on a government-owned server, and the government had a specific notice that "users logging on to this system consent to monitoring by the administrator."[226] Implicitly applying the *O'Connor* totality of the circumstances test,[227] the court held that "Monroe had no reasonable expectation of privacy in his e-mail messages or e-mail box at least from the personnel charged with maintaining the . . . system."[228]

The limited nature of the CAAF's holding is important. By adopting the intermediate appellate court's reasoning that Staff Sergeant Monroe had no privacy expectation "from the personnel charged with maintaining the . . . system,"[229] the CAAF was able to embrace both its reasoning in *Maxwell* and the work-related/law enforcement distinction underlying federal workplace privacy case law. Citing *Maxwell*, the court explicitly stated, "[t]he transmitter of an e-mail message enjoys a reasonable expectation of privacy that police officials will not intercept the transmission without probable cause and a search warrant."[230] No such expectation, however, is available as against those tasked with routine systems maintenance.[231]

Having found the systems administrators' search did not violate the Fourth Amendment, the CAAF next considered whether the systems administrators had disclosed the messages' contents in violation of the SCA.[232] Noting the distinction Congress had drawn between intercepted and stored electronic communications, the CAAF found, without explanation, "the e-mail messages in this case were accessed from storage and not intercepted in transit," and therefore the SCA's disclosure provisions (as opposed to the Wiretap provisions) applied.[233] Under the SCA, the court

225. *Id.* at 330.

226. *Id.*

227. O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987) (plurality opinion).

228. *Monroe*, 52 M.J. at 330.

229. *Id.*

230. *Id.* (citing United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996)).

231. *Id.*

232. *Id.* at 330–31. Interestingly, *Monroe* is the only one of the four seminal communications privacy cases in which CAAF considered the SCA. For a discussion of the SCA's limitations on disclosure, see *supra* text accompanying notes 121–23123.

233. *Monroe*, 52 M.J. at 330–31. It would have been interesting if the CAAF had explored the distinction between "in transit" and "stored" communications before concluding the SCA was the applicable statutory scheme, especially since e-mails that have not been delivered to the recipient due to a technical malfunction are, in a sense, intercepted while "in transit." The Wiretap Act prohibits unauthorized "interception" of electronic communications, while the SCA prohibits the unauthorized access of an electronic communication while it is in "electronic storage." Under 18 U.S.C. § 2510(4) (2006),

observed, disclosure by a communications systems provider (such as the U.S. Air Force) to a law enforcement agency is permissible "if such contents (A) were inadvertently obtained by the service provider; and (B) appear to pertain to the commission of a crime."[234] Because the systems administrators had obtained the e-mail inadvertently without a law enforcement purpose, the disclosure was appropriate.[235]

In *Maxwell*, the CAAF laid the foundation for finding a reasonable expectation of privacy in personal e-mail. In *Monroe*, the CAAF built on that foundation by holding that a user sending e-mail over a government network does not possess a reasonable expectation of privacy against systems monitoring, but also stating in dicta that users do enjoy a reasonable

---

" 'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Under 18 U.S.C. § 2510(17)(A), " 'electronic storage' means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." Based on these definitions, the e-mails at issue in *Monroe* most likely fall under the SCA because they were in "temporary" storage even while in transit. For a discussion of the distinction between "in transit" and "stored" communications, see *supra* text accompanying note 123.

234. *Monroe*, 52 M.J. 326, 331 (citing 18 USC § 2702(b) (1994)) (internal quotation marks omitted). By design, the SCA distinguishes between "public" and "nonpublic" service providers. Commentators disagree about the SCA's applicability to the military as a "public" service provider. *Compare* Coacher, *supra* note 152, at 178 (arguing SCA is not applicable to U.S. Air Force), *with* Edell, *supra* note 9, at 11 (arguing DoD regulations and military practice make SCA applicable U.S. Army). Either way, the court in *Monroe* applied the SCA to the Air Force, 52 M.J. at 330, and the DoD requires electronic communications interceptions be conducted in accordance with the federal statutory scheme. *See* DEP'T OF DEFENSE, DIR. 5505.9, INTERCEPTION OF WIRE, ELECTRONIC, AND ORAL COMMUNICATIONS FOR LAW ENFORCEMENT (1995). On May 21, 2009 the Air Force Network Operations Commander, Major General David Senty, issued an Air Force-wide memorandum stating, "[a]s a *non-public* communications service provider, the Electronic Communications Privacy Act (ECPA) authorizes Air Force systems administrators to access stored communications stored [sic] if they are acting within their authority." Memorandum from the Air Force Network Operations for All Installation Commanders and All Network Control Centers (May 21, 2009) (on file with author) (emphasis added); *see also* Rich Ladue, *Bullet Background Paper on the Voluntary Provision of Stored Communications and Data, the Designated Accrediting/Approval Authority, & Computer Trespasser Monitoring*, U.S. AIR FORCE, May 26, 2009 (advising AFOSI agents need only obtain Air Force approval—not user approval—before searching service member e-mails under SCA). Whether the Air Force's claim of its non-public service provider status will survive judicial scrutiny, especially given that the Air Force portal allows non-military family members to establish e-mail and instant messaging accounts, remains to be seen. *See* Air Force Portal: Friends & Family Instant Messenger, https://guest.my.af.mil/ (last visited Sept. 4, 2009); *see also* Jim Tice, *Stricter Security Won't Interfere with AKO Access*, ARMY TIMES, May 29, 2006, at 16 (discussing "Army Knowledge Online" access for service members, contractors, retirees, and military family and friends).

235. *Monroe*, 52 M.J. at 331. Even if the disclosure had been in violation of the SCA, Staff Sergeant Monroe still would have been unsuccessful in suppressing the e-mails because the SCA does not provide a statutory exclusionary remedy, and the court had already determined a constitutional violation did not occur. *See supra* text accompanying note 122.

expectation of privacy against the police. In *Long*, the CAAF had occasion to test that proposition by considering a "police" intrusion in the form of a command-directed criminal investigation. The question at issue was whether and to what extent military members enjoy a reasonable privacy expectation in their workplace e-mail when the purpose of the intrusion is law enforcement.[236]

3. United States v. Long—*The Fourth Amendment and Government E-Mail Searches*

In 2006, six years after its decision in *Monroe* and ten years after its decision in *Maxwell*, the CAAF heard *United States v. Long*, a case in which "the reasonable expectation of privacy a military person has in e-mail messages sent and stored on a government computer system" was placed front and center.[237] Because the e-mails at issue were searched for law enforcement purposes, rather than routine systems monitoring, the CAAF found a reasonable expectation of privacy, confirming in *Long* what it had stated in dicta in *Monroe* regarding the distinction between work-related and law enforcement intrusions.[238]

Contrary to her pleas, Lance Corporal Long was convicted of unlawful drug use in violation of Article 112a, UCMJ.[239] The evidence against her was based in part on e-mails obtained from her government e-mail account in which she had indicated "a fear that her drug use would be detected by urinalysis testing and the steps she had taken in an attempt to avoid such detection."[240] The e-mails were found during the course of an investigatory search conducted by the systems administrator at the direction of an investigator from the Marine Corps Inspector General, who was investigating—not possible drug use—but "allegations of an improper

236. United States v. Long, 64 M.J. 57 (C.A.A.F. 2006). In her dissenting opinion in *Long*, Judge Crawford, who had joined the majority in *Monroe*, recognized that the court left open in *Monroe* the issued presented in *Long*, stating, "[i]n *United States v. Monroe*, we held that a defendant does not have an expectation of privacy in his e-mail, 'at least from the personnel charged with maintaining the . . . [electronic mail host] system.' We left open the issue presented in this particular case." *Id.* at 67 (Crawford, J., dissenting).

237. *Id.* at 57–58. In *Long*, Judge Gierke, who had concurred in part and concurred in full in *Maxwell* and *Monroe*, respectively, delivered the court's opinion. Judge Effron, who was not on the court for *Maxwell* but had concurred in *Monroe*, joined him. The other majority members, Judge Baker and Judge Erdmann, had not been on the court for either *Maxwell* or *Monroe*. *Id.*

238. *Id.* at 65.

239. *Id.* at 59. 10 U.S.C. § 912 (2006) prohibits the wrongful use, possession, manufacturing, distribution, or importation of controlled substances.

240. *Long*, 64 M.J. at 57–59.

relationship between [Lance Corporal Long] and an officer."[241] After the search, the drug-related e-mails were provided to officials and subsequently introduced against Lance Corporal Long at trial.[242]

At trial, the defense moved to suppress the e-mails as violating the Fourth Amendment.[243] The systems administrator testified for the government in opposition to the suppression motion, stating (a) the search had been conducted to find evidence of misconduct, not as part of routine systems monitoring; (b) each computer user "had his or her own unique password known only to them"; (c) the systems administrator could access users' e-mails, although "it was general policy to avoid examining e-mails and their content because it was a 'privacy issue' "; (d) the policy regarding personal e-mails "had always been lenient and that such use of the network was considered authorized"; and (e) a logon banner appeared every time a user logged onto the network, informing the user that using the network constituted consent to monitoring.[244] The banner stated:

> 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.[245]

Although the trial judge determined the search was a non-consensual search for evidence conducted without search authorization, the judge denied the

241. *Id.* at 59.
242. *Id.*
243. *Id.*
244. *Id.* at 59–60, 64.
245. *Id.* at 60.

motion to suppress on the basis that Lance Corporal Long "had no expectation of privacy in the e-mails stored on the government server."[246]

The intermediate appellate court, the Navy–Marine Corps Court of Criminal Appeals, disagreed, finding the logon banner removed Lance Corporal Long's expectation of privacy only as to systems monitoring, not law enforcement activity.[247] The court sustained the conviction, however, on the basis of harmless error.[248]

Employing the *Katz* two-part inquiry in the context of the *O'Connor* workplace privacy analysis, the CAAF first reviewed whether Lance Corporal Long had a subjective expectation of privacy in her government e-mail account. The CAAF noted Lance Corporal Long had her own password, the systems administrator had "repeatedly emphasized the agency practice of recognizing the privacy interests of users in their e-mail," and the banner described monitoring, not law enforcement, activity.[249] Finding a subjective privacy expectation, the CAAF then reviewed the "operational realities of the workplace" to determine whether Lance Corporal Long's expectation was objectively reasonable.[250] While acknowledging the e-mails were sent from a government computer, over a government computer network, and stored on a government server, the court found that actual office practices "reaffirm[ed] rather than reduce[d] the expectations regarding privacy on office computers."[251] The court then contrasted *Monroe*, in which the e-mails were discovered in the course of routine monitoring, not law enforcement.[252] In light of the banner's limited monitoring notice and actual workplace practices, the CAAF found Lance Corporal Long's expectation of privacy reasonable.[253] Because the search was for a law enforcement—not work-related—reason, the search required probable cause, which had not been obtained.[254] The e-mails were accordingly suppressed, the error was deemed not harmless, and the conviction was set aside.[255]

The CAAF's opinion in *Long* sent ripples through the military legal and law enforcement communities, with critics expressing concern that such privacy expectations could deprive the military "of the ability to effectively

246. *Id.* at 59–60.
247. *Id.* at 60.
248. *Id.*
249. *Id.* at 63.
250. *Id.*
251. *Id.* at 64.
252. *Id.* at 64–65.
253. *Id.*
254. *Id.*
255. *Id.* at 66.

monitor government communications and respond to threats to national security."[256] The military responded by issuing guidance for military attorneys and investigators about the impact of *Long* on criminal military investigations,[257] and the Joint Task Force–Global Network Operation began drafting a revised logon banner for the DoD Chief Information Officer to "preclude any claims to an expectation of privacy on base network servers for e-mails or any other digital evidence."[258] To some critics, it may have seemed ludicrous that a military member could possess a reasonable expectation of privacy in e-mail sent from a government computer over a government network, especially when the government computer was issued for official use and contained a logon banner to that effect.[259] Two years later, the concerns of those critics would find expression in the CAAF's next major computer privacy case, *United States v. Larson*.[260]

---

256. Mary L. Walker, *Lack of Privacy in Government Computer Systems*, GEN. COUNSEL'S Q. (2007).

257. *See* Edell, *supra* note 9, at 24 n.325 (citing e-mail from Deputy Assistant Staff Judge Advocate Gen. (Criminal Law) to All Navy and Marine Corps Judge Advocates, subject: Search Authorization for Computer Files in Light of *United States v. Long*, 64 M.J. 57, Part II (1 June 2007)); Rich Ladue, *Bullet Background Paper*—U.S. v. Long, 4 TJAG ONLINE NEWS, Oct. 4, 2006 [hereinafter Ladue, U.S. v. Long]; Rich Ladue, *Bullet Background Paper on* U.S. v. Long *and Its Impact on Investigations*, U.S. AIR FORCE, Oct. 3, 2006 [hereinafter Ladue, *Impact on Investigations*]; Mary L. Walker, *Expectation of Privacy in Computer Systems: Follow-Up*, GEN. COUNSEL'S Q. (2007); Memorandum from W. Kipling At Lee, Jr., Deputy Gen. Counsel (Nat'l Sec. & Military Affairs), to Air Force Office of Special Investigations Judge Advocate, subject: Computer Privacy (Dec. 14. 2006) (on file with author).

258. Ladue, *Impact on Investigations*, *supra* note 257.

259. In fact, these were largely the concerns raised by Judge Crawford in her vigorous dissent. *Long*, 64 M.J. at 67 (Crawford, J., dissenting). In her dissent, Judge Crawford argued that the majority's decision rested on the erroneous assumption that "an objective reasonable expectation of privacy can be preserved for some forms of seizure despite being nonexistent for others." *Id.* In Judge Crawford's view,

> Once [Lance Corporal Long] was given notice of and consented to monitoring of any kind, she could not maintain a reasonable expectation of privacy against other forms of intrusion . . . . That the communications were obtained specifically for law enforcement purposes has no bearing on her expectation of privacy.

Id. at 67–68. Judge Crawford also argued the search was lawful on the basis of consent. *Id.* at 70. Judge Crawford's opinion that the purpose of the search is irrelevant is difficult to square with the Supreme Court's view in *O'Connor*, which explicitly stated the purpose of the search was relevant. *See* O'Connor v. Ortega, 480 U.S. 709, 716 (1987) (plurality opinion) ("Within the workplace context, this Court has recognized that employees may have a reasonable expectation of privacy against intrusions by police." (citation omitted)). For additional discussion of user consent, see *infra* Section IV.B.3.

260. 66 M.J. 212 (C.A.A.F. 2008). I use the term "computer privacy" case purposefully, as *Larson* involves internet files rather than e-mails. On this basis alone, future courts may find *Larson* distinguishable from its predecessors.

4. United States v. Larson—*The Fourth Amendment and Government Computer Searches*

Unlike *Maxwell*, *Monroe*, and *Long*, which all involved e-mail, *United States v. Larson* involved a service member's privacy expectation in electronic files residing on his government computer hard drive.[261] In an opinion that, in some ways, stands analytically apart from the three prior communications privacy cases, the CAAF[262] held that the facts presented did not provide a basis to find either a subjective or objective expectation of privacy.[263]

Contrary to his pleas, a general court-martial convicted Major Larson of attempted carnal knowledge, attempted indecent acts with a minor, violation of a general regulation, communicating indecent language, and attempting to entice a minor to engage in sexual activity.[264] Evidence was presented that Major Larson, a 36-year-old reservist at Schriever Air Force Base, Colorado Springs, Colorado, was temporarily occupying the office of a deployed activity duty member when he began using his government computer to send instant messages (IM) to a fourteen-year-old girl named "Kristin."[265] "Kristin" was, in fact, a civilian detective posing online as a young girl to catch sexual predators.[266] After multiple salacious conversations, Major Larson and "Kristin" agreed to meet at a nearby mall to have sex.[267] Major Larson was met instead by local police, who arrested him and alerted the

---

261. *Id.* at 214. The prior CAAF case most factually analogous to *Larson* is *United States v. Tanksley*, which also addressed a service member's privacy interest in his government workplace computer. United States v. Tanksley, 54 M.J. 169, 171–72 (C.A.A.F. 2007) (finding no reasonable privacy expectation from work-related intrusion uncovering criminal evidence in document open on computer screen). However, Tanksley did not involve a law enforcement search. *Id.*

262. In a unanimous decision, Judge Ryan, who was not on the court for any of the three prior decisions, issued the opinion of the court in *Larson*. She was joined by Judge Baker, Judge Erdmann, and Judge Stucky. Judge Effron, filing a separate concurring opinion here, had also joined the majority opinion in *Long*. 66 M.J. at 213.

263. *Long*, 66 M.J. at 216. In addition to the Fourth Amendment challenge, the CAAF also addressed a claim of ineffective assistance of counsel. The CAAF found that the defendant's civilian defense counsel had been deficient in conceding guilt to one of the charged offenses, but that the defendant was not prejudiced by his attorney's tactical decision. *Id.* at 219. Because the ineffective assistance of counsel claim is not relevant to this Article, I do not discuss it here.

264. *Id.* at 213. The specifications alleged violations of Articles 80, 92, and 134, UCMJ. Major Larson was sentenced to nine years confinement, dismissal from the military, and forfeiture of all pay and allowance. The convening authority reduced his confinement to six years. *Id.*

265. United States v. Larson, 64 M.J. 559, 561 (A.F. Ct. Crim. App. 2006).

266. United States v. Larson, 66 M.J. 212, 214 (C.A.A.F. 2008).

267. *Id.* at 214.

AFOSI.[268] Continuing the investigation, the AFOSI contacted Major Larson's commander, who opened Major Larson's office using a master key and allowed the AFOSI to seize Major Larson's government computer.[269] A search of the computer "revealed stored pornographic material, a web browser history that showed [Major Larson] visited pornographic websites and engaged in sexually explicit chat sessions in his office on his government computer, and other electronic data implicating [Major Larson] in the charged offenses."[270]

At trial, Major Larson unsuccessfully moved to suppress all evidence seized from his government computer, arguing a violation of his Fourth Amendment privacy rights.[271] Unlike *Long*, in which the systems administrator testified on behalf of the government, the government placed Major Larson's commander on the stand.[272] Based on his testimony, the military judge found that (a) Major Larson occupied a private, lockable office, though others had keys, (b) the government computer was for official use, (c) the computer was password protected, although a systems administrator still could access the hard drive, and (d) a logon banner appeared every time a user logged onto the network, informing the user "the computer was DoD property, was for official use, and that [the user] consented to monitoring."[273] In accordance with these findings, the military judge denied the defense's suppression motion.[274]

On appeal, the Air Force Court of Criminal Appeals characterized the case as one "of first impression in some respects."[275] Citing both *Long* and *Monroe*, the appellate court noted that prior military cases involving computers and the Fourth Amendment focused on e-mail communications, whereas "[t]he search of the government computer here did not focus on such communications."[276] In this case, the AFOSI's investigative search involved "certain data files, created as part of the 'normal operating procedure' of the Microsoft Windows operating system . . . ."[277] Because the

268. *Id.*; *Larson*, 64 M.J. at 562.

269. *Larson*, 66 M.J. at 214.

270. *Id.* at 214–15. The CAAF opinion characterizes the evidence as "files" stored on Major Larson's workplace computer. *Id.* The intermediate appellate court opinion clarifies, however, that the files were all temporary Internet files, cached from Major Larson's Internet browsing. *Larson*, 64 M.J. at 563.

271. 66 M.J. at 214.

272. *Larson*, 66 M.J. at 214.

273. *Id.*

274. *Id.* at 215; *Larson*, 64 M.J. at 563.

275. *Larson*, 64 M.J. at 563.

276. *Id.*

277. *Id.*

"data files" were created as part of a "normal operating procedure," they were more akin to routine systems monitoring than active law enforcement efforts:

> There is no evidence the appellant was aware the Internet history files existed, and we are unconvinced the appellant could entertain a subjective expectation of privacy in them without such knowledge. Moreover, we conclude such an expectation, even if it existed, would on these facts not be reasonable. *The data in question was recorded automatically, not for law enforcement purposes, but as part of the computer's operating system.* The appellant could not expect to keep private automatically-recorded data stored on government property he would reasonably have known would be turned over to another officer on that officer's return from deployment.[278]

Finding Major Larson had neither a subjective nor an objective expectation of privacy in such data, the intermediate appellate court held the trial judge had not abused his discretion.[279]

Surprisingly, the CAAF took an entirely different tack from the lower appellate court, avoiding any discussion of the case as one of first impression. Further, the court did not analyze either the impact of the deployed member's departure or return on Major Larson's privacy interest or the nature of the data files as being "recorded automatically, not for law enforcement purposes."[280] In fact, the CAAF even took a different analytical tack from its previous approaches in *Maxwell*, *Monroe*, and *Long*, focusing heavily on Major Larson's privacy interest in the situs of the search rather than the data files on the computer: "[i]n addressing *Fourth Amendment* privacy claims, the threshold issue is whether the person has a legitimate expectation of privacy in the invaded *place*."[281] The CAAF continued its emphasis on "place" by quoting MRE 314(d), which, in CAAF's view, created a rebuttable presumption that individuals cannot have a reasonable expectation of privacy in government property:

> Government property may be searched under this rule unless the person to whom the property is issued or assigned has a reasonable expectation of privacy therein at the time of the search. Under

278. *Id.* (emphasis added).

279. *Id.*

280. *Compare Larson*, 66 M.J. at 214–16, *with Larson*, 64 M.J. at 563.

281. *Larson*, 66 M.J. at 215 (final emphasis added). The *Larson* court's recitation of the law was not in any way incorrect. In fact, the court's statement was taken almost verbatim from *Rakas v. Illinois*, 439 U.S. 128, 143 (1978), a Supreme Court opinion relying on *Katz*. However, *Rakas* was not a communications privacy case. It involved search of a vehicle and heavily emphasized property and possessory interests. 439 U.S. at 143.

> normal circumstances, a person does not have a reasonable expectation of privacy in government property that is not issued for personal use . . . .[282]

The CAAF noted that Major Larson had utilized a government computer that was accessible by both the commander and systems administrator, and located in an office that was also accessible by the commander and others.[283] Finding no evidence that Major Larson had a subjective expectation of privacy in his government computer, and finding evidence based on the commander's testimony and logon banner to support "the validity of the presumption that [Major Larson] had no reasonable expectation of privacy in the government computer," the CAAF sustained the lower courts' rulings.[284]

What is surprising in *Larson* is not the outcome reached by the CAAF (after all, the lowers courts had reached the same conclusion, and the CAAF had also found no reasonable expectation of privacy in *Monroe*), but rather the path it took to get there. First, as discussed below, the court did not utilize the *O'Connor* workplace analysis. Second, the court did not discuss the distinction between work-related and law enforcement searches. Finally, the court did not analyze (as the intermediate appellate court had done) whether Major Larson had any privacy expectation in the data files on his computer as opposed to the computer itself. The reasoning in *Larson* thus differed substantially from that the CAAF adopted in *Maxwell*, *Monroe*, and *Long*, all of which are fundamentally based on the normative "content" inquiry the Supreme Court set forth in *Katz*.[285]

---

282. *Larson*, 66 M.J. at 215 (quoting MIL. R. EVID. 314(d)).

283. *Id.* at 215–16. Although the CAAF opinion did not mention it, the intermediate appellate court relied on the fact that the office belonged to another service member who was deployed, still had the deployed member's personal things in it, and would be used (including the computer) upon the deployed member's return. *Larson*, 64 M.J. at 563.

284. *Larson*, 66 M.J. at 216. To a certain extent, in *Larson* the CAAF balanced its current and prior rulings on the head of a pin by referring to the scope of judicial review, leaving open the possibility of continuing developments. Military appellate courts review a military judge's decision to admit or exclude evidence for an abuse of discretion. *See* United States v. McCollum, 58 M.J. 323, 335 (C.A.A.F. 2003). In *Larson*, the CAAF reiterated its limited holding in *Long*, which only affirmed "the lower court was not clearly erroneous" in finding a subjective expectation of privacy, and stated in its present holding, "we agree with the [Court of Criminal Appeals] that the military judge did not abuse his discretion" in finding no expectation of privacy in Major Larson's government computer. 66 M.J. at 216.

285. Professor Freiwald argues that the Supreme Court, in *Smith v. Maryland*, 442 U.S. 735 (1979), similarly "avoided the normative inquiry required by *Katz*" by failing to discuss "the vital nature of the telephone system" and "whether telephone users should be entitled to expect their telephone numbers to remain protected by the Fourth Amendment." Freiwald, *supra* note 22, at 47.

In *O'Connor*, the Supreme Court relied on actual workplace practices to determine the reasonableness of the employee's privacy expectation.[286] It was not enough to aver summarily that a particular office was accessible to or subject to search by others.[287] What mattered was whether others actually accessed the office, how often, and in what manner.[288] In *Larson*, however, the CAAF cited the fact that "fire department and the command's facility manager" had keys to Major Larson's office, but never queried how often they actually used those keys to enter the office in Major Larson's absence.[289] Similarly, the court found that both the systems administrator and commander could access the computer's hard drive without Major Larson's password, but did not discuss whether they had ever done so.[290] Further, while it was important to the intermediate appellate court's opinion that Major Larson occupied a deployed member's office, the CAAF's opinion did not mention that the office was only temporarily assigned to Major Larson, still had the deployed officer's personal things in it, and would be reoccupied by the deployed officer upon his return.[291]

---

286. *See supra* text accompanying notes 68–73.

287. In *United States v. Kahan*, the district court expressly found that government employees have an expectation of privacy from government criminal investigators and government supervisors may not provide third-party consent to private office areas. 350 F. Supp. 784, 795–96 (S.D.N.Y. 1972); *see also supra* text accompanying notes 74–80 (discussing *Kahan*). In *Larson*, the CAAF completely overlooked *Kahan* and the Supreme Court's endorsement of it in *O'Connor*. *Larson*, 66 M.J. at 215–16. *But see* United States v. Muniz, 23 M.J. 201, 205–06 (C.M.A. 1987) (citing Mancusi v. DeForte, 392 U.S. 364, 369–70 (1968), for the proposition that "a business supervisor [can] consent to the search of company property in the custody of a subordinate").

288. *See supra* text accompanying notes 68–73.

289. *Larson*, 66 M.J. at 214. As one blogger noted on CAAFlog, a blog about military law, in response to *Larson*:

> Does the fact that a fire dept (or a cleaning person) has [sic] access to a space means it is not private? Of course not. Society still expects that space to be private, notwithstanding who might have keys. Otherwise, the fact that an apartment building manager has keys to your apartment would destroy your expectation of privacy.

Posting of Dwight Sullivan to CAAFlog, Government Computers and Expectations of Privacy, http://caaflog.blogspot.com/2008/04/government-computers-and-expectation-of.html (Apr. 27, 2008 11:09 PM).

290. *Larson*, 66 M.J. at 214.

291. *Compare Larson*, 66 M.J. at 214–16, *with Larson*, 64 M.J. at 563. With no exigent circumstances presented as to why the AFOSI did not obtain search authorization when it clearly could have done so, the Supreme Court's reasoning in *Chapman v. United States* is especially applicable: "We think it must be concluded here, as it was in *Johnson*, that 'If the officers in this case were excused from the constitutional duty of presenting their evidence to a magistrate, it is difficult to think of a case in which it should be required.' " 365 U.S. 610 (citing Johnson v. United States, 333 U.S. 10, 15 (1948)).

Similarly, the CAAF chose not to inquire into whether and to what extent the purpose of the intrusion—law enforcement—factored into the reasonableness of Major Larson's privacy expectation. In *Monroe* and *Long*, the court's holdings largely turned on the distinction raised by the Supreme Court in *O'Connor* regarding the purpose of the search. In *O'Connor*, the Supreme Court held that employers require wide latitude to ensure "the efficient and proper operation of the workplace," but distinguished between employer intrusion for work-related and law enforcement purposes.[292] Thus, employees may not have a reasonable privacy expectation against work-related intrusion by fellow employees and supervisors, but may have a reasonable privacy expectation against police intrusion. In *Larson*, however, the CAAF avoided this inquiry, even though AFOSI agents who were cooperating with civilian authorities in a clearly criminal investigation conducted the search.

Finally, the CAAF failed to explore the rather technologically savvy analytical hook the Air Force Court of Criminal Appeals used in resolving the case's work-related/law enforcement conundrum. The conundrum may be approached as follows:

- The search of Major Larson's office was conducted pursuant to a criminal investigation. Although it was work-related in the sense that, in the military, workplace misconduct may constitute criminal misconduct, the crimes at issue generally did not pertain to Major Larson's duties.

- Based on the testimony of Major Larson's commander, who testified that he and others had access to Major Larson's office and computer, Major Larson probably did not have a reasonable expectation of privacy against his work associates for work-related intrusions. The fact that Major Larson was occupying a deployed member's office also militates against finding a work-related privacy expectation.

- The conclusion that Major Larson did not have a reasonable expectation of privacy for work-related intrusions does not mean that he did not have a reasonable expectation of privacy against intrusions for law enforcement purposes. If the logon banner was limited to "monitoring," and if Major Larson's office and computer were not

292. O'Connor v. Ortega, 480 U.S. 709, 721 (1987) (plurality opinion) ("While police, and even administrative enforcement personnel, conduct searches for the primary purpose of obtaining evidence for use in criminal or other enforcement proceedings, employers most frequently need to enter the offices and desks of their employees for legitimate work-related reasons wholly unrelated to illegal conduct.").

> routinely monitored and searched, arguably, he could have had a reasonable expectation of privacy against a law enforcement search of his computer files.[293]

To avoid this conundrum, and the conclusion to which it may have lead, the intermediate appellate court relied on the fact that the files downloaded by Major Larson were temporary Internet files, "recorded automatically, not for law enforcement purposes" as part of " 'normal operating procedure' of the Microsoft Windows operating system."[294] By finding they were automatically recorded files, which the deployed service member could have found upon his return, the court sidestepped the law enforcement issue.[295] This approach does not completely resolve the issue as the search itself was still for law enforcement purposes, but it at least acknowledges the notion that reasonableness depends on the purpose of the search.[296]

Whatever the shortcomings of *Larson*, there is little doubt that those who had expressed dismay over the holding reached by the CAAF in *Long* were relieved by the apparent turnabout in *Larson*.[297] Not everyone, however, viewed *Larson* as a complete panacea for the problems caused by the court's holding in *Long*.[298] Perhaps several reasons support such caution. First, as the Air Force Court of Criminal Appeals noted in its intermediate appellate opinion, *Larson* is almost a matter of first impression.[299] Second, unlike *Maxwell*, *Monroe*, and *Long*, which all addressed communications privacy as it

---

293. One downside of emphasizing "actual" workplace practices is that it creates a perverse incentive for employers to routinely invade their employees' workspaces to nip any expectation of privacy in the bud before it has a chance to grow.

294. *Larson*, 64 M.J. at 563.

295. *Id.*

296. The *Larson* court could have drawn on *United States v. Muniz* for guidance. United States v. Muniz 23 M.J. 201 (C.M.A. 1987); *see also supra* text accompanying notes 82–87. As discussed above, in *Muniz* the Court of Military Appeals addressed whether a service member had a reasonable expectation of privacy in the address on an envelope kept in a locked credenza in a lockable private office. 23 M.J. at 205 n.5. In discussing the service member's reasonable privacy expectations, the court observed, "[t]he government property was the drawer itself. Assuming the legitimacy of that entry, the return address, on what was undeniably private property, could apparently be seen in plain view." *Id.* (citation omitted). In *Larson*, the temporary Internet files were stored on Major Larson's hard drive, a locked but accessible "container." *Larson*, 64 M.J. at 563. Like the envelope in *Muniz*, the CAAF could have found that the Internet files were "envelope" information available for public view (though whether temporary Internet files are "envelope" or "content" information is still unresolved). *See* Tokson, *supra* note 21, at 2109.

297. *See supra* Section III.C.4.

298. *See* Mendelson, *supra* note 9, at 9 (urging judge advocates to continue seeking probable cause search authorization for government e-mail accounts even after *Larson*).

299. *Larson*, 64 M.J. at 563.

pertained to e-mail, *Larson* involved the government computer itself, making it much more like earlier military cases addressing privacy interests in a government desk or credenza than a true communications privacy case. Finally, *Larson* pre-dated the DoD's new logon banner and user agreement policy, which has yet to be reviewed by military appellate courts.[300] As discussed in Part IV below, to the extent that military authorities and investigators rely on *Larson* for the proposition that the government may conduct warrantless searches of government e-mail accounts for law enforcement purposes, they may be doing so at their own risk.

IV. THE LANDSCAPE AFTER *LONG* AND *LARSON*

Having surveyed the law of workplace privacy in the military and the guidepost communications privacy cases issued by the CAAF, this Part turns to the DoD's response to the *Long* decision. This Part first reviews the DoD's new logon banner and user agreement policy. It then explores the possibility that the DoD's new logon banner constitutes an unconstitutional violation of U.S. service members' Fourth Amendment rights by functioning as a general warrant. I advocate for a revised policy based on a normative determination that electronic communications—even in the workplace—are sufficiently vital to warrant limited workplace protections. This Part then concludes by suggesting that both military interests and individual service member interests are best protected by a legal standard that requires probable cause search authorization whenever the primary purpose of a search is law enforcement.

A. THE DOD'S NEW LOGON BANNER AND CONSENT AGREEMENT

For military practitioners struggling to reconcile the holdings of *Long* and *Larson*, two dissimilar factual findings must have seemed particularly thorny. First, the *Long* court placed significant weight on the systems administrator's testimony that "it was a general policy to avoid examining e-mails and their content because it was a 'privacy issue.' "[301] The court noted that the systems administrator "repeatedly emphasized the agency practice of recognizing the privacy interests of users in their e-mail"[302] and that it found "the testimony of the network administrator, describing the agency practices and policies to be most persuasive."[303] In *Larson*, however, the military commander testified "he could log onto [Major Larson's] computer with his own password and

300. *See infra* text accompanying note 323.
301. United States v. Long, 64 M.J. 57, 60 (C.A.A.F. 2006).
302. *Id.* at 63.
303. *Id.* at 64.

access all portions of the hard drive unless [Major Larson] protected something with his own password."[304] Although the court in *Larson* did not state whether the commander had actually logged onto Major Larson's computer, it found the possibility that he could do so persuasive.[305] Comparing these two approaches, it appears that the CAAF was concerned with the *practice* of intrusion in *Long*, but only the *possibility* of intrusion in *Larson*.

The second prickly point in both cases is the logon banner. In *Long*, the court relied heavily on the language of the logon banner, which "described access to 'monitor' the computer system, [but] not to engage in law enforcement intrusions by examining the contents of particular e-mails in a manner unrelated to maintenance of the e-mail system."[306] As a result, the court found that military authorities overstepped their bounds by intruding for law enforcement purposes.[307] In *Larson*, however, the logon banner appeared to say much the same thing, but it led the court to a different conclusion. The logon banner "state[d] that it was a DoD computer, it [was] for official use, [and] not to be used for illegal activity."[308] The banner "also had a statement that users of the computer consent to monitoring."[309] Yet, the *Larson* court found the banner was sufficient to place Major Larson "on notice that the computer was not to be used for illegal activity and that there could be third-party monitoring."[310]

---

304. United States v. Larson, 66 M.J. 212, 215 (C.A.A.F. 2008).

305. To me, it is troubling that the court was persuaded by the fact that the commander could (but not necessarily did) log onto the network using Major Larson's computer. First, it is not surprising that the commander—who apparently had a network account—could access the network by logging onto it from Major Larson's networked computer. Second, analogizing the computer to an office, the mere fact that a supervisor can access an employee's office is hardly grounds, at least under *O'Connor*, an employee does not have reasonable expectation of privacy in the computer. *O'Connor* seems to stand for the proposition that it is office practices—not possibilities—that define what is and is not reasonable for Fourth Amendment workplace privacy protections. *See* O'Connor v. Ortega, 480 U.S. 709 (1987) (plurality opinion). Third, there is no evidence that Major Larson even knew the commander could log onto his computer.

306. *Long*, 64 M.J. at 63.

307. *Id.* at 63, 65.

308. *Larson*, 66 M.J. at 216.

309. *Id.*

310. *Id.* As far as I know, no government property—or any other property—is intended to be used for illegal activity. To the extent the court relied on this provision to negate a subjective or objective expectation of privacy, its reliance appears to be misplaced. A prohibition against illegal use hardly seems the same as a knowing consent to a search for illegal use.

The questions left by these cases are tangled. With respect to access, does a user retain a reasonable privacy expectation in his e-mail (or computer) when a systems administrator can—but normally does not—access the user's e-mail account? Or is the mere possibility that a third party can access the e-mail (or computer) enough to extinguish the user's privacy interest? With respect to monitoring, does a user have to be on notice that his computer activity may be monitored for both work-related and law enforcement purposes, or is it sufficient to simply instruct the user that monitoring may occur and the system may not be used for illegal purposes?

The DoD's response to these questions was to revise and broaden its logon banner.[311] On May 8, 2008, two years after *Long* and a few weeks after *Larson*, the DoD issued its "Standard Consent Banner and User Agreement" policy, notifying users that DoD computer communications were not private and could be monitored, searched, inspected and seized at any time and for any purpose.[312] The new policy required all DoD computer systems to adopt the new banner within sixty days, and encouraged widespread training, publication, and security awareness briefings to inform DoD users of the policy. Attachment 1 to the Banner and User Agreement policy contained the new Standard Mandatory DoD Notice and Consent Banner, which DoD users were to acknowledge each time they logged onto their computers:

311. *See* Ladue, *Impact on Investigations*, *supra* note 257 (noting the "Joint Task Force–Global Network Operations is updating the banner and requesting approval from the DoD Chief Information Officer so that the DoD Notice and Consent Banner will preclude any claims to an expectation of privacy on base network servers for e-mails or any other digital evidence").

312. Memorandum from John Grimes, Chief Info. Officer, Dep't of Defense to Sec'ys of the Military Dep'ts (May 9, 2008). The new policy directly impacted service regulations. For example, a prior version of the U.S. Army's Information Assurance regulation "specifically stated that computer users had a reasonable expectation of privacy." Edell, *supra* note 9, at 1 n.7 (citing U.S. DEPARTMENT OF ARMY, REGULATION 25-2, INFORMATION ASSURANCE para. 4–5r (Nov. 14, 2003)).

Figure 1: Standard Mandatory DoD Notice and Consent Banner

ATTACHMENT 1
STANDARD MANDATORY
DOD NOTICE AND CONSENT BANNER

[A. Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."]

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.

OK

[B. For Blackberries and other PDAs/PEDs with severe character limitations:]

I've read & consent to terms in IS user agreem't.[313]

313. Memorandum from John Grimes, *supra* note 312, at Attachment 1.

Attachment 2 to the Banner and User Agreement policy contained the new mandatory User Agreement, which DoD users were required to sign:

Figure 2: Standard Mandatory Notice and Consent Provision

ATTACHMENT 2
STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access

Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.
- You consent to the following conditions:
  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and seize data stored on this information system.
  - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.
    - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below: Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in

> accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
>
> - All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.[314]

Under the terms and conditions of the new Banner and User Agreement policy, use of a government information system constitutes consent for the government to access users' communications and data for any purpose, including "penetrations testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) activities."[315] In addition, users consent that "[c]ommunications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose."[316]

By addressing both "privacy" and "law enforcement" simultaneously, the new Banner and User Agreement directly responded to the facts of *Long*. No longer could systems administrators testify of a "general policy to avoid examining e-mails and their content because it was a 'privacy issue.' "[317] No longer could courts find logon banners insufficient in notifying users of law enforcement monitoring and searching.[318] On its face, the policy extinguished any reasonable privacy expectation users had in their government computer activity, with the exception of activity related to privileged communications (i.e., attorneys, psychotherapists, clergy, and their assistants).[319] In addition, to

314. *Id.* at Attachment 2.

315. *Id.*

316. *Id.*

317. United States v. Long, 64 M.J. 57, 60 (C.A.A.F. 2006).

318. *See id.* at 64.

319. Memorandum from John Grimes, *supra* note 312, at Attachments 1 and 2. A discussion of the potential impact of the new Banner and User Agreement on privileged communications is beyond the scope of this Article. However, some commentators have expressed concern. *See, e.g.*, Edell, *supra* note 9, at 17; William H. McMichael, *Lawyers: DoD rule threatens confidential client e-mails*, ARMY TIMES, June 16, 2008, at 22. For a discussion of workplace e-mails and the attorney–client privilege, see Kelcey Nichols, *Hiding Evidence from the Boss: Attorney–Client Privilege and Company Computers*, 3 SHIDLER J.L. COM. & TECH. 6 (2006).

the extent a limited reasonable expectation of workplace privacy in a government computer still existed under *O'Connor*, the Banner and User Agreement policy established that law enforcement searches were based on user consent and, thus, did not require search authorization.[320]

The core question, of course, is whether the Banner and User Agreement policy structurally changed the communications privacy underpinnings that led the *Long* court to its holding, or if it simply rearranged the factual furniture. Certainly, response to the new logon banner was mixed. The legal division of the Air Force Office of Special Investigation announced that criminal search authorization was no longer required for government computers,[321] while attorneys from the Air Force Government Trial and Appellate Operations Division (who, interestingly, were the ones who successfully argued *Larson* before the CAAF) urged practitioners not to read *Larson* too broadly and to continue seeking search authorization for criminal searches of government information systems.[322] As discussed below, the jury is still out on this issue—and for good reason.

---

320. In her dissent in *Long*, Judge Crawford argued the search was permissible even assuming a reasonable expectation of privacy, because Lance Corporal Long had consented to the search by clicking the logon banner. *Long*, 64 M.J. at 70 (Crawford, J., dissenting). As discussed below, however, it is debatable whether clicking on a mandatory logon banner constitutes consent under MRE 314(e)(4). *See infra* text accompanying notes 352–54354.

321. In a background paper issued for Air Force attorneys, the legal division of AFOSI stated:

> [W]ith exceptions for privileged communications, . . . [law enforcement] . . . investigators seizing, searching, and intercepting communications or data stored on 1) a bannered government computer in a government office lacking an expectation of privacy, or 2) a base network control center (BNCC) storing data transmitted from a bannered government computer, may do so without a criminal search authorization . . . in accordance with the revised DoD Notice and Consent Banner/User Agreement and findings in *Larson*.

AFOSI/JA, *Background Paper on the Revised DoD Notice and Consent Banner and* U.S. v. Larson, U.S. AIR FORCE, Jun. 19, 2008 (on file with author), *quoted in* Mendelson, *supra* note 9, at 9.

322. In her column, Captain Mendelson, an appellate attorney for the Air Force, cautioned practitioner's against adopting AFOSI's blanket approach:

> We strongly advise against any blanket policy that a search authorization need not be sought. To the contrary, we advise that in every case a search authorization should be sought. We fully appreciate that *Larson* was a major victory for the Government, and that the newly revised DoD consent banner will address some of the issues present in *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006) (holding the servicemember had a reasonable expectation of privacy in her government email stored on a government server). However, we caution that *Larson* can be distinguished in future cases, particularly with respect to the Court's reliance on the fact that *Larson* presented no evidence that he enjoyed a *subjective* expectation

B. GENERAL WARRANTS AND FOURTH AMENDMENT PROTECTIONS

Military courts have yet to address a case involving the new Banner and User Agreement.[323] However, a number of factors militate in favor of seeking search authorization for search and seizure of service members' workplace communications.[324] First, as previously discussed, the analytical shortcomings of the court's reasoning in *Larson*—even if ultimately leading to the correct conclusion—caution against giving this case too much precedential value. The court's opinion simply omits too many factual and legal signposts, including the *O'Connor* workplace privacy analysis, which could have led the court (or may lead the next court) to an altogether different destination. Second, as discussed below, it is at least questionable whether courts will uphold searches based on consent when, for military members, consent is arguably an unavoidable term and condition of employment. Like "general warrants" the Supreme Court has previously struck down, the new Banner and User Agreement policy could be argued to bestow *a priori* authority on DoD law enforcement officials to conduct broad, general searches to discover criminal misconduct. Third, as also discussed below, the Fourth Amendment requires, absent exigent circumstances, that "a neutral and detached" authority be interposed between the police and the public.[325] The new Banner and User Agreement policy may be viewed as violating this principle by authorizing ex parte criminal searches of potentially protected privacy expectations without judicial oversight or a commander's probable cause review. Finally, the voluntariness of service members' consent in agreeing to the new Banner and User Agreement policy is debatable. By virtue of the nature of military service, service members could claim little agency in choosing whether to accept or reject the policy's prospective, unbounded intrusions.

1. General Warrants and the Particularity Requirement

The Fourth Amendment, in addition to prohibiting "unreasonable searches and seizures," states that "no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly

> of privacy in the contents of his government computer. . . . While *Larson* is a very favorable case for the Government, it does not create a blanket rule obviating the need for search authorization and it should not be treated as such.

Mendelson, *supra* note 9, at 9.

323. At the time of this writing, a search revealed only five cases citing to *United States v. Larson*, 66 M.J. 212 (C.A.A.F. 2008), none of which addressed communications privacy.

324. This is the same approach recommended by attorneys from the Air Force Trial and Appellate Division. *See* Mendelson, *supra* note 9, at 9.

325. Johnson v. United States, 333 U.S. 10, 14 (1948).

describing the place to be searched, and the person or things to be seized."[326] The requirement for particularity "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[327] Both courts and commentators have observed that the inclusion of the particularity requirement in the Fourth Amendment was in response to the pre-Revolutionary use of "general warrants," which, among other things, gave customs officials "blanket authority to conduct general searches for goods imported to the Colonies in violation of the tax laws of the Crown."[328]

Judicial consideration of general warrants extends back at least as far as 1765, when, in *Entick v. Carrington*, Lord Camden reviewed whether a general warrant by Earl Halifax "to search for and seize the [papers of Mr. Entick]" was issued in contravention to law.[329] The warrant—which included all of Mr. Entick's papers—had been issued under Earl Halifax's executive authority as a principal secretary of state for England to investigate suspected cases of seditious libel.[330] In his opinion, Lord Camden first held that the secretary of state was not empowered to issue warrants, an authority reserved by law to justices of the peace.[331] Then, in an analysis at once both colorful and brilliant, Lord Camden (a) articulated the dangers of such unchecked power, (b) dissected the argument that "this power is essential to government, and the only means of quieting clamors and sedition," and (c) explained the normative value inherent in individual privacy.[332] Although reflective of the strong connection between property interests and privacy rights in existence at the time, Lord Camden's reasoning is instructive in our consideration of electronic communications:

> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are

326. U.S. CONST. amend. IV.

327. Berger v. New York, 388 U.S. 41, 58 (1967) (quoting Marron v. United States, 275 U.S. 192, 196 (1927)) (internal quotation marks omitted).

328. *Id.* (noting the use of general warrants "was a motivating factor behind the Declaration of Independence" and the Fourth Amendment "repudiated these general warrants") (citations omitted); *see also* Freiwald, *supra* note 22, at 59 (2007) (discussing the framers' concern with general warrants and citing Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 619–68 (1999)).

329. Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).

330. *Id.*

331. *Id.*

332. *Id.*

> removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be *subversive of all the comforts of society*.[333]

Lord Camden then held that the general warrant to "seize and carry away the party's papers in the case of a seditious libel [was] illegal and void."[334]

Taking notice of *Entick v. Carrington*, the Supreme Court in *Berger v. New York* quoted Lord Camden's reference to privacy intrusions as "subversive of all the comforts of society."[335] Decided in 1967, *Berger* involved a New York statute which authorized "the issuance of the order, or warrant for eavesdropping, upon the oath of the attorney general, the district attorney or any police officer above the rank of sergeant stating that 'there is reasonable ground to believe that evidence of crime may be thus obtained . . . .' "[336] Pursuant to the statute, New York law enforcement officials had obtained a warrant for electronic surveillance that led to the discovery of evidence of a conspiracy relating to the issuance of state liquor licenses.[337]

In striking down the New York law, the Supreme Court held it failed to meet the Fourth Amendment's requirement for "particularization," observing, "[i]t lays down no requirement for particularity in the warrant as to what specific crime has been or is being committed, nor 'the place to be searched,' or 'the persons or things to be seized' as specifically required by the Fourth Amendment."[338] The Court then went on to explain that the purpose of the Fourth Amendment's probable cause requirement is "to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed. . . ."[339] Like general warrants, the New York statute left "too much to the discretion of the officer executing the order." Finally, the Court found additional cause for concern with the length of the two-month surveillance authorization of the warrant that effectuated "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause," the lack of a

333. *Id.* (emphasis added).
334. *Id.*
335. 388 U.S. 41, 49 (1967). Both *Berger* and *Katz* were both issued during the Court's 1967 term.
336. *Id.* at 54.
337. *Id.* at 45.
338. *Id.* at 56.
339. *Id.* at 59.

termination date "once the conversation sought is seized," and the lack of notice to the subject of the intrusion.[340]

For all intents and purposes, the Banner and User Agreement policy could be argued to function as a standing general warrant issued by an executive agency to search for evidence of general criminal misconduct. It goes well beyond the "monitoring" policies previously upheld in both civilian and military courts, which are soundly based on the "operational realities of the workplace" described by the Supreme Court in *O'Connor*[341] and easily connected to the authority in MRE 313 to conduct work-related inspections.[342] In effect, it permits the government to conduct continuous and unending law enforcement searches without meeting any of the requirements for particularity. To the extent that service members have a reasonable expectation of privacy in their workplace e-mail—and I do not argue that they always do—the policy appears to permit a privacy intrusion of the sort which Lord Camden found in 1765 to be subversive of "all the comforts of society,"[343] and which the Framers of the Constitution specifically intended to avoid.[344]

On the other hand, distinctions clearly exist between general warrants and the Banner and User Agreement policy. For example, one could argue there are substantive differences between entering a home to generally search and seize papers, and entering a military member's e-mail account to generally monitor, intercept, search, and seize e-mails.[345] This is especially true given the different complexion of constitutional guarantees for military members and the distinctiveness of military service.[346] However, we should ask whether the difference in privacy expectations held by the individual being intruded upon is a matter of kind or simply one of degree. As previously discussed, service members do not cast aside their cloak of constitutional protections simply by entering military service.[347] Factoring in the possibility that (a) with web-based e-mail, service members may be

340. *Id.*

341. O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion).

342. For a discussion of MRE 313, see *supra* text accompanying notes 48–51. *See also* Edell, *supra* note 9, at 23 (arguing "[t]he monitoring policy was consistent with an inspection under MRE 313 [as] an inspection directed at everyone using the network and subjecting everyone to the same level of scrutiny.").

343. Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).

344. *See supra* note 22.

345. After all, homes retain the highest Fourth Amendment protections, see Silverman v. United States, 365 U.S. 505, 511 (1961), while the workplace enjoys only limited Fourth Amendment protections. *See O'Connor*, 480 U.S. at 717–18.

346. *See supra* text accompanying notes 25–34.

347. *See supra* text accompanying notes 40–41.

accessing precisely the same e-mails from both home and work, (b) when deployed, service members may have no means of communication with family and friends other than computers and Internet access provided by the government,[348] and (c) military service regulations expressly authorize service members to use government information systems for limited personal use,[349] and the normative divide between communications privacy in the home and workplace—especially the military workplace—narrows considerably.

Analogizing the Banner and User Agreement policy to general warrants may be imperfect because service members are not subject to the same warrant requirements of the Fourth Amendment, and by extension, the particularity requirement. However, while the military is not subject to federal civilian warrant requirements,[350] MRE 315 does require both a probable cause review and a particular articulation of the property, evidence, or person to be seized, neither of which are incorporated into the Banner and User Agreement policy.[351]

Finally, one could argue that even if the Banner and User Agreement policy functioned as a standing general warrant, national security concerns provide enough particularity for its enforcement.[352] This argument is especially persuasive in light of the Fourth Circuit's holding in *United States v. Simons*, in which the internet policy of a division of the Central Intelligence Agency (a workplace vital to national security) effectively removed Mr. Simons' limited privacy interest in his workplace computer.[353] However, the Banner and User Agreement policy authorizes searches for any law enforcement purposes, not simply those linked to national security concerns. Moreover, as previously described, military courts in other contexts have

---

348. *See* Edell, *supra* note 9, at 23 ("Often e-mail is the only means of communication for deployed Soldiers.")

349. *See supra* text accompanying note 11. Edell observes that

> [t]he Army and DOD further reinforce a Soldier's expectation of privacy in government e-mail by allowing personal use. . . . The Army has even touted [Army Knowledge Online] 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.

Edell, *supra* note 9, at 23.

350. *See, e.g.*, United States v. Chapman, 954 F.2d 1352, 1367–70 (7th Cir. 1992) (finding while military procedures differ from federal civilian procedures, Fourth Amendment constitutional guarantees were upheld).

351. MIL. R. EVID. 315(b)(1), (f); *see also* United States v. Hester, 47 M.J. 461, 463 (C.A.A.F. 1998) ("To satisfy the *Fourth Amendment* and the Military Rules of Evidence, there must be probable cause for a search authorization, Mil.R.Evid. 315(f)(1), and the search authorization must be specific. Mil.R.Evid. 315(b)(1).").

352. For a brief discussion of national security concerns requiring stringent DoD communications monitoring, see *supra* text accompanying notes 256–60.

353. United States v. Simons, 206 F.3d 392 (4th Cir. 2000).

rejected a bright line rule that service members have no workplace privacy expectations, effectively establishing that national security concerns alone do not obviate all military workplace privacy expectations.[354]

2. Neutral and Detached Interposition

Absent exigent circumstances, both the Fourth Amendment[355] and MRE 315(d) require law enforcement officials to obtain authorization from a neutral and detached authority before conducting a search requiring probable cause.[356] As the Supreme Court noted in *Johnson v. United States*,

> [t]he point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.[357]

In the military, such search authority may be issued by a civilian magistrate in the form of a warrant, by a commander "who has control over the place where the property or person to be searched is situated or found," or by a military judge.[358]

In certain exigent circumstances, of course, law enforcement officials may dispense with the requirement to obtain a search warrant. In *Chapman v. United States*, the Supreme Court considered whether Georgia law enforcement officials properly entered a rented home when they did so with the landlord's consent but without a warrant.[359] Holding that the tenant's Fourth Amendment rights had been violated, the Court acknowledged that exceptional circumstances exist in which the warrant requirement may be obviated.[360] On the facts of the case, however, the Court found that "inconvenience to the officers and some slight delay necessary to prepare papers and present the evidence to a magistrate" did not constitute exigent circumstances.[361]

---

354. *See supra* text accompanying notes 83–88.

355. *See* Johnson v. United States, 333 U.S. 10, 14 (1948).

356. *See* MIL. R. EVID. 315(d).

357. 333 U.S. at 13–14, *quoted in* Chapman v. United States, 365 U.S. 610, 614–15 (holding warrantless search of rented home unlawful).

358. MIL. R. EVID. 315(b)(2), (d)(1)–(2).

359. 365 U.S. at 610–11.

360. *Id.* at 615.

361. *Id.* (quoting Johnson v. United States, 333 U.S. 10, 15 (1948)) (internal quotation marks omitted). The Supreme Court noted, "[n]o suspect was fleeing or likely to take flight,"

With respect to the new Banner and User Agreement policy, it is difficult to see what exigent circumstances warrant the DoD to extend its authority from routine work-related monitoring of its information systems to warrantless law enforcement searches.[362] In support of the Banner and User Agreement policy, perhaps it could be argued that the viability of electronic evidence is threatened by the logistical difficulty in obtaining search authorization. This seems unlikely. The scope of persons authorized to conduct probable cause reviews in the military (civilian magistrates, commanders, and military judges) is broader than it is in the civilian world, meaning there are more people to provide authorization in emergency situations.[363] By virtue of their military association, commanders and military judges are normally accessible to military law enforcement officials twenty-four hours a day, 365 days a year, regardless of duty location. Moreover, unlike civilian jurisprudence, the MRE do not require a sworn affidavit (although it is recommended) before search authorization is granted, and the authorization itself may be issued orally or in writing.[364]

Proponents of the Banner and User Agreement policy also could argue that the "operational realities" of military service require unrestricted access to otherwise constitutionally protected privacy interests for purposes of criminal investigations involving national security. As previously noted, constitutional protections do "take on a different complexion" when applied to members of the military,[365] in part because the military workplace "can range from an office building to a bunker or tent in a combat zone."[366] Furthermore, protection of national security assets from state and non-state actors is justifiably a critical concern.[367] However, the Banner and User Agreement policy goes beyond national security concerns by permitting

---

the search "was of permanent premises, not of a movable vehicle," and "[n]o evidence or contraband was threatened with removal or destruction. . . ." *Id.* (quoting Johnson v. United States, 333 U.S. at 15) (internal quotation marks omitted).

362. Some may criticize the characterization that the Banner and User Agreement policy extended, rather than reaffirmed, the scope of search authority which existed prior to *Long*. Certainly, the Air Force General Counsel Memorandum took the position that search authorization was not required prior to *Long* based on users' consent to the logon banner. *See* Memorandum from W. Kipling At Lee, Jr., *supra* note 257. Other branches of the service disagreed, however. Edell, *supra* note 9, at 23 ("Prior to the decision in [*United States v. Long*], the Army specifically ensured that Soldiers had a reasonable expectation of privacy from law enforcement during systems monitoring.").

363. MIL. R. EVID. 315(b)(2), (d)(1)–(2).

364. MIL. R. EVID. 315(b)(1).

365. United States v. Allen, 1999 CCA LEXIS 116, at *11 (A.F.C.C.A. April 22, 1999); *see also supra* text accompanying notes 25–34.

366. *Long*, 64 M.J. at 62.

367. *See supra* text accompanying note 152.

warrantless law enforcement searches for any purpose, essentially making permissible what arguably had been impermissible prior to the new policy. Moreover, even some military attorneys, who certainly are aware of national security needs of the military, argue for continued reliance on search authorization.[368] While "operational realities" may certainly justify stringent monitoring, perhaps we should ask whether they necessarily require warrantless searches that invade otherwise reasonable expectations of privacy. As the Supreme Court found in *Chapman*, "inconvenience to the officers and some slight delay necessary to prepare papers and present the evidence to a magistrate . . . are never very convincing reasons and, in these circumstances, certainly are not enough to by-pass the constitutional requirement."[369]

3. Voluntariness of Consent

One of the arguments advanced in support of warrantless law enforcement searches of government e-mail accounts is user consent.[370] By clicking the logon banner, proponents argue that service members have consented to the terms of the logon banner and, by extension, the scope of any search defined in the logon banner.[371] Those who sign user agreements are similarly agreeing to the scope of any search defined in the user agreement. In the case of the new DoD Banner and User Agreement policy, the scope of permissive searches is "any U.S. Government-authorized purpose[,]" which includes both "personnel misconduct" and "law enforcement . . . ."[372] Given the breadth of such language, the government has a strong argument that service members have provided a priori consent to general or specific searches for criminal evidence, even assuming *arguendo*

368. *See* Edell, *supra* note 9, at 24; Mendelson, *supra* note 9, at 9.

369. Chapman v. United States, 365 U.S. 610, 615 (1961) (internal quotation marks omitted) (citation omitted).

370. The Military Rules of Evidence provide "[s]earches may be conducted of any person or property with lawful consent." MIL. R. EVID. 314(e)(1).

371. *See, e.g.*, *Long*, 64 M.J. at 67–68 (Crawford, J., dissenting); Coacher, *supra* note 152, at 176–77 ("Under most circumstances, use of a government computer constitutes actual consent to systems protection monitoring. . . . Even if the act of accepting the conditions in the monitoring banner does not constitute actual consent, sufficient circumstances should exist to find implied consent . . . ."); AFOSI/JA, *supra* note 321, at 1 ("This revised DoD Notice and Consent Banner/User Agreement provides the consent necessary to satisfy the Federal Wiretap Act . . . and the Stored Communications Act . . . ."); Memorandum from W. Kipling At Lee, Jr., *supra* note 257, at 1 ("At the time of login on each properly configured Air Force computer an electronic banner appears. . . . Courts have consistently held that consent to monitoring eliminates any expectation of privacy.").

372. Memorandum from John Grimes, *supra* note 312, at Attachment 2.

they retain a reasonable expectations of privacy in their workplace communications.

This argument is not without considerable appeal. In her dissenting opinion in *United States v. Long*, Judge Crawford vigorously argued that even if Lance Corporal Long held a reasonable expectation of privacy, search authorization was unnecessary because she had consented to the logon banner, which, in Judge Crawford's view, contained language broad enough to encompass law enforcement searches:

> Even when there is a reasonable expectation of privacy, one of the exceptions is consent to search. Consent is such that one would not rely upon an assumption of risk that the service provider would not reveal this information to law enforcement officials. . . . Certainly, a communicator's expectation of privacy is not reasonable once he or she has given consent to search. . . . Where consent is given to an administrator or someone with mutual use of the property, the originators of e-mail assume the risk that the administrator may give consent to law enforcement officials.[373]

Judge Crawford thus identified two types of consent which may be relevant in evaluating a claim of e-mail privacy: the consent of the user and the consent of the systems administrator.[374] By agreeing to the logon banner, the user essentially assumes the risk that the systems administrator will consent to searches by law enforcement officials.[375] This is especially true, one might argue, if the banner explicitly mentions law enforcement searches, as does the new Banner and User Agreement policy.

The merits of this argument rise or fall on the validity of the consent. Under MRE 314, "consent must be given voluntarily," a question derived from all the circumstances.[376] If the voluntariness of consent is questioned at trial, the government must "show by clear and convincing evidence that such consent was, in fact, freely and voluntarily given."[377] Importantly, "[m]ere submission to the color of authority of personnel performing law

373. 64 M.J. at 70 (Crawford, J., dissenting) (internal citations omitted).

374. *Id.* Even if service members do not possess a reasonable expectation of privacy in their government e-mail, the SCA still requires law enforcement agents to obtain "service provider" consent from appropriate military officials. This assumes, of course, the military is a non-public service provider. *See* 18 U.S.C. § 2701(a); *see also* Kerr, *supra* note 115, at 1220 n.82.

375. *Long*, 64 M.J. at 70.

376. MIL. R. EVID. 314(e)(4); *see also* United States v. Middleton, 10 M.J. 123, 132–33 (C.M.A. 1981).

377. *Middleton*, 10 M.J. at 132 (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973)) (internal quotation marks omitted); *see also* Coacher, *supra* note 152, at 176 (discussing actual and implied consent by use of government e-mail).

enforcement duties or acquiescence in an announced or indicated purpose to search is not voluntary consent."[378]

Whether the government can prove by clear and convincing evidence that military service members have "freely and voluntarily" consented to the scope of searches in the new Banner and User Agreement policy remains to be seen. First, the government must overcome the argument that consent is hardly consensual when it is mandated as a term and condition of an employment relationship the employee is bound to continue.[379] Unlike their civilian counterparts, military members generally are obligated for a term of service and are not free to separate when they no longer approve of their employment conditions.[380] To leave is desertion, a criminal offense under Article 85, UCMJ, and to refuse to consent to the Banner and User Agreement policy (which, in turn, could prevent service members from accessing their computers and fulfilling their duties), could be construed as dereliction of duty in violation of Article 92, UCMJ. Second, to the extent service member consent is based on a contract theory of agreement, perhaps similar to the contracts at issue in *United States v. Hart*[381] and *United States v. Maxwell*,[382] the government must overcome the negative inference created by the inequality of bargaining power between the government and service members. As employees bound to their employer, service members have little choice in accepting the terms of the Banner and User Agreement policy.

---

378. MIL. R. EVID. 314(e)(4); *Middleton*, 10 M.J. at 133 ("An additional—and weighty—factor to be considered here is that for the Government to carry successfully its burden of proving that the 'consent' was, in fact, freely and voluntarily given, it must show that there was more than mere acquiescence to a claim of lawful authority.") (citations omitted).

379. Although military workplace privacy law generally follows civilian workplace privacy law, one of the distinctions is that service members are not free to leave their employ if they no longer agree with the terms and conditions of employment. As a result, civilian cases involving employees who "consent" to logon banners are only partially persuasive. In those cases, actual or implied consent can be imputed into the employee's decision to remain with the employer. In the military, it cannot. *See* AFOSI/JA, *supra* note 321, at 1 (citing only civilian cases to establish that employees may consent to searches by clicking logon banners).

380. *See In re* Grimley, 137 U.S. at 151–52. The Court held that

> Enlistment is a contract; but it is one of those contracts which changes the status; and, where that is changed, no breach of the contract destroys the new status or relieves from the obligations which its existence imposes. . . . By enlistment the citizen becomes a soldier. His relations to the State and the public are changed. He acquires a new status, with correlative rights and duties; and although he may violate his contract obligations, his status as a soldier is unchanged. He cannot of his own volition throw off the garments he has once put on . . . .

Id.

381. 2009 U.S. Dist. LEXIS 72473 (W.D. Ky. Aug. 17, 2009).

382. 45 M.J. 406 (C.A.A.F. 1996).

As such, courts could construe the Banner and User Agreement policy as a non-binding contract of adhesion.[383]

C. THE NEED FOR A NORMATIVE APPROACH

Foundationally, Fourth Amendment privacy analysis requires a normative inquiry into what "society is prepared to recognize as 'reasonable.' "[384] This is not a mechanical factual analysis into the limited privacy expectations a person has accepted as a cost of doing business as a citizen. Rather, as Justice Marshall observed in his dissent in *Smith v. Maryland*, it is an inquiry into "the risks [a person] *should* be forced to assume in a free and open society."[385] Justice Blackmun, writing the majority opinion in *Smith*, acknowledged as much when he conceded the possibility of situations in which the *Katz* two-part inquiry "would provide an inadequate index of *Fourth Amendment* protection," such as a general government announcement "that all homes henceforth would be subject to warrantless entry . . . ."[386] In that extreme situation, in which subjective privacy expectations had been obviated by "influences alien to well-recognized *Fourth Amendment* freedoms," a person's subjective expectation of privacy "could play no meaningful role in ascertaining what the scope of *Fourth Amendment* protection was" and a "normative inquiry would be proper."[387]

To a significant degree, the DoD's Banner and User Agreement policy amounts to a government announcement of the sort of warrantless search envisioned by Justice Blackmun in *Smith*. The Banner and User Agreement policy notifies DoD users that the government can search and seize otherwise protected communications for any and all purposes, including law enforcement, effectively quashing all subjective privacy expectations service members may have in their workplace communications. As a result, service members can never satisfy the *Katz* two-part inquiry. Absent the normative approach endorsed by Justice Marshall and notionally suggested by Justice Blackmun in *Smith*, service members' Fourth Amendment protections in their workplace electronic communications would be utterly extinguished.

Critics may object to my comparing Justice Blackmun's Orwellian vision to the Banner and User Agreement policy, arguing that the policy—and any searches conducted pursuant to it—is based on consent rather than executive

383. *See* BLACK'S LAW DICTIONARY 341(8th ed. 2004).

384. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Minnesota v. Olson, 495 U.S. 91, 97 (1990).

385. Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (emphasis added).

386. *Id.* at 741 n.5.

387. *Id.*

fiat.[388] As an "agreement" between parties, they might suggest, the policy is wholly unlike Justice Blackmun's unilateral government announcement "that all homes henceforth would be subject to warrantless entry . . . ."[389] However, there are two similarities. In theory, citizens who disagreed with the government's unilateral announcement about the warrantless search of their homes could, if they chose to do so, simply leave the country for a social contract elsewhere. Similarly, service members who disagree with the Banner and User Agreement policy could, if they choose to do so, refuse to sign the agreement and risk disciplinary action. In either case, however, the costs are so high as to render any implied consent (in the case of the citizen who chooses to remain in the country) or actual consent (in the case of the service member who accedes to the policy) anything but "freely and voluntarily" given.[390]

Even if the government *can* establish such an agreement, the normative question begging to be asked is *should* it? Applying Justice Marshall's reasoning to service members, what risks *should* service members be forced to assume as they serve their country? Is it reasonable for these risks to include communications privacy expectations that are not simply diminished, like those in the civilian workplace, but fully extinguished? Does it matter that service members work in foreign and remote environments where the only communications access they have is provided by the government?

While not always explicit, the tenor of analysis in the *Maxwell*, *Monroe*, and *Long* decisions suggests these were precisely the types of questions the CAAF was asking as it reflected on the privacy interests inherent in electronic communications. In *Maxwell*, the CAAF presciently observed the vital nature of electronic communications in modern society:

---

388. For example, in her dissent in *Long*, Justice Crawford specifically focuses on Lance Corporal Long's consent to the logon banner. United States v. Long, 64 M.J. 57, 70 (C.A.A.F. 2006) (Crawford, J., dissenting). The Air Force General Counsel likewise relied on the Air Force logon banner in its opinion that users had consented to any searches for law enforcement purposes. Memorandum from W. Kipling At Lee, Jr., *supra* note 257.

389. *Smith*, 442 U.S. at 741 n.5.

390. United States v. Middleton, 10 M.J. 123, 132 (C.A.A.F. 1981) (internal citation omitted). For additional discussion of consent, see *supra* text accompanying notes 370–75. Critics may also object that Justice Blackmun's hypothetical is based on the warrantless search of homes, not workplace information systems. To be clear, I am not arguing that warrantless searches of government computers or workplace electronic communications are equivalent to warrantless searches of homes, which retain the highest Fourth Amendment protections. *See* Silverman v. United States, 365 U.S. 505, 511 (1961). I am simply offering the unsurprising suggestion that a normative inquiry is requisite when the government pierces established Fourth Amendment protections through an agreement to which the other party is not in a position to disagree.

> New technologies create interesting challenges to long established legal concepts. Thus, just as when the telephone gained nationwide use and acceptance, when automobiles became the established mode of transportation, and when cellular telephones came into widespread use, now personal computers, hooked up to large networks, are so widely used that the scope of Fourth Amendment core concepts of "privacy" as applied to them must be reexamined. Consequently, this opinion and the ones surely to follow will affect each one of us who has logged onto the "information superhighway."[391]

The court went on to discuss the risks a user accepts in sending e-mail messages over a network by comparing e-mail to first-class mail and telephone calls.[392] With first-class mail and telephone calls, the originator bears the risk that the recipient will "reveal what is said to others."[393] The originator can reasonably expect, however, "the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause."[394] Similarly, the sender of an e-mail bears the risk of an e-mail being revealed by the recipient, but "enjoys a reasonable expectation that the initial transmission will not be intercepted by the police."[395] In *Monroe*, the CAAF expanded the e-mail sender's risk to include the risk of monitoring by systems administrators.[396] Even there, however, the CAAF noted, "[t]he transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[397] This proposition was tested—and upheld—in *Long*, in which the CAAF found that the "sole purpose of seizing the e-mails was to search for evidence of misconduct."[398]

The normative principles drawn from these cases are clear. First, despite distinctions, electronic communications merit privacy expectations similar to first-class mail and telephone. Second, users of electronic communications

391. United States v. Maxwell, 45 M.J. 406, 410 (C.A.A.F. 1996). As of 2008, nearly 75% of U.S. households had Internet access, approaching the ubiquity of telephone service. THE NIELSEN COMPANY, HOME TECHNOLOGY FACTBOOK, DEVICE AND SERVICE ADOPTION RATES (2008), http://en-us.nielsen.com/forms/report_forms/Nielsen_Home_Technology_Factbook. Congress has commented on the essential nature of information and communications services. *See* H.R. CONF. REP. NO. 109-702, at 840 (noting that "restoring basic information and communications capacity is a fundamental element of humanitarian and civic assistance" for civil military operations conducted in foreign locations).

392. *Maxwell*, 45 M.J. at 417–18.

393. *Id.* at 418 (citation omitted).

394. *Id.* at 417 (citation omitted).

395. *Id.* at 418.

396. United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000).

397. *Id.*

398. United States v. Long, 64 M.J. 65 (C.A.A.F. 2006).

should bear some risk—like telephone or first-class mail users—that the recipient of the communication will disclose it to others. Third, users of electronic communications should bear the additional risk that systems administrators will monitor the content of their communications when they have been notified of such monitoring by contract, user agreement, or logon banner. Fourth, given the vital role of electronic communications in society, a normative distinction between search and seizure of e-mails for work-related and law enforcement purposes is wholly appropriate. Users who bear the risk of intrusion by systems administrators should not be made—absent exigent circumstances—to bear the additional risk of intrusion by law enforcement. Instead of simply asking what *is* protected, policy makers and courts should ask what *should be* protected.

Based on these normative principles, I propose the following: (a) the DoD revise its Banner and User Agreement policy, providing robust system protection through monitoring, but omitting the authority to conduct warrantless searches for general law enforcement purposes, and (b) the CAAF limit its holding in *Larson* to its facts and require the DoD, like other federal agencies, to seek appropriate search authorization whenever its primary purpose in searching service members' electronic communications is law enforcement.

For a number of reasons, recognizing a limited privacy interest from law enforcement searches in service members' electronic communications could serve the interests of both service members and the military. First, it could boost morale among service members, who could communicate with friends and family from remote, deployed locations without fear that "big brother" is perusing every communication for signs of misconduct. Second, it would provide service members with workplace privacy protections similar to those as their civilian counterparts, who work alongside service members in preserving national security but who enjoy certain workplace privacy expectations from law enforcement, as opposed to work-related, searches. Third, it could promote efficiency of resources by forcing federal investigators to focus on specific crimes, rather than trolling through vast storehouses of communications for general evidence of criminal activity. Fourth, it could increase the quality of criminal evidence by interposing a neutral and detached probable cause search authority between investigators and the evidence they hope to search and seize. Fifth, it would honor the implicit commitment to privacy the military services have made to military family and friends in providing e-mail and instant messaging capabilities to communicate with deployed loved ones. Sixth, it would bring military judge advocates into the investigative process sooner rather than later, helping

investigators focus on criminal evidence which is particular, relevant, and admissible. Finally, it would recognize that service members, who take an oath to uphold the Constitution, are protected by those same constitutional guarantees. As Blackstone observed, "he puts not off the citizen when he enters the camp; but it is because he is a citizen, and would wish to continue so, that he makes himself for a while a soldier."[399]

V. CONCLUSION

It remains to be seen whether the CAAF's next communications privacy case will follow the reasoning in *Larson*, or return to the pre-*Larson* pattern of distinguishing work-related searches from those of law enforcement. It also remains to be seen whether the CAAF will entertain a constitutional challenge to the DoD's new Banner and User Agreement policy and, if so, will find it an appropriate exercise of executive authority. I have argued that the policy unnecessarily violates constitutional protections by expanding the DoD's search authority from mere systems monitoring, which is clearly work-related, to law enforcement, which the Supreme Court distinguished in *O'Connor*. In my view, there seems little to lose and much to preserve by adopting the view that service members, like their civilian counterparts, have a reasonable expectation of privacy from law enforcement searches in electronic communications sent over a government information system. Service members are deployed around the world in support of their country and often have no systems of communication to use other than those provided by the government. In that case, providing the limited workplace privacy protections recognized by the Supreme Court in *O'Connor* seems appropriate, especially given the normative importance of electronic communications in contemporary society. Doing so adheres to case law and ensures service members are protected by the very Constitution they are sworn to defend.

399. United States v. Culp, 14 U.S.C.M.A. 199, 206 (C.M.A. 1963) (quoting WILLIAM BLACKSTONE, COMMENTARIES *408 (Wendell ed.)) (internal quotation marks omitted).