NAVAL LAW REVIEW

ARTICLES

VOL. 48 2001

Published by the Naval Justice School, the NAVAL LAW REVIEW *encourages frank discussion of relevant legislative, administrative, and judicial developments in military and related fields of law.*

The NAVAL LAW REVIEW *is published from appropriated funds by authority of the Judge Advocate General in accordance with Navy Publications and Printing Regulations P-35.*

This issue of the NAVAL LAW REVIEW *may be cited as 48* NAVAL L. REV. *[page number] (2001).*

INFORMATION FOR AUTHORS

Authors are invited to discuss prospective articles with the NAVAL LAW REVIEW, editor at (401) 841-2437 ext. 121 or DSN 948-2437 ext. 121 or by writing to Editor, NAVAL LAW REVIEW, Naval Justice School, 360 Elliot Street, Newport, RI 02841-1523.

The editor, in conjunction with article editors, carefully reviews each manuscript for clarity, accuracy, and scholarly merit. The editor reserves the right to make editorial changes to a manuscript selected for publication. Manuscripts will not normally be altered in a manner inconsistent with the substance of the author's position. Where practical, the board will notify the author of any substantive changes before publication. There are no specific guidelines on manuscript length: brevity is not an obstacle to publication of a quality manuscript.

Manuscripts must be typed. The author should also submit a disk in WordPerfect or Microsoft Word compatible format. Authors should include an abstract of the proposed article, a short biography, and a statement as to whether the manuscript has been submitted elsewhere for publication. Per current directives, authors are solely responsible for security review. Authors may take a different position from that held by the government; when the author purports to state the views of the Department of the Navy or another governmental entity, however, security review is essential to ensure that the official position is stated accurately. No compensation can be paid for any articles published.

Articles should conform to the current edition of *A Uniform System of Citation* (17th ed.) and *Military Citation* (7th ed.). Authors should consult the *United States Government Printing Office Style Manual* (rev. ed 1984), on matters not addressed in *A Uniform System of Citation* (the "Bluebook").

David A. Berger
Lieutenant Commander,
Judge Advocate General's Corps
U.S. Navy
Editor

SUBSCRIPTIONS

Subscription information may be obtained by writing to the Managing Editor, NAVAL LAW REVIEW, Naval Justice School, 360 Elliot Street, Newport, RI 02841-1523. Publication exchange subscriptions are available to organizations that publish legal periodicals.

INDIVIDUAL PURCHASES

Individual copies of the NAVAL LAW REVIEW, formerly titled the *JAG Journal*, may be purchased by contacting the Defense Technical Information Center (DTIC) and the National Technical Information Service (NTIS) for republication and sale. Copies are not available from the Naval Justice School.

Commands not already registered with the DTIC may obtain registration forms and information on ordering publications by writing to:

Defense Technical Information Center
Attention: Code DTIC-FDRA
Cameron Station, Building 5
Alexandria, VA 22304-6145

COMM (703) 767-8273
DSN 427-8273
1-800-CAL-DTIC (225-3842)

Individual purchasers may obtain information on ordering publications by writing to:

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

An alternative means of obtaining the NAVAL LAW REVIEW is by downloading it from the Naval Justice School Web Page at www.njs.jag.navy.mil.

CONTENTS

Articles

Book Reviews

SEARCHING FOR PRIVACY IN ALL THE WRONG PLACES: USING GOVERNMENT COMPUTERS TO SURF ONLINE

Lieutenant Commander R. A. Conrad, JAGC, USN*

> ***It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.*** [1]

I. Introduction

This paper explores whether there is, or should be, a reasonable expectation of privacy in the use of government computer systems. Two primary sources of law apply when analyzing privacy issues in cyberspace.[2] The first is the Fourth Amendment.[3] The second is the Electronic Communications Privacy Act (ECPA).[4] Despite these constitutional and statutory protections, courts are unlikely to find that a reasonable expectation of privacy exists for persons sending or receiving electronic mail (e-mail) and surfing the Internet using government computer systems. However, federal agencies should establish policies and procedures for monitoring government computer systems that are designed to minimize intrusions on the subjective

---

Prior assignments include: Staff Judge Advocate, USS KITTY HAWK (CV 63), homeported in Yokosuka, Japan. Legal Assistance Attorney, Defense Counsel, and VITA/ELF Coordinator, Naval Legal Service Office Northwest, Bremerton, Washington. Imagery Intelligence Action Officer, United States Strategic Command, Omaha, Nebraska. Aviation Intelligence Officer, Patrol Squadron EIGHT, Brunswick, Maine. L.LM. The Judge Advocate General's School of the Army; J.D. Duke University School of Law. B.A. University of Vermont. Lieutenant Commander Conrad is currently assigned to the Naval Justice School as the Head, Legal Assistance Division. This article was edited by LCDR David A. Berger, JAGC, USN.

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

[2] U.S. DEP'T OF JUSTICE, SEARCH AND SEIZURE MANUAL, SEARCHING AND SEIZING COMPUTERS AND OBTAINING EVIDENCE IN CRIMINAL INVESTIGATIONS, Introduction (2001) (Computer Crime and Intellectual Property Section) [hereinafter, CCIPS MANUAL].

[3] *Id.*

[4] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-21, 2701-11, 3117, 3121-26 (1988)); CCIPS MANUAL, *supra* note 2.

privacy interests of individual users.

The principal Fourth Amendment hurdle is consent.[5] Users of government computers systems are required to view a warning banner when logging onto the system.[6] This banner clearly puts each user on notice that use

[5] Scott A. Sundstrom, *You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2090-93 (Dec., 1998) (arguing that by accepting workplace monitoring policies, employees consent to such monitoring) [hereinafter Sundstrom].

[6] A typical DoD notice contains language similar to the following:

> 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. . . . 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.

Message, 131256Z May 97, Chief of Naval Operations, subject: Communications Security (COMSEC) and Information Systems Monitoring Requirements; Message, 191445Z May 97, Commandant, Marine Corps, C4I-CIO, subject: Computer Notice and Consent Log-On Banner (Warning Screen) (19 May 1997) (citing Memorandum, Department of Defense General Counsel, subject: Communications Security (COMSEC) and Information Systems Monitoring (27 Mar.

of the system constitutes consent to monitoring.[7] The banner explains the reasons for monitoring, the type of monitoring that may take place, and the adverse consequences of unauthorized use of the system.[8] Proceeding beyond the banner establishes the user's implied, if not express, consent.[9]

The ECPA fails to provide any level of privacy protection because the government qualifies, under the statute, as a provider of electronic communications services.[10] The statute distinguishes between two types of providers of electronic communication services.[11] First, there are those who provide services to the general public, typically for a fee.[12] Second, there are those who only provide services to a limited, identifiable segment of users.[13] The latter group includes private employers and government agencies that provide e-mail services and Internet access to their employees.[14] The statute offers scant restraint on the monitoring activities of this second group of provider vis- -vis users.[15]

This paper will focus solely on Fourth Amendment analysis and the ECPA in the context of the monitoring of government—particularly Department of Defense (DoD)—computer systems.[16] While the conclusion of

---

1997)) [hereinafter CNO and CMC msgs].

[7] CNO and CMC msgs., *supra* note 6.

[8] *Id.*

[9] CCIPS MANUAL, *supra* note 2, at Part IV(C)(3)(b)(i).

[10] 18 U.S.C. § 2510.

[11] CCIPS MANUAL, *supra* note 2, at Part III(E).

[12] *Id.* Examples of such Internet Service Providers are America Online, Microsoft Network, Prodigy, Earthlink, and Netscape.

[13] *Id.*

[14] *Id.*

[15] *Id. See also*, Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).

[16] This paper will not discuss the extent to which private employers can monitor employee e-mail and Internet usage on employer computers and computer systems. The Fourth Amendment is not applicable to private employers, since it only applies to actions by government agents. *United States v. Jacobsen*, 466 U.S. 109, 113-15 (1984). The analysis under the ECPA is substantially the same. *See generally*, CCIPS MANUAL, *supra* note 2, at Part III(B). For more on this topic, see Amy Rogers, *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace*, 5.1 J. TECH. L. & POL'Y 1 (Spring, 2000) [hereinafter Rogers]; Rod Dixon, *With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age*, 4 J. TECH. L. & POL'Y 1 (Spring, 1999); Peter Schnaitman, *Building a Community Through Workplace E-Mail: The New Privacy Frontier*, 5 MICH. TELECOMM. & TECH. L. REV. 177 (1998/1999); Alexander I. Rodriguez, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L.J. 1439 (Fall, 1998); Jared D. Beeson, *Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read Their Employees' E-mail?*, 20 HAWAII L. REV. 165 (Summer/Fall, 1998); Kevin P. Kopp, *Electronic Communications in the Workplace: E-Mail Monitoring and The Right of Privacy*, 8 SETON HALL CONST. L.J. 861 (Summer, 1998); Anne L. Lehman, *E-Mail in the Workplace: Question of Privacy, Property or Principle?*, 5 COMMLAW CONSPECTUS 99 (Winter, 1997); Rod Dixon,

this paper is that courts are unlikely to find a reasonable expectation of privacy in the use of government computer systems, certain communications, at a minimum, should be protected from content monitoring.

In navigating the legal minefield of privacy law in cyberspace, the primary focus will be on three key decisions of the Court of Appeals for the Armed Forces (CAAF). Beginning with *United States v. Maxwell*,[17] the CAAF ventured into the uncharted territory of cyberspace.[18] In *Maxwell*, a case that did not involve the use of government computers, the CAAF recognized a limited reasonable expectation of privacy in the content of e-mail.[19] Where the use of government computers is involved, however, any such reasonable expectation of privacy is substantially degraded, if not completely eviscerated.

Next, in *United States v. Monroe*,[20] the CAAF reassessed *Maxwell*'s limited expectation of privacy in e-mail in the context of government computer systems. This time, the court appeared to conclude that there was no reasonable expectation of privacy.[21] Key to the decision were: (1) the computer contained a log-on banner warning notifying users that use constituted consent to monitoring; and (2) providers of electronic communications services were "specifically exempted from any statutory liability for unlawful access to stored electronic communications" under the ECPA.[22] However, the court stopped short of definitively finding that there was no reasonable expectation of privacy in the use of government computer systems. Instead, the CAAF hedged by agreeing with the lower court that there was no reasonable expectation of privacy vis- -vis the system administrators performing their official duties in monitoring the system and not viewing the files for law

---

Windows Nine-to-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications, 2 VA. J.L. & TECH. 4 (Fall, 1997); Jarrod J. White, *E-Mail @Work.Com: Employer Monitoring of Employee E-Mail*, 48 ALA L. REV. 1079 (Spring, 1997); Kevin J. Baum, *E-Mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011 (1997); and John Araneo, *Pandora's (E-Mail) Box: E-Mail Monitoring in the Workplace*, 14 HOFSTRA LAB. L.J. 339 (Fall, 1996).

[17] 45 M.J. 406 (1996).

[18] The CAAF's decision in *Maxwell*, while holding no precedential value outside the military courts, has been used as an analytical model by several federal district and circuit courts on the issue of privacy in cyberspace. *See* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999); United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999), *aff'd* 225 F.3d 656 (4th Cir. 2000), *and cert. denied*, 531 U.S. 1099 (2001); United States v. Stevens, 29 F. Supp. 2d 592 (D. Alaska 1998); United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997).

[19] *Maxwell*, 45 M.J. at 418.

[20] 52 M.J. 326 (2000).

[21] *Id*. at 330.

[22] *Monroe*, 52 M.J. at 326.

enforcement purposes.[23] Relying on the provision of the ECPA that permits disclosure to law enforcement of unlawful activity inadvertently discovered, the court further found that system administrators properly turned over the contents of Monroe's e-mails to law enforcement personnel.[24]

Finally, in *United States v. Allen*,[25] the CAAF again avoided deciding the issue of whether there could ever be a reasonable expectation of privacy in the content of e-mail sent through cyberspace from a government computer system. This time, finding no suppression remedy under the ECPA,[26] the court relied on the fact that the records at issue would have been inevitably discovered.[27] *Allen* is the most recently decided military case to consider the boundaries of privacy in cyberspace.

While the CAAF stopped short of deciding the ultimate issue, sooner or later there will be a case where this issue will have to be squarely decided. E-mail and use of the Internet have become more than just a form of entertainment. They have become the way the world communicates and conducts business. The military is no less affected by this phenomenon. Each service has a web site,[28] as do most individual commands.[29] Each federal government agency has a web site.[30] Each military service encourages its members to use e-mail and the Internet, because proficiency in this new medium is not just "nice to know," but is imperative.[31] At the same time, government computer systems are government resources and must be used appropriately.[32] To this end, as well as others (such as protection of national

---

[23] *Monroe*, 52 M.J. at 329-30.
[24] *Id*. at 331.
[25] 53 M.J. 402 (2000).
[26] *Id*. at 409 ("If Congress had intended to have the exclusionary rule apply, it would have added a provision similar to the one found under Title III of the statute, concerning intercepted wire, oral, or electronic communications.").
[27] *Id*. (stating "[w]e need not decide what type of privacy interest attaches to the information in this case . . . because . . . a warrant would have inevitably have been obtained for these very same records.").
[28] U.S. Navy: http://www.navy.mil; U.S. Marine Corps: http://www.usmc.mil; U.S. Army: http://www.army.mil; U.S. Air Force: http://www.af.mil; U.S. Coast Guard: http://www.uscg.mil; Army National Guard: http://www-ngb5.ngb.army.mil; Air National Guard: http://ang.af.mil.
[29] *See e.g.*, Links to Navy Web Sites on U.S. Navy home page at http://www.navy.mil. *See also*, U.S. DEP'T OF NAVY, SEC'Y OF THE NAVY INSTR. 5720.47, DEPARTMENT OF THE NAVY POLICY FOR CONTENT OF PUBLICLY ACCESSIBLE WORLD WIDE WEB SITES (1 July 1999).
[30] *See e.g.*,Defense: http://www.defenselink.mil; Justice: http://www.usdoj.gov; State: http://www.state.gov; Veterans Administration: http://www.va.gov; National Security Council: http://www.whitehouse.gov/nsc.
[31] *See infra* note 206 (U.S. Navy current policy).
[32] U.S. DEP'T OF DEFENSE, DIR. 5500.7R, JOINT ETHICS REGULATION 2-301 (C3, 12 December 1997) ("Federal Government communication systems and equipment (including Government

security), the monitoring of government computer systems serves a legitimate—if not compelling—government interest.[33]

Under the ECPA, the distinction between "content" and "context" monitoring of computer systems is critical, akin to the difference between a telephone operator listening to an entire conversation or simply recording the number called and the duration of the call. "Context refers to information about the electronic communication, including such things as the duration, size, and routing of the communication."[34] There is always a legitimate government interest in context monitoring.[35] With respect to the DoD, it is operationally imperative to protect communications systems and the communications infrastructure from unlawful intrusions.[36] It is also necessary, from a policy standpoint, to ensure that users of government computer systems adhere to basic standards of conduct.[37]

For the DoD, these standards are enumerated in the Joint Ethics Regulation (JER).[38] Public confidence in government is essential to our democratic way of life.[39] Public confidence in the military is important for the same reason. The appropriate use of government resources—to include government computer systems—is one key component of securing this confidence. Context monitoring of government computer systems, then, ensures that government computer systems are being used in a manner that will not erode public trust and confidence.[40] Content monitoring serves the same interests, but substantially infringes on individual user privacy and risks compromising the confidentiality of certain communications. Thus, there may be circumstances[41] where content monitoring should be proscribed. Such proscriptions are unlikely to come from the courts. Therefore, they must

---

owned telephones, facsimile machines, electronic mail, Internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official and authorized purposes only.") [hereinafter JER]; Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.101(b)(9) (2001) ("Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.").

[33] *See* Lieutenant Colonel LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See*, 46 A.F. L. REV. 155, 155-56 (1999) (providing indepth analysis of what author terms "system protection monitoring") [hereinafter Coacher].

[34] *Id*. at 173.

[35] *Id*. at 155-56.

[36] *See generally*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (Aegis Research Corp. 1999) [hereinafter SHARP].

[37] Coacher, *supra* note 33, at 155.

[38] JER, *supra* note 32.

[39] *Id*. at 2-100 (specifically, 5 C.F.R. § 2635.101(a) (2001)).

[40] Coacher, *supra* note 33, at 155.

[41] For example, privileged legal and medical communications, as well as those coming from higher command level intended for a limited audience.

come from the governmental agencies themselves, if at all.

This paper proposes that context monitoring should always be permissible on government computer systems. Systems administrators should be able to freely monitor and identify the sites visited by users of government computer systems to ensure that such use comports with ethical standards. Content monitoring, on the other hand, should be used judiciously. The specific recommendations set forth in the conclusion seek to strike a balance between the government's legitimate need to monitor e-mail and Internet usage, while at the same time giving some semblance of privacy to individual users.

II. Background

A. The Fourth Amendment

> ***[T]he Framers were men who focused on the wrongs of that day but who intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth.***[42]

The Fourth Amendment's core protection is to prevent the government from conducting unreasonable searches and seizures. First, there must be a search or seizure by a government agent, or by someone acting on behalf of the government. If the individual conducting the search is not a government agent, or acting on behalf of government agents, then the protections of the Fourth Amendment are not available.[43] In determining whether a private search becomes government action, the Tenth Circuit set forth a two-part test: "(1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."[44] An affirmative answer to both prongs is necessary "before an otherwise private search will be deemed governmental for Fourth Amendment purposes."[45]

---

[42] United States v. Chadwick, 433 U.S. 1, 8-9 (1977), *overruled on other grounds by* California v. Acevedo, 500 U.S. 565, 579-80 (1991).
[43] United States v. Jacobsen, 466 U.S. 109, 113-15 (1984).
[44] United States v. Kennedy, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000), *quoting* Pleasant v. Lovell, 876 F.2d 787, 797 (10th Cir. 1989). *See also*, United States v. Barth, 26 F. Supp. 2d 929, 935 (W.D. Tex. 1998); United States v. Holland, 18 M.J. 566 (A.C.M.R. 1984).
[45] *Kennedy*, 81 F. Supp. 2d at 1112 (citing United States v. Leffal, 82 F.3d 343, 347 (10th Cir. 1996)).

> This Court has . . . consistently construed this protection as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, ***even an unreasonable one***, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.[46]

If the search is being conducted by, or on behalf of, government agents, the issue becomes one of whether there is a legitimate expectation of privacy in the place to be searched, and whether the search is reasonable.[47] *United States v. Katz*[48] established the current test for determining whether the protections of the Fourth Amendment apply to a particular search. The central issue is whether there is a legitimate expectation of privacy in the place to be searched.[49] If there is no legitimate expectation of privacy, then there is no search and no Fourth Amendment protection.[50] The test has two prongs: (1) a subjective expectation of privacy on the part of the person asserting the right; and (2) whether that subjective expectation is one society is willing to recognize as reasonable.[51] Military courts apply this test to determine whether there is an expectation of privacy.[52]

The Fourth Amendment has adapted over the years to numerous technological advancements.[53] Fourth Amendment case law responding to

---

[46] United States v. Jacobsen, 466 U.S. 109, 113 (1984) (citation omitted; emphasis added). *See also*, United States v. Carter, 15 C.M.A. 495, 498 (1969) ("The Constitutional provision against unreasonable search and seizure has consistently been applied only to action by, or under the aegis of, Government authority.").

[47] Cady v. Dombrowski, 413 U.S. 433, 439 (1973) ("The ultimate standard set forth in the Fourth Amendment is reasonableness.").

[48] 389 U.S. 347 (1967).

[49] *Id.*

[50] *Id.* at 351.

[51] *Id.* at 361 (Harlan, J., concurring).

[52] United States v. Curry, 46 M.J. 733, 736 (N.M. Ct. Crim. App. 1997).

[53] *See* Amy E. Wells, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 109-110 (Spring, 2000) (tracing development of Fourth Amendment analysis from property-based protection in *Boyd v. United States*, 116 U.S. 616 (1886), through "constitutionally protected areas" in *Olmstead v. United States*, 277 U.S. 438 (1928), *overruled by Katz v. United States*, 389 U.S. 347 (1967), to the current 2-part test as enunciated in *Katz*) [hereinafter Wells]. *See also*, Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy For The Advancement of Technology?*, 48 DRAKE L. REV. 239, 240 (2000) ("The Fourth Amendment has, throughout its

these advancements has not always been consistent,[54] as it is not always a simple matter to apply old paradigms to new technologies. The key, as recognized by the Court in *Katz*, is to understand that "the Fourth Amendment protects people, not places."[55] In the realm of cyberspace, this is a critical foundational principle, particularly because cyberspace is not a "place," but rather an amorphous entity.[56] Unlike a person's house, there are no readily identifiable boundaries. "The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home . . . ."[57] And at present, in none is the zone of privacy less clearly defined than when unbounded by the completely ambiguous, non-physical dimensions of cyberspace.

The gigantic leaps in technology over the last decade[58] have created complex legal challenges never envisioned by the Framers of the Fourth Amendment.[59] Yet the Fourth Amendment has lost none of its vitality or purpose and, despite skepticism about the appropriateness of traditional Fourth Amendment analyses,[60] is utterly capable of adapting to this new frontier.[61]

---

history, not only faced technological advancement but has met technological challenges head on.") [hereinafter Bayens].

[54] Wells, *supra* note 53.

[55] *Katz*, 389 U.S. at 351.

[56] Wells, *supra* note 53, at 99 ("[C]yberspace has no physical geography; no territorial boundaries exist").

[57] Payton v. New York, 445 U.S. 573, 589 (1980).

[58] The Internet was "born" in 1969, as a Department of Defense project, but has really only been widely available to the general public since the early 1990s. David T. Cox, *Litigating Child Pornography and Obscenity Cases in the Internet Age*, 4 J. TECH. L. & POL'Y 1, ¶ 4 (Summer, 1999) [hereinafter Cox].

[59] United States v. Chadwick, 433 U.S. 1, 8-9 (1977), *overruled on other grounds by* California v. Acevedo, 500 U.S. 565, 579-80 (1991); Olmstead v. United States, 277 U.S. 438, 472-85 (1928) (Brandeis, J., dissenting) (stressing that Fourth Amendment protections are not limited to conditions and issues in existence at time of amendment; protections capable of adapting to new technologies).

[60] *See e.g.*, Darla W. Jackson, *Protection Of Privacy In The Search And Seizure Of E-Mail: Is the United States Doomed to an Orwellian Future?*, 17 TEMP. ENVTL. L. & TECH. J. 97 (Spring, 1999) [hereinafter Jackson]; Wells, *supra* note 53; Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61 (1999/2000) [hereinafter Skok]; Allegra Knopf, *Privacy and the Internet: Welcome to the Orwellian World*, 11 J. LAW & PUB. POL'Y 79 (Fall, 1999) [hereinafter Knopf].

[61] Bayens, *supra* note 53, at 240 ("The Fourth Amendment's simplicity and flexibility has permitted the judiciary to shape and mold its prescriptions into a timeless document."); Frances A. Gilligan & Edward J. Imwinkelried, *Cyberspace: The Newest Challenge For Traditional Legal Doctrine*, 24 RUTGERS COMPUTER & TECH. L.J. 305, 342 (1998) ("At a substantive level, the framework of contemporary Fourth Amendment doctrine proved satisfactory in *Maxwell*.") [hereinafter Gilligan & Imwinkelried].

It is important to understand the basics of how information moves through cyberspace and how truly fundamental a change in technology the Internet represents. When the Framers drafted the Fourth Amendment, post mail took days, weeks, even months in some cases, to reach the intended recipient. E-mail, by contrast, can travel across the world almost instantly.

> When we speak of the Internet . . . we are not speaking of something visual or tangible, rather we speak of something conceptual. . . . The Internet is not really a computer or even a set of computers, though computers help run it. The Internet is really just the communications system that computers use to interact, literally a super highway for information.[62]

The Internet is essentially a communications system used by computers to exchange information, utilizing existing telephone lines,[63] or, more recently, cable lines.[64] To make this happen, the Internet uses a technology called packet-switching protocols.[65]

> Packet switching allows data to be broken up in to small, identifiable packages and sent over various routes to the same destination. Computers that understand and use the protocol can create the data packets, send them, receive them and reassemble them in their original form. The protocols are written so that computers speaking different languages . . . can still communicate using the protocols.[66]

---

[62] Cox, *supra* note 58, at ¶ 88.
[63] *Id.* at ¶ 83.
[64] *See In re* United States Order Pursuant to 18 U.S.C. § 2703(d), 36 F. Supp. 2d 430 (D. Mass. 1999) (highlighting conflicts between the Cable Communications Privacy Act of 1984 and the ECPA that will be encountered as cable companies begin providing Internet service, and asking for an interpretation of 18 U.S.C. § 2703(d)) *and* United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000) (acknowledging the potential conflict, but not deciding the issue). *See generally*, Barbara Esbin, *Internet Over Cable: Defining the Future in Terms of the Past*, 7 COMMLAW CONSPECTUS 37 (Winter, 1999).
[65] Cox, *supra* note 58, at ¶ 84 (noting that another name for this is TCP/IP, or Transmission Control Protocol/Internet Protocol).
[66] Cox, *supra* note 58, at ¶ 84.

Computers, then, "talk" to each other over the Internet through existing communication lines.[67] This can take one of several forms, such as e-mail, web surfing, chat rooms, and bulletin boards. E-mail messages travel through the various Internet Service Providers (ISPs),[68] which act as central switching locations and as temporary storage facilities for reassembled messages, until they are "picked up" by the intended recipients.[69]

As one travels through cyberspace via the Internet, electronic footprints, commonly referred to as a "clickstream,"[70] are left behind.[71] These clickstreams can easily be, and routinely are, monitored, recorded and analyzed by private companies, ISPs, law enforcement, and anyone else with the requisite technical capability.[72] While advertisers and online merchants generally are only able to monitor a user's activity at particular web sites, "ISPs can precisely monitor and record an entire clickstream, since all of the user's online commands are sent through the ISP."[73] The reality is that we are extremely exposed to snooping when navigating through the Internet, including when we send or receive e-mail.[74]

---

[67] *Id.* at ¶ 85.

[68] Although there are several different levels of online services available, and the providers of such services may be called different things depending on the type of service they provide (e.g., Internet service providers, Internet access providers, remote service providers, network service providers, etc.), the term ISP will be used to generically include any commercial Internet access provider.

[69] Cox, *supra* note 58, at ¶ 85.

[70] Meaning, essentially, clickstream data that leaves an easily accessible and exploitable trail of a user's travel through cyberspace, recording every mouse click made and every web site visited.

> The name 'clickstream' refers to the series of mouse clicks users make as they travel the Web. Each click translates into an electronic signal which is then sent by the surfer's computer to the other computers on the Net, telling them what information to return to the user. Since online movement requires the user to send or request certain information from other computers on the Web, every step in cyberspace inevitably becomes part of the clickstream record.

Skok, *supra* note 60, at 64.

[71] *Id.* at 61.

[72] *Id.* at 61-70.

[73] Skok, *supra* note 60, at 66-67.

[74] *See generally*, Gilligan & Imwinkelried, *supra* note 61; Rogers, *supra* note 16; Skok, *supra* note 60; Deborah M. McTigue, *Marginalizing Individual Privacy on the Internet*, 5 B.U. J. SCI. & TECH. L. 5 (Spring, 1999) [hereinafter McTigue]; Suzanne M. Thompson, *The Digital Explosion Comes With a Cost: The Loss of Privacy*, 4 J. TECH. L. & POL'Y 3 (Spring, 1999) [hereinafter Thompson]; Myrna Wigod, *Privacy in Public and Private E-Mail and On-Line Systems*, 19 PACE L. REV. 95 (Fall, 1998) [hereinafter Wigod]; Joshua B. Sessler, *Computer Cookie Control:*

When using a government computer system, the government is effectively the ISP for any online activity performed through that system.[75] This is true even if the user accesses a commercial ISP account through a government computer system.[76] Thus the government can monitor clickstream data as a result of its employees using the Internet from a government computer system. ISPs, including the government and employers who provide e-mail and Internet capability to their employees, also have the capability to monitor the content of e-mails and any attached files, as these files pass through the system or network, often for temporary or back-up storage, when enroute from sender to recipient.[77]

Computers can be used directly, as a means of committing crime, such as identity theft, fraud, cyber-stalking, and transmitting and receiving child pornography.[78] Computers can also be storage repositories for evidence of criminal conduct, such as computerized records of drug transactions.[79]

Privacy interests in cyberspace do not exist solely vis- -vis the government.[80] While unscrupulous practices by law enforcement personnel are the ultimate evil targeted by the Fourth Amendment, other actors invade our privacy. These include employers (like the government), ISPs, web site providers, other users, and criminals.[81] "To evaluate protections of e-mail privacy, it is helpful to analyze the conflicting interests involved."[82] Obviously, there are individual privacy interests at stake.[83] But weighed heavily against these interests "are legitimate reasons why such protections should not be absolute."[84] There are law enforcement interests in preventing and punishing criminal behavior that harms innocent members of society, such as hacking, cyber-stalking, drug trafficking, identity theft, and child

---

Transaction Generated Information and Privacy Regulation on the Internet, 5 J.L. & POL'Y 627 (1997) [hereinafter Sessler]; Maria Helena Barrera & Jason Montague Okai, *Digital Correspondence: Recreating Privacy Paradigms*, 3 INT'L J. COMM. L. & POL'Y 4 (Summer, 1999) [hereinafter Barrera & Okai]; and Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (Nov. 1999) [hereinafter Schwartz].

[75] CCIPS MANUAL, *supra* note 2.

[76] *Id*. at Part III(B).

[77] *Id.; See also*, Wigod, *supra* note 74, at 103 and Sundstrom, *supra* note 5, at 2066-68.

[78] CCIPS MANUAL, *supra* note 2, at Part III(B).

[79] *Id.*

[80] Wigod, *supra* note 74, at 99-100.

[81] Wigod, *supra* note 74, at 99-100.

[82] *Id*. at 95.

[83] *Id*. at 96.

[84] *Id*. at 97.

pornography.[85] There are employment related interests, including ensuring the efficiency and propriety of employee conduct, protecting trade secrets and employer property, and guarding against vicarious liability for employee misconduct, such as sexual harassment and discrimination.[86]

There are various methods by which our privacy may be violated.[87] The collection of clickstream data, as discussed previously, is a prevalent means by which ISPs, merchants, advertisers, and others routinely obtain extensive data on Internet users, enabling a profile to be compiled about the user.[88]

"Cookies" are another means of invading the privacy of Internet users.[89] Cookies are user files that are placed on an Internet user's hard drive when a web site is accessed.[90] "In general, cookies allow sites to 'tag' their visitors with unique identifiers so they can be identified each time they visit."[91] "[A]ny information disclosed by a user while visiting a site (e.g. name, address, credit card number) could be stored in a cookie for later access by the web site."[92]

Search engines can also be programmed to collect information about users.[93] The most common data collected includes name, e-mail address, home address and phone number.[94] Other users can then retrieve this data by searching for key terms.[95] There are also more insidious collection practices.[96]

As discussed previously, ISPs—including employers—can monitor every single mouse click and every single site visited while a user is online, since every single movement on the Internet goes through the ISP.[97] While the ECPA places some limits on the information that ISPs can disclose, the license to collect is virtually unrestricted.

---

[85] *Id.*
[86] Wigod, *supra* note 74, at 97-98.
[87] *Id.* at 100-108.
[88] *Id. See also*, Skok, *supra* note 60.
[89] Wigod, *supra* note 74, at 101; Sessler, *supra* note 74, at 632-634.
[90] Sessler, *supra* note 74, at 632.
[91] *Id.* at 632-33.
[92] Wigod, *supra* note 74, at 101.
[93] *Id.* at 102-103.
[94] Wigod, *supra* note 74, at 103. (Wigod states that Altavista, Yahoo, Excite and Lycos each collect this type of data for possible retrieval by other users).
[95] *Id.*
[96] *Id.* at 102-103.
[97] *Id.* at 103; Skok, *supra* note 60, at 67.

Against this background, determining whether there is—or should be—a reasonable expectation of privacy when using government computers in cyberspace is not a simple matter of just looking at the privacy interests of the individual. The Supreme Court has recognized that the individual's right to privacy must be balanced against substantial government interests served by intruding on that privacy.[98] Where government computer systems are involved, there are numerous substantial government interests involved. All of these give rise to the necessity for systems protection monitoring.[99] Systems protection monitoring provides "[a] way of ensuring that government computer systems are protected and that the resource[s are] being used properly[.]" [100]

The first and foremost substantial government interest is proprietary, in that the computer system is the property of the United States Government. Ensuring the proper use of government resources is of paramount importance in maintaining the confidence of the American people in the Government.[101] "The Government has an interest in ensuring government-provided resources are not abused or used for any illegal or improper purpose." [102]

Equally high on the list is ensuring national security.[103] Government computer systems, which have become a central part of our governmental infrastructure and national defense, must be protected from hackers and cyber-terrorists who exploit the information gleaned from unauthorized access.[104] These threats to our safety and security cannot be overlooked.[105] Taking out our communications infrastructure, or tampering with it in any way, can utterly cripple our ability to defend ourselves in this modern, computer-driven world.[106] Notably, such attacks can be carried out remotely, from anywhere in the world.[107]

---

[98] O'Connor v. Ortega, 480 U.S. 709 (1987).
[99] *See generally*, Coacher, *supra* note 33.
[100] *Id*. at 155.
[101] JER, *supra* note 32, at 2-301; Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.101(a) (2001) ("Public service is a public trust.").
[102] JER, *supra* note 32, at 2-301; Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.101(b)(9) (2001) ("Employees shall protect and conserve Federal property and shall not use it for other than authorized activities."); *See also*, Coacher, *supra* note 33, at 155.
[103] Chris J. Katopis, *Searching Cyberspace: The Fourth Amendment and Electronic Mail*, 14 TEMP. ENVTL. L. & TECH. J. 175, 182 (Fall, 1995) [hereinafter Katopis].
[104] *See generally*, SHARP, *supra* note 36; David Hueneman, *Privacy on Federal Civilian Computer Networks: A Fourth Amendment Analysis of the Federal Intrusion Detection Network*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1049 (Summer, 2000) [hereinafter Hueneman].
[105] SHARP, *supra* note 36; Hueneman, *supra* note 104.
[106] SHARP, *supra* note 36; Hueneman, *supra* note 104. *See also*, Katopis, *supra* note 103.
[107] SHARP, *supra* note 36; Hueneman, *supra* note 104.

In the military, "demands of discipline and duty" may supercede the individual's right to privacy.[108] The Supreme Court has long recognized the military's unique nature.

> This 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." . . . Its law is that of obedience.[109] To prepare for and perform its vital role, the military must insist upon a respect for duty and a discipline without counterpart in civilian life.[110]

As the body charged with securing our national defense, the military is held to a higher standard of conduct by society. Therefore, assuring the appropriate, particularly non-criminal, conduct of military members in cyberspace is a substantial government interest that weighs heavily against the individual's legitimate expectation of privacy, especially when accessing the Internet through government computer systems.

B. The Electronic Communications Privacy Act

First and foremost, the case law in this area, particularly as it relates to cyberspace, is still very much in the developmental stages. There is no Supreme Court guidance. "The structure of the ECPA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests." [111]

> The ECPA consists of three distinct sections. The first section, often referred to as Title I, outlines statutory procedures for intercepting wire, oral, and electronic

[108] Coacher, *supra* note 33, at 165.
[109] Parker v. Levy, 417 U.S. 733, 743 (1974) (citations omitted).
[110] Schlesinger v. Councilman, 420 U.S. 738, 757 (1975).
[111] CCIPS MANUAL, *supra* note 2, at Part III (A).

> communications. The second section, known as Title II, pertains to stored communications. The final section, Title III, addresses pen registers and trap and trace devices.[112]

The ECPA "creates statutory privacy rights for customers and subscribers of computer network service providers . . . ."[113] Title I prohibits the "interception" of electronic communications with one huge exception.[114] The exception allows for a provider of Internet service (commercial ISPs, government service providers, private employer service providers) "to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . ."[115] This exception grants broad latitude to ISPs to "conduct business." There is also an exception for lawful electronic surveillance operations.[116] But perhaps most important, courts have narrowly construed "intercept," to the point where it is virtually inapplicable to electronic communications.[117]

Title II "creates statutory privacy rights for customers and subscribers of computer network service providers."[118] While the "ECPA exists largely to 'fill in the gaps' left by the uncertain application of Fourth Amendment protections to cyberspace . . . ",[119] it is important to understand that "[t]he ECPA does not represent a legislative determination of a reasonable

---

[112] Coacher, *supra* note 33, at 171.
[113] CCIPS MANUAL, *supra* note 2, at Part III.
[114] 18 U.S.C. § 2511.
[115] *Id*. at § 2511(2)(a)(i).
[116] *Id*. at § 2511(2)(a)(ii).
[117] *See* Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (seizure of computer containing unretrieved e-mail not an "intercept"); Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997) (viewing e-mail on another's computer screen not an intercept because not involving use of "electronic, mechanical, or other device"); United States v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997) (ruling that "intercept" requires acquisition contemporaneous with transmission); Bohach V. Reno, 932 F. Supp. 1232 (D. Nev. 1996) (holding that in determining whether "intercept" occurred, must distinguish between very narrow "transmission phase" and much broader "storage phase"); United States v. Reyes, 922 F. Supp. 818, 836 (S.D. N.Y. 1996) ("the acquisition of the data [must] be simultaneous with the original transmission of the data"); Coacher, *supra* note 33, at 173 ("To fall within the definition of intercept, the acquisition of the electronic communication's content must be contemporaneous with its transmission.").
[118] CCIPS MANUAL, *supra* note 2, at Part III(A).
[119] *Id.*

expectation of privacy in non-content information released by ISPs."[120] The portion of the ECPA pertaining to stored communications, 18 U.S.C. § 2701 *et seq.*, provides for civil damages and criminal penalties for violation, but "speaks nothing about the suppression of information in a court proceeding."[121] In other words, there is no built-in exclusionary rule for violations of this part of the statute.[122] The statutory privacy rights created by the ECPA in stored communications, as with Fourth Amendment analysis, apply only vis- -vis disclosure to government agents, also subject to a significant exception.[123] The contents of a stored communication can be disclosed to law enforcement agents if the contents were inadvertently discovered by the service provider (such as during the normal course of routine system monitoring or troubleshooting) and appear to indicate criminal activity.[124]

When litigating cyberspace issues under the ECPA, for the most part only Title II is applicable. Very few cases have applied Title I, and those that have interpret "intercept" very narrowly.[125] "To fall within the definition of intercept, the acquisition of the electronic communication's content must be contemporaneous with its transmission."[126] With respect to e-mail, this limitation is critical. "Given the narrow definition of intercept, Title I's provision prohibiting the interception of electronic communications may not apply to e-mail transmissions. In fact, the interception must occur as the e-mail is being transmitted in order for Title I to apply."[127] As a result of this

---

[120] United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999), *aff'd* 225 F.3d 656 (4th Cir. 2000), *and cert. denied*, 531 U.S. 1099 (2001).

[121] United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000). *See also*, United States v. Allen, 53 M.J. at 410.

[122] *See* 18 U.S.C. § 2701(b) (1988) (providing for criminal penalties), § 2707 (providing for civil remedies), and § 2708 ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.") (citations omitted); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000). *But see*, McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.C. 1998) (regarding a violation of 18 U.S.C. § 2703(c)(1)(B), "it is elementary that information obtained improperly can be suppressed where an individual's rights have been violated.").

[123] 18 U.S.C. §§ 2702–2703.

[124] *Id.* at § 2702(b)(6).

[125] *See e.g.*, Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (holding that unopened e-mails, sent to electronic bulletin board but not yet retrieved, found on seized computer were in "electronic storage," and thus not intercepted). Additional case law examples are provided in note 116.

[126] Coacher, *supra* note 33, at 173. *See Steve Jackson Games*, 36 F.3d at 360 ("[T]he Secret Service did not intercept the communications, because its acquisition of the contents of those communications was not contemporaneous with their transmission."). *See also*, Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997); United States v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997); Bohach v. Reno, 932 F. Supp. 1232 (D. Nev. 1996); and United States v. Reyes, 922 F. Supp. 818 (S.D. N.Y. 1996).

[127] Coacher, *supra* note 33, at 174.

minimal impact, this paper will not devote additional analysis to Title I.

Section 2703 of the ECPA, entitled "Requirements for Governmental Access" is the operative section concerning governmental access to stored communications. The best way to navigate the requirements of the statute is to classify the type of information sought and then determine whether what is being sought from the ISP is a compelled or voluntary disclosure.[128] There are three basic categories of information that might be obtained about a user from an ISP.[129]

The first of these categories is basic subscriber information.[130] ECPA section 2703(c)(1)(C) identifies the following types of information as pertaining to this category: name, address, telephone billing records, telephone number, subscriber identification number, duration of subscription to the service, and types of services utilized by the subscriber. The information under this category is afforded the lowest level of protection and can be provided to a governmental entity with a subpoena.[131]

The second category covers "record[s] or other information pertaining to a subscriber or customer of such service (not including the contents of a communication . . .)."[132] This type of information includes basic subscriber information as well as "transactional records, such as account logs that record account usage . . . and e-mail addresses of other individuals with whom the account holder has corresponded."[133] A provider of electronic communications services can disclose this type of information to anyone "other than a governmental entity" without apparent restriction.[134] However, such information can only be disclosed to a governmental entity pursuant to consent, a warrant, or a section 2703(d) court order.[135]

---

[128] CCIPS MANUAL, *supra* note 2, at Part III(C).
[129] *Id.*
[130] *Id.*
[131] 18 U.S.C. § 2703(c)(1)(C).
[132] *Id.* at § 2703(c)(1)(A).
[133] CCIPS MANUAL, *supra* note 2, at Part III(C)(2).
[134] 18 U.S.C. § 2703(c)(1)(A). *See* Jessup-Morgan v. America Online, 20 F. Supp. 2d 1105 (E.D. Mich. 1998).
[135] 18 U.S.C. § 2703(c)(B)(i)-(iii): A section 2703(d) court order,

> [M]ay be issued by any court that is a court of competent jurisdiction … and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information

The final category is contents. "The contents of a network account are the actual files stored in the account."[136] Stored e-mails are included in this category.[137] Disclosure of contents is governed by ECPA section 2702. There are several exceptions under this section, but the most important one is that contents evidencing criminal activity may be disclosed to law enforcement without any additional process "if the contents . . . were inadvertently obtained by the service provider . . . ."[138]

When discussing voluntary disclosure, it is important to distinguish between two types of providers of electronic communication services.[139] First, there are those who provide services to the general public, such as America Online (AOL).[140] Second, there are those who do not provide services available to the public, but rather to an identifiable segment, such as employers and government agencies.[141] These distinctions are critical when analyzing the voluntary disclosure provisions of ECPA sections 2702 and 2703(c).[142] "Providers of services not available 'to the public' may freely disclose the contents of stored communications."[143]

Providers of services to the public may disclose the contents of stored communications only in certain situations."[144] These situations include: inadvertent discovery of criminal activity; disclosure "necessarily incident to the rendition of service or to the protection of the rights or property of the provider of that service . . .";[145] mandatory disclosure pursuant to the Child Protection and Sexual Predator Punishment Act of 1998;[146] and disclosure "made to the intended recipient of the communication, with the consent of the

---

> sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d). There are four operative phrases under this section: (1) specific and articulable facts; (2) reasonable grounds to believe; (3) that the information sought is material and relevant; (4) to an ongoing criminal investigation.

[136] CCIPS MANUAL, *supra* note 2, at Part III(C)(3).

[137] *Id.*

[138] 18 U.S.C. § 2702(b)(6).

[139] CCIPS MANUAL, *supra* note 2, at Part III(E).

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] CCIPS MANUAL, *supra* note 2, at Part III(E). *See also*, Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).

[144] CCIPS MANUAL, *supra* note 2, at Part III(E); Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).

[145] 18 U.S.C. § 2702(b)(5). *See generally*, CCIPS MANUAL, *supra* note 2, at Part III(E).

[146] 42 U.S.C. § 13032. *See generally*, CCIPS MANUAL, *supra* note 2, at Part III(E).

intended recipient, to a forwarding address, or pursuant to a court order."[147]

One additional privacy-related issue concerns subscriber information provided to ISPs as a precondition to obtaining Internet access. From a Fourth Amendment perspective, the Supreme Court has generally held that there is no reasonable expectation of privacy in information voluntarily turned over to third parties.[148] However, the ECPA provides specific statutory guidance on this point and imposes certain requirements before such information may be turned over to a government agent.[149]

C. Maxwell, Monroe, and *Allen*

These three cases, decided by the CAAF, define the current parameters of military case law on the issue of privacy in cyberspace. *Maxwell* establishes that there can be a reasonable expectation of privacy in e-mail, but is limited in context to the practices and procedures of a particular ISP (e.g., America Online) and does not involve the use of government computer systems.[150] *Monroe*, at first glance, appears to establish that there is no reasonable expectation of privacy in the use of government computer systems.[151] However, the CAAF qualifies this proclamation by finding that there is no reasonable expectation of privacy "at least from the" system administrators.[152] In *Allen*, the CAAF sidestepped the issue of whether there can ever be a reasonable expectation of privacy in the use of government computer systems by relying on the doctrine of inevitable discovery.[153]

In *Maxwell*, United States Air Force Colonel James Maxwell used his personal home computer, only during off-duty hours, to access the Internet and send e-mails through AOL.[154] AOL's policy and practices provide heightened privacy protections to subscriber e-mail messages.[155] First, they are privately stored "on AOL's centralized and privately-owned computer bank located in

---

[147] CCIPS MANUAL, *supra* note 2, at Part III(E), *citing* 18 U.S.C. § 2702(b)(1)-(4).
[148] *See* United States v. Miller, 425 U.S. 435 (1976) (holding no reasonable expectation of privacy in bank records); Couch v. United States, 409 U.S. 322 (1973) (finding no reasonable expectation of privacy in financial records held by accountant); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000), *and cert. denied*, 531 U.S. 1099 (2001) (ruling no reasonable expectation of privacy in basic subscriber information maintained by ISP).
[149] 18 U.S.C. §§ 2701-11. *See generally*, CCIPS MANUAL, *supra* note 2, at Part III(B).
[150] 45 M.J. 406 (1996).
[151] United States v. Monroe, 52 M.J. 326 (2000).
[152] *Id.* at 330.
[153] United States v. Allen, 53 M.J. 402 (2000).
[154] *Maxwell*, 45 M.J. at 411.
[155] *Id.* at 417.

Vienna, Virginia."[156] Second, it is "AOL's practice to guard these [as] 'private communications' and only disclose them to third parties if given a court order."[157] When Colonel Maxwell signed up for service with AOL, he had to provide his name, address and billing information to AOL.[158] He then chose screen names.[159] The screen name is a unique identifier.[160] Colonel Maxwell chose at least two screen names, "Redde1" and "Zirloc."[161] Colonel Maxwell's screen name "Redde1" was provided by another AOL subscriber to the authorities as one of several screen names alleged to be distributing child pornography on AOL.[162] The FBI opened an investigation and obtained a search warrant to obtain information from AOL about the identities of the users for the identified screen names.[163] In anticipation of the warrant, AOL created a "software program to extract the anticipated requested information . . . ."[164] The software program not only extracted the user information for the identified screen names, but also provided additional screen names for the identified users, thereby exceeding the scope of the warrant.[165] Thus, Colonel Maxwell's other user name, "Zirloc," was provided in AOL's response to the search warrant.[166] While there was no child pornography associated with the "Zirloc" screen name, it did contain e-mails from Colonel Maxwell to a junior Air Force officer discussing Colonel Maxwell's sexual orientation.[167] The FBI turned its files on Colonel Maxwell over to the Air Force for prosecution.[168] Colonel Maxwell was ultimately convicted of offenses pertaining to child pornography, pursuant to his "Redde1" screen name, and communicating indecent language, pursuant to his "Zirloc" screen name.[169] The CAAF held that the "Redde1" files were properly obtained.[170] However, the "Zirloc" files were improperly obtained, would not have been inevitably discovered, and thus were inadmissible.[171]

---

[156] *Id.*
[157] *Id.*
[158] *Id.* at 411.
[159] *Maxwell*, 45 M.J. at 411.
[160] *Id.*
[161] *Id.* at 413 (AOL permits each user to have multiple screen names).
[162] *Id.* at 412-13.
[163] *Id.*
[164] *Id.* at 413.
[165] *Maxwell*, 45 M.J. at 412-13. The warrant, because of a typographical error, incorrectly listed Colonel Maxwell's "Redde1" screen name as "REDDEL," but this "scrivener's error" did not invalidate the warrant. *Id.* at 420.
[166] *Maxwell*, 45 M.J. at 413-14.
[167] *Id.* at 414.
[168] *Id.* at 414.
[169] *Id.* at 410.
[170] *Id.* at 419-20.
[171] *Maxwell*, 45 M.J. at 421-23.

In *Monroe*, United States Air Force Staff Sergeant (E-5) Robert Monroe accessed the Internet and sent and received e-mails through a government computer system in Osan, Korea.[172] Users logging onto the system were alerted, by means of a banner message, that use constituted consent to monitoring by "HOSTADM."[173] Incoming e-mail messages were directed to a queue where a software program read, sorted, and directed them to the proper e-mail account.[174] Rather than being delivered to the proper e-mail account, defective or oversized messages were maintained in the queue for 72 hours.[175] After 72 hours, they were automatically deleted.[176] Occasionally, the automatic deletions did not take place and the system would become slow due to a backlog of undeliverable messages in the queue.[177] Several e-mails addressed to Monroe became "stuck" in the queue.[178] The system became slow and the system administrator, troubleshooting the problem as part of his official duties, opened several of the messages.[179] He noticed that many of the e-mails addressed to Monroe came from sexually oriented newsgroups.[180] To clear the queue, the problem messages were moved to another directory for later examination.[181] Several of these e-mails contained large graphic image file attachments.[182] Opening some of these image files in an attempt to determine the cause of the system problems, the system administrator found that they contained pornography.[183] To rule out the possibility that Monroe was the victim of a prank, the system administrator opened Monroe's account and determined that Monroe had requested the images.[184] The system administrator then turned the files over to Air Force Office of Special Investigations (OSI).[185] The files formed the basis for a search warrant of Monroe's dormitory room.[186] The search turned up both adult and child pornography.[187] Monroe entered a conditional guilty plea to child pornography charges, preserving his right to challenge the legality of the search on appeal.[188] The CAAF held that there was no reasonable expectation

---

[172] *Monroe*, 52 M.J. at 328.
[173] *Id*. at 328. "HOSTADM" is a term for system administrator.
[174] *Id*.
[175] *Id*.
[176] *Id*.
[177] *Id*.
[178] *Monroe*, 52 M.J. at 328.
[179] *Id*.
[180] *Id*..
[181] *Monroe*, 52 M.J. at 328.
[182] *Id*.
[183] *Id*.
[184] *Id*.
[185] *Id*.
[186] *Monroe*, 52 M.J. at 329.
[187] *Id*.
[188] *Id*. at 329.

of privacy in the use of government computers, at least vis- -vis the system administrators.[189] The court further found that the files were legally turned over to OSI under the ECPA.[190]

In *Allen*, United States Air Force First Lieutenant James Allen accessed his private ISP ("Super Zippo") through a government computer system.[191] A system administrator, monitoring the system as part of his official duties, suspected that pornographic images were passing through the firewall and coming onto the system.[192] The system administrator viewed a portion of one image and "concluded it involved child pornography."[193] The discovery was reported to OSI.[194] Because Allen lived off-post, OSI agents turned to local law enforcement for a search warrant for Allen's home.[195] The warrant did not cover obtaining subscriber information from Super Zippo.[196] An OSI agent contacted Super Zippo and asked whether a search warrant or subpoena was needed to obtain information pertaining to Allen's account.[197] The manager of Super Zippo consulted with legal counsel and informed the OSI agent that the only thing needed was a "lawyer request."[198] This advice was erroneous under the ECPA and Monroe sought to exclude the information provided by Super Zippo at his courts-martial.[199] The CAAF briefly analyzed the requirements of the ECPA, but declined to reach the issue of whether Allen had a reasonable expectation of privacy in the e-mails accessed through a government computer system by concluding that "a warrant would have inevitably been obtained for these very same records" had the OSI agent been correctly advised of the requirement.[200]

These three cases provide some guidance on the issue of e-mail privacy expectations on government computer systems. The CAAF is willing to recognize a reasonable expectation of privacy in e-mail communications in limited circumstances. These circumstances are unlikely to extend to e-mail sent from or received through government computer systems. In addition, the

---

[189] *Id*. at 330.
[190] *Id*. (citing 18 U.S.C. § 2702(b), which provides that contents of stored electronic communications may be turned over to law enforcement when they were inadvertently discovered and indicate the commission of a crime).
[191] *Allen*, 53 M.J. at 404.
[192] *Id*.
[193] *Id*.
[194] *Id*.
[195] *Id*.
[196] *Id*.
[197] *Allen*, 53 M.J. at 404.
[198] *Id*.
[199] *Id*. at 408-09.
[200] *Id*. at 409.

doctrine of inevitable discovery is clearly applicable to evidentiary issues in cyberspace.

D. Policy Considerations

"Public service is a public trust."[201] Standards of ethical conduct for the Executive branch were promulgated "[t]o ensure that every citizen can have complete confidence in the integrity of the Federal Government."[202] Public confidence in government is essential to our democratic way of life. Public confidence in the military is important for all the same reasons. The appropriate use of government resources—in this case government computer systems—is one key component of securing this trust. "Employees shall protect and conserve Federal property and shall not use it for other than authorized activities."[203]

The starting point for policy issues pertaining to the use of government computers is the JER.[204] Section 2-301(a) provides that ***"Federal Government communications systems and equipment (including Government owned telephones, facsimile machines, electronic mail, Internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only."*** This section is punitive, as indicated by the bold italics letters.[205] The critical issue is what constitutes "authorized purposes." While some personal use is expressly permitted as an "authorized purpose," there are certain limitations.[206] Subsection (a)(2)(d) provides the most express guidance as to limitations on use of e-mail and the Internet:

> Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial

[201] JER, *supra* note 32, at § 2-301; Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.101(a) (2001) ("Public service is a public trust.").
[202] JER, *supra* note 32, at § 2-301.
[203] *Id.*; Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635.101(b)(9) (2001) ("Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.").
[204] JER, *supra* note 32.
[205] *Id*. at Promulgating ltr, ¶ (B)(2)(a) (30 Aug. 1993) ("The prohibitions and requirements printed in bold italics in [this] reference are general orders and apply to all military members without further implementation.").
[206] JER, *supra* note 32, at § 2-301(a)(2) (identifying limited circumstances where Federal Government communication systems may be used for personal communications).

> advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service . . .).

Each of the services has some form of policy that permits or even encourages military personnel to use e-mail for personal, morale related purposes (to communicate with family and friends) and to use the Internet for familiarization.[207] The policies differ somewhat, but the bottom line is that personal use, subject to reasonable limitations, is authorized.[208] The service policies all identify examples of acceptable and prohibited uses. Some common baseline prohibitions, consistent with the guidance provided in the JER section 2-301, limit personal use to a reasonable duration and frequency (preferably on personal time),[209] to not overburden the communication system,[210] to result in no significant additional cost to DoD,[211] to not adversely affect performance of official duties,[212] and to not reflect adversely on DoD or the service component.[213]

---

[207] U.S. Army current policy provides, in part, that "Army email users should use e-mail resources responsibly and abide by normal standards of professional and personal courtesy and conduct at all times. Message, 151106Z Apr 98, Headquarters, Dep't of Army, SAIS-ZA, subject: Inappropriate Use of Electronic Mail (E-mail) (15 Apr. 1998). U.S. Air Force current policy starts out with the statement that "Air Force members and employees use government communications systems with the understanding that any type of use, authorized or unauthorized, incidental or personal, serves as consent to monitoring. " U.S. DEP'T OF AIR FORCE, SECRETARY OF THE AIR FORCE INSTR. 33-119, ELECTRONIC MAIL (E-MAIL) MANAGEMENT AND USE, ¶ 3.1 (1 Mar. 1999). U.S. Navy current policy. At present, there is no Navy-wide policy. Delineating the scope of the use of e-mail and the Internet for personal use is left up to individual commands. However, a joint message to all Atlantic, Pacific, European and Central fleet commands established a policy to "promote the widest permissible use of Government information systems to access . . . the Internet, brows[e] the World Wide Web, and communicat[e] via electronic mail." Message, 042354Z May 00, Commander in Chief, Atlantic Fleet, subject: Internet Policy, ¶ 1 (04 May 2000). This policy was established in recognition that the best way to develop information technology skills is to get on the internet as the preferred means to access, develop and exchange information. *Id.*,¶ 2. U.S. Marine Corps policy is also to leave local commands to determine permissible uses, with the understanding that personal use is specifically authorized, subject to reasonable limitations. Message, 020800 May 99, Commandant, Marine Corps, DC/C4I, subject: Information Assurance Bulletin 1-99, Appropriate Use of Marine Corps Information Resources, ¶ 1 (2 May 1999).

[208] *Id.*

[209] JER, *supra* note 32, at § 2-301(a)(2)(b).

[210] *Id.* at § 2-301(a)(2)(e).

[211] *Id.*

[212] *Id.* at § 2-301(a)(2)(a).

[213] *Id.* at § 2-301(a)(2)(d).

Both the JER and the log-on banner on government computers put military members on notice that their use constitutes consent to monitoring.[214] Both the applicable punitive section in the JER[215] and the log-on banner clearly pertain to monitoring of content, as well as context (where the person travels in cyberspace). "Every user who sees the banner before logging on to the network has received notice of the monitoring: by using the network in light of the notice, the user impliedly consents to monitoring pursuant to 18 U.S.C. § 2511(2)(c)-(d)."[216]

Inevitably, some type of monitoring must take place on government computer systems, particularly as we become more and more reliant on this technology to perform our missions. Systems protection monitoring is necessary to protect "against system malfunction and, more importantly, unlawful intrusions into our communications networks . . . " and defense infrastructure.[217]

While context monitoring is easily justified in the use of government computers, and content monitoring is arguably justified in at least some instances, there is one area where the courts must recognize a reasonable expectation of privacy in the use of government computers. This area is that of privileged communications. One military case came close to confronting this issue.

In *United States v. Tanksley*,[218] a Navy doctor (O-6), under suspicion for taking indecent liberties with a female under the age of 16, was relieved of his medical duties and temporarily assigned to other duties.[219] He was given the use of an office and a computer.[220] He was working on the computer when he was called away from his office.[221] He closed the office door, but did not

---

[214] *Id*. at § 2-301(a)(3) (provides: "***In accordance with applicable laws and regulations, use of Federal Government communications systems may be monitored. . . . DoD employees shall use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized."***). *See supra* note 6 for an example of a computer notice banner. The U.S. Air Force has implemented a "Computer User Agreement" to document users express agreement that they have no expectation of privacy in the use of DoD computers. See Appendix A for a copy of the agreement, which appears at Appendix 4 of the COMPUTER CRIMES INVESTIGATOR'S HANDBOOK, prepared by the Office of the Staff Judge Advocate, Air Force Office of Special Investigations, May 1999 (updated Feb. 2001).

[215] JER, *supra* note 32, at § 2-301(a)(3) (bold italics in the JER indicates provision is punitive).

[216] CCIPS MANUAL, *supra* note 2, at Part IV(C)(3)(b)(i).

[217] Coacher, *supra* note 33, at 156-57.

[218] 54 M.J. 169 (2000).

[219] *Id.* at 171.

[220] *Tanksley*, 54 M.J. at 171.

[221] *Id.*

lock it and did not close out the document or secure the computer.[222] When he got to his destination, he was apprehended and placed in pre-trial confinement.[223] A judge advocate subsequently went to Captain Tanksley's office to secure his personal belongings and saw the document Captain Tanksley had been working on, entitled "Regarding the Charges Now Pending Against Me," in plain view on the computer screen.[224] The officer printed the document and removed the disk from the computer.[225] The document was not used at trial, but on appeal Captain Tanksley claimed that the document was being prepared for his attorney and was therefore privileged.[226]

The CAAF disagreed on several grounds.[227] First, though no one else shared the office Captain Tanksley was given to use, he did not have exclusive use of the office and therefore had a reduced expectation of privacy therein.[228] Second, the court found that Captain Tanksley had left the document in "plain view."[229] Finally, the court noted that the document was entirely exculpatory in nature, did not reveal any confidential information about the defense strategy, produced no new leads for the government, and was not used at trial.[230] This decision is potentially troubling unless read narrowly. That is, that the document really did not contain any privileged matter. If the document had clearly contained privileged matter, and the CAAF's decision were the same, some troubling ethical issues with regard to client confidentiality could be raised where defense and legal assistance client files are maintained on government computers.[231]

The aspect of systems protection monitoring causing the most concern involves the system administrator's ability to monitor all activity and all content. In the military, system administrators tend to be relatively junior or mid-grade enlisted personnel.[232] Subject to local regulations, they are essentially free to roam at will through the system they are responsible for

---

[222] *Id*.
[223] *Id*.
[224] *Id*. at 171-72.
[225] *Id*.
[226] *Tanksley*, 54 M.J. at 172.
[227] *Id*.
[228] *Tanksley*, 54 M.J. at 172.
[229] *Id*.
[230] *Id*. (relying on the Supreme Court's rejection, in *Weatherford v. Bursey*, 429 U.S. 545, 554 (1977), of a *per se* rule finding a Sixth Amendment violation when privileged communications are overheard or read).
[231] *But see infra* note 408. Notwithstanding the provisions of note 428, however, ethical issues may still exist where the attorney *knows* that government agents are free to view the contents of files at any time and for any reason.
[232] Observation based on author's experience.

administering. At least for certain types of communications,[233] such unchecked freedom is unacceptable.

III. Analysis

A. The Fourth Amendment

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[234]

The Fourth Amendment protects against unreasonable searches and seizures. Before proceeding to the analysis set forth in *United States v. Katz*,[235] a threshold issue must be addressed: whether the search or seizure is being conducted by or at the behest of government agents. Only if this issue is resolved in the affirmative, does application of *Katz*' two-part test become necessary to determine whether a legitimate expectation of privacy exists. The analysis then proceeds to the final step of asking whether the search was reasonable.

In *United States v. Jacobsen*,[236] the Supreme Court considered the issue of whether a search was being conducted by government agents. In *Jacobsen*, employees of a private freight carrier were examining a package that had been damaged by a forklift.[237] The package was opened to determine whether its contents were also damaged and inside was found a ten-inch long tube taped at both ends.[238] The employees cut open the tube and found a zip-lock plastic bag with several other zip-lock plastic bags inside.[239] The innermost bag contained a white powder.[240] The employees put the contents

---

[233] For example, privileged legal and psychiatric communications, as well as those coming from higher command level intended for a limited audience.
[234] U.S. CONST. Amend. IV.
[235] 389 U.S. 347 (1967).
[236] 466 U.S. 109 (1984).
[237] *Id.* at 111.
[238] *Id.*
[239] *Id.*
[240] *Id.*

back in the box and called the Drug Enforcement Administration (DEA).[241] The DEA agents removed the contents from the box to the same extent as had the freight carrier employees, but then went one step further and removed a trace amount of the powder for a field test.[242] The field test "identified the substance as cocaine."[243]

The Court found that the "initial invasions" of the package clearly constituted a private search.[244] The Court went on to say that "[w]hether those invasions were accidental or deliberate, and whether they were reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character."[245] The reopening of the package by the DEA agents was also not a search so long as it did not exceed the scope of the private search.[246] Thus, the governmental nature of the search is a critical prerequisite for Fourth Amendment protections. If the search is a private one, there is no requirement that it be reasonable. If a government search is done subsequently to a private search, the government search can be unreasonable to the same extent as the private search without triggering a Fourth Amendment violation.

The case controlling Fourth Amendment analysis is *Katz v. United States*.[247] The test was actually set forth in Justice Harlan's concurring opinion: "[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[248] Only if both of these conditions are met does the inquiry proceed to the next step—whether the search is "reasonable."

> If there is no reasonable expectation of privacy, the Fourth Amendment does not

---

[241] *Id.*
[242] *Jacobsen*, 466 U.S. at 111-12.
[243] *Id.* at 112.
[244] *Id.* at 115.
[245] *Id.* at 111.
[246] *Jacobsen*, 466 U.S. at 111 (noting the court did not find the removal of a trace amount of the white powder for the purpose of a field test to impermissibly exceed the scope of the private search). On the issue of scope in the context of a computer search, see *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (finding law enforcement conducting consent search of computer for evidence of drug trafficking exceeded scope of consent when they continued to view JPG files after opening one and determining it to contain child pornography; discovery of the first file was inadvertent, but searching additional files was unreasonable).
[247] 389 U.S. 347 (1967). For more detail on pre-*Katz* Fourth Amendment analysis, see Wells, *supra* note 53, at 109-116.
[248] *Katz*, 389 U.S. at 361. This test has since been officially adopted by the Supreme Court as the controlling standard. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). *See* Gilligan & Imwinkelried, *supra* note 61, at 326.

> apply and the government may search and seize without a warrant, probable cause, or any of the safeguards established by the Amendment. If there is a reasonable expectation of privacy, then courts proceed to look at the reasonableness of a particular search or seizure within a particular context.[249]

Applying the *Katz* test, several activities have been identified where there is no reasonable expectation of privacy and thus no search protected by the Fourth Amendment.[250] These activities include:

> [e]xamining trash left at the curb side for pickup, sniffing of luggage or automobile by detection dogs, employing a pen register, monitoring vehicles on the road by use of beeper, placing beepers in containers outside of the home or curtilage, subpoenaing bank records, using undercover agents, flying over residential property, searching destroyed property, and examining magazines in a bookstore.[251]

The common rationale in each of these activities, except in the case of drug-sniffing dogs, is the inability to control access to, and/or disclosure of the information by, third parties. In essence, the control of disclosure to/by third parties either never existed or has been surrendered. In the case of drug-sniffing dogs, the issue is not so much whether a person has a reasonable expectation of privacy in the item "sniffed," as it is a judgment by the Court that this type of search is so non-intrusive that it does "not constitute a 'search' within the meaning of the Fourth Amendment." [252]

Courts have also found the existence of a reasonable expectation of privacy lacking in items that have been previously searched. While there is generally a reasonable expectation of privacy in closed containers,[253] this

---

[249] Sundstrom, *supra* note 5, at 2071.
[250] Gilligan & Imwinkelried, *supra* note 61, at 327.
[251] Gilligan & Imwinkelried, *supra* note 61, at 327 (citations omitted).
[252] United States v. Place, 462 U.S. 696, 707 (1983).
[253] United States v. Chadwick, 433 U.S. 1 (1977) (holding luggage and other closed containers generally cannot be searched without consent or a warrant). *See also*, United States v. Most, 876 F.2d 191 (D.C. Cir. 1989) (ruling reasonable expectation of privacy in bag left with store clerk

expectation is not absolute. Returning to the issue of the private search initiated by the freight carrier in *Jacobsen*,[254] the Supreme Court has held that an individual has no reasonable expectation of privacy in the contents of a container previously searched in a lawful manner.[255] Nor will resealing the container for some purpose, such as to effect a controlled delivery, restore the original privacy rights.[256]

While the Fourth Amendment protects against unreasonable searches of our "papers" and "effects,"[257] there is no reasonable expectation of privacy in records turned over to third parties.[258] The rationale is that by turning them over to third parties, with whom there is no legally recognized privilege, the individual has no control over the third party's ability to turn the documents over to the government.

Turning to case law dealing with computers and/or e-mail, courts have found no reasonable expectation of privacy in chat rooms, largely because these are public forums and a user has no control over who can observe the communications that take place.[259] In a private employer situation, a court found no reasonable expectation of privacy in e-mail sent through the employer's network, despite the fact that the employer assured employees that the system was confidential—in other words, employees believed they were not being monitored.[260] (Of course, the Fourth Amendment does not apply to

---

for safekeeping where store policy is to leave bags with clerk while shopping; expectation of privacy retained even where owner of bag left store where he specifically asked clerk to continue watching it for him); United States v. Barry, 853 F.2d 1479 (8th Cir. 1988) (finding reasonable expectation of privacy in suitcase left in airport locker service where locker key and claim check retained by owner of suitcase). Note that this closed container exception does not apply to automobiles. *See Chadwick*, 433 U.S. at 11-13; Cardwell v. Lewis, 417 U.S. 583, 590 (1974); Cady v. Dombrowski, 413 U.S. 433, 441-42 (1973). *See also*, Florida v. Jimeno, 500 U.S. 248 (1991) (ruling search of container in automobile not violative of Fourth Amendment); Wyoming v. Houghton, 526 U.S. 295 (1999) (holding that if probable cause exists to search a vehicle, then the entire vehicle along with all of its contents may be searched and refusing to create a "passenger property" exception.).

[254] 466 U.S. 109 (1984).

[255] Illinois v. Andreas, 463 U.S. 765, 771 (1983).

[256] *Id.*

[257] U.S. CONST. Amend. IV.

[258] United States v. Miller, 425 U.S. 435 (1976) (no reasonable expectation of privacy in bank records); Coach v. United States, 409 U.S. 322 (1973) (no reasonable expectation of privacy in records handed over to accountant for purpose of preparing tax returns).

[259] United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997).

[260] Smythe v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996):

> [W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail

private employer-conducted searches.[261] This was a civil tort case for wrongful termination, but the court employed a reasonable expectation of privacy analysis and found no reasonable expectation of privacy despite the employer's policy that the e-mail would be private.)[262] Another court found no reasonable expectation of privacy in a computer password when it was entered within plain view of law enforcement.[263] Yet another court found that a reasonable expectation of privacy in closed computer files is sufficiently analogous to the well-established reasonable expectation of privacy in closed containers to warrant Fourth Amendment protection.[264]

"In considering the reasonableness of asserted privacy expectations, the Court has recognized that no single factor invariably will be determinative."[265] Factors that the Court has considered include the precautions taken by a person to maintain privacy and the "precautions customarily taken by those seeking privacy."[266] The Court also considers relevant the manner in which a person uses a location.[267] This factor is particularly important in those cases where a person is asserting privacy in a place other than his own home or office. Whereas a person generally does have a reasonable expectation of privacy in an apartment that does not belong to him, but which he regularly stays in and keeps belongings in (in other words, a place in which he is legitimately on the premises),[268] he will not have a reasonable expectation of privacy in a home that he is burglarizing.[269] "The Court on occasion has also looked to history to discern whether certain types of government intrusions were perceived to be objectionable by the Framers of the Fourth Amendment."[270] Finally, the Court will look to property rights, as they "reflect society's explicit recognition of a person's authority to act as he wishes in certain areas, and therefore should be considered in determining

---

> system notwithstanding any assurances that such communications would not be intercepted by management. … [T]he company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.

[261] United States v. Jacobsen, 466 U.S. 109, 113-15 (1984).
[262] *Smythe*, 914 F. Supp. 97.
[263] United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991).
[264] United States v. Barth, 26 F. Supp. 2d 929 (W.D. Tex. 1998).
[265] Rakas v. Illinois, 439 U.S. 128, 152 (1978) (Powell, J., concurring).
[266] *Id.* at 152 (Powell, J., concurring).
[267] *Id.* at 153.
[268] Jones v. United States, 362 U.S. 257 (1960).
[269] *Rakas*, 439 U.S. at 143, n.12.
[270] *Id.* at 153 (Powell, J., concurring).

whether an individual's expectations of privacy are reasonable." [271]

Applying these factors to e-mail is not overly instructive. However, a few points are worth making. On the subject of precautions taken to preserve privacy, e-mail can be encrypted, but there are some substantial legal hurdles to making this a widespread reality.[272] Perhaps the *Maxwell* court hit on the best solution in this regard, in that the security practices of the ISP may impact on the reasonableness of a user's expectation of privacy in e-mail communications.[273] On the subject of the manner in which a person uses e-mail, clearly this has become an extremely important means of communicating, both in our personal lives and in business. The use of e-mail is very similar to the use of more traditional means of communication. It has, in many respects, replaced not only first-class mail, because it is so much faster, but it has also replaced the telephone conversation to a large extent. [274] When communicating by e-mail, one does not have to worry about busy signals, answering machines, or administrative assistants screening calls. E-mail bypasses all of that and goes directly to the desk of the intended recipient. Nor is e-mail dependent on whether a person is "in," on vacation, or otherwise away from the workplace. In most cases, e-mail can be retrieved from wherever one may be. Even without a portable computer, e-mail can now be accessed from airports and hotels, Internet cafes, libraries, and even cellular phones. This unmatched versatility has made e-mail the preferred method of communicating. Building on the manner of use factor, although there is no "history," *per se*, with e-mail, there is ample case law history pertaining to traditional mail, files, and telephone conversations. All are generally recognized as protected by the Fourth Amendment.[275] We must decide what is important to us, as a society, to protect.[276]

The primary obstacle to finding a reasonable expectation of privacy is

---

[271] *Id.*

[272] *See* Joel C. Mandelman, *Lest We Walk Into the Well: Guarding the Keys—Encrypting the Constitution: To Speak, Search & Seize in Cyberspace*, 8 ALB. L.J. SCI. & TECH. 227 (1998) (discussing "federal government's mandate that it have access to the code keys used to encrypt computer transmitted messages, and its restrictions on exporting codes and technology used to encrypt messages by using any algorithm containing more than 56 bits.").

[273] *Maxwell*,45 M.J. 406 (1996).

[274] For example, the use of "Instant Messaging" allowing near real-time communication on-line with another party.

[275] *See Ex parte Jackson*, 96 U.S. 727 (1877) (mail); O'Connor v. Ortega, 480 U.S. 709 (1987) (file cabinets); Katz v. United States, 389 U.S. 347 (1967) (telephones).

[276] Note: *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1607 (May, 1997) [hereinafter 110 HARV. L. REV. 1591].

consent.[277] There are two general types of consent. Actual or implied consent by the party whose Fourth Amendment rights are at stake, and third-party consent by someone with "common authority"[278] to consent.

In *United States v. Matlock,*[279] the Supreme Court decided the issue of whether someone other than the defendant can lawfully consent to a search of the defendant's belongings.[280] The Court answered this question in the affirmative, provided the prosecution can show that the party who consented to the search had "common authority over or other sufficient relationship to the premises or effects sought to be inspected."[281] In *Matlock,* it was the cohabitant of the defendant's bedroom who provided the consent.[282]

The Court further refined the requirements for third-party consent searches in *Illinois v. Rodriquez*.[283] In this case, police gained entry to the defendant's apartment to arrest him with the assistance of a woman who claimed she shared the apartment with the defendant.[284] The woman had a key to the apartment and let the police in.[285] The defendant sought to suppress all evidence seized at the time of his arrest on the grounds that the woman did not have actual authority to consent, since she was no longer living in the apartment with him at the time she consented to the entry.[286] The Court held that third-party consent is valid when based upon a reasonable belief, at the time of entry, that the consenting party has "common authority."[287] Thus, apparent authority, so long as reasonable, suffices for purposes of third-party consent.[288]

There are limits, however, to the authority of third parties to consent. Third-party consent has not been held valid in cases where a landlord consented to a search of leased premises,[289] or where a hotel clerk consented to a search of a rented hotel room.[290] In *Stoner v. California,* the Court stated

---

[277] Sundstrom, *supra* note 5, at 2090-91.
[278] United States v. Matlock, 415 U.S. 164 (1974).
[279] *Id.*
[280] *Matlock*, 415 U.S. at 171.
[281] *Matlock*, 415 U.S. at 171.
[282] *Id.* at 166-169.
[283] 497 U.S. 177 (1990).
[284] *Id.* at 179-80.
[285] *Rodriguez,* 497 U.S. at 179-80. *See also,* United States v. Reister, 40 M.J. 666 (N.M. Ct. Crim. App. 1994) (addressing third party consent).
[286] *Rodriguez,* 497 U.S. at 179-80.
[287] *Id.*
[288] *Id.*
[289] Chapman v. United States, 365 U.S. 610 (1961).
[290] Stoner v. California, 376 U.S. 483 (1964).

"the rights protected by the Fourth Amendment are not to be eroded by strained applications of the law of agency or by unrealistic doctrines of 'apparent authority.'" [291]

From the standpoint of the government employer, if an employee has a reasonable expectation of privacy in his office or desk, the supervisor's consent to law enforcement personnel to search the protected area(s) may be ineffective.[292] However, under the Supreme Court's holding in *O'Connor v. Ortega,*[293] the supervisor can probably conduct the search himself without constitutional consequences.[294] This is a fine, but extremely important distinction. "Searches and seizures by government employers or supervisors of the *private* property of their employees . . . are subject to the restraints of the Fourth Amendment."[295] However, "[t]he workplace includes those areas and items that are related to work and are generally within the employer's control."[296] Thus, there may be legitimate needs for a supervisor to enter an employee's workspace and search for work-related items.[297] For example, an employee may be working on a report. While the employee is out of the office, the supervisor may need to look at the report. For this purpose, the supervisor can legitimately enter the employee's office to look for the report. In this quest, the supervisor may find contraband. So long as the supervisor was searching the employee's workspace for work-related purposes, rather than law enforcement purposes, the search will almost certainly be considered reasonable. The key is the purpose of the search. Additionally, the court found that "[p]ublic employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[298] The lesson for government employers is to have a policy or regulation permitting broad supervisor access to employee workspaces. Absent such policy or regulation, however, the Fourth Amendment is not likely to be offended so long as the supervisor conducts the

---

[291] *Id*. at 488.
[292] United States v. Blok, 188 F.2d 1019 (D.C. Cir. 1951).
[293] 480 U.S. 709 (1987).
[294] *Id.* at 720-21.
[295] *Id*. at 714.
[296] *Id*. at 715.
[297] *Id*. at 717.
[298] O'Connor v. Ortega, 480 U.S. 709, 717 (1987). *See also, Katz,* 389 U.S. at 361. In *Katz,* the Court established a two prong analysis to determine the existence of a Fourth Amendment expectation of privacy: (1) the objective test – is the accused's expectation reasonable and one that society is willing to recognize; (2) the subjective test -- has the accused manifested a subjective belief that he or she possesses a privacy interest in the matter? Command or agency regulations and practices can reduce or eliminate the individual's subjective expectation of privacy under the Fourth Amendment (e.g., the use of computer log on banners and/or user agreements).

search and can articulate a work-related purpose.

Particularly in the context of a military base or other federal facility, the actual or implied consent of the individual is an extremely powerful exception to the Fourth Amendment's warrant requirement. In *United States v. Ellis*,[299] William Gaskamp drove his personal vehicle onto the Naval Air Station, Pensacola, Florida.[300] When he entered the base, he accepted a visitor's pass at the gate.[301] The front of the pass states:

> DISPLAY IN WINDSHIELD WHILE ON STATION DESTROY AFTER LEAVING STATION **VISITOR** Acceptance of this pass gives your consent to search of this vehicle while entering, aboard, or leaving this station.[302]

While on the Naval Air Station, a station investigator observed Gaskamp removing a "neatly wrapped brown towel" from the trunk of his car and taking it into the barracks.[303] The investigator followed Gaskamp to the room of David Ellis, a member of the United States Navy.[304] The investigator requested permission to search Gaskamp's vehicle.[305] Gaskamp hesitated, so the investigator asked if he had read the visitor's pass.[306] Gaskamp acknowledged that he had read the visitor's pass and the investigator asserted his right to search the vehicle.[307] He found twenty plastic bags of marijuana.[308] On the issue of the validity of the warrantless search, the court found that "[a] base commander may summarily exclude all civilians from the area of his command. It is within his authority, therefore, also to place restrictions on the right of access to a base."[309] The court held "the consent was knowing and voluntary and could have left Gaskamp with no reasonable expectation of privacy in his vehicle. The right to make a search pursuant to such consent does not turn on the presence of probable cause."[310]

---

[299] 547 F.2d 863 (5th Cir. 1977).
[300] *Ellis*, 547 F.2d at 865.
[301] *Ellis*, 547 F.2d at 865.
[302] *Id.*
[303] *Id.*
[304] *Id.* at 864-65.
[305] *Id.* at 865.
[306] *Ellis*, 547 F.2d at 865.
[307] *Id.*
[308] *Id.*
[309] *Id.* at 866.
[310] *Id.*

Consent, whether express or implied, is a powerful exception to the Fourth Amendment search restrictions. For purposes of implied consent, at least in certain circumstances, such as when logging onto government computer systems or accessing a military facility, the fact that consent is a mandatory prerequisite to access is not relevant. The choice is to proceed onto the military installation knowing that to do so constitutes consent to a search, or choosing not to proceed. The choice is to log onto the government computer system, knowing that to do so constitutes consent to monitoring, or to choosing not to log on. In *Ellis*, Gaskamp acknowledged that he had read the visitor's pass.[311] However, had he not done so, it is unlikely the court's decision would have been any different. Again, Gaskamp had a choice to read or not read the pass. He should not be able to use ignorance or obstinacy to avoid the consequences of his choices. To the extent users of government computer systems consent to monitoring each time they log on to the system, there can be no reasonable expectation of privacy in that use.

While many cases have further shaped the Fourth Amendment analysis to keep up with technological advancements, *Maxwell* was the first to directly tackle the issue with respect to e-mail.[312] As the court stated, "[t]his case takes us into the new and developing area of the law addressing the virtual reality of 'cyberspace . . . .'"[313]

Maxwell is extremely important for establishing, albeit in a limited context, that there can be a reasonable expectation of privacy in e-mail.[314] It is important to note that *Maxwell's* holding in this regard is very fact dependent. The facts relevant to this inquiry are that Colonel Maxwell used only his personal home computer and only during off-duty hours, to access the Internet and send e-mails through AOL.[315] AOL's policy and practices provide e-mail messages heightened privacy.[316] First, they are privately stored "on AOL's centralized and privately-owned computer bank located in Vienna, Virginia."[317] Second, "[i]t was AOL's practice to guard these 'private communications' and only disclose them to third parties if given a court order."[318] The court found

---

[311] *Ellis*, 547 F.2d at 865.
[312] 45 M.J. 406, 410 (1996).
[313] *Maxwell*, 45 M.J. at 410.
[314] *Id*. at 417-18 (*Maxwell* has no precedential value outside the military courts, but is frequently cited with approval: Guest v. Leis, 255 F.3d 325, 333, 336 (6th Cir. 2001); United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999); United States v. Reppert, 76 F. Supp. 2d 185, 187 (D. Conn. 1999); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999); United States v. Stevens, 29 F. Supp. 2d 592, 594 (D. Alaska 1998)).
[315] *Maxwell*, 45 M.J. at 411.
[316] *Id*. at 417.
[317] *Id.*
[318] *Id.*

these factors critical to its holding that Colonel Maxwell had a limited reasonable expectation of privacy in his e-mail messages sent and received through AOL.[319]

In terms of Internet communications, the *Maxwell* court found that "the more open the method of transmission, such as the 'chat room,' the less privacy one can reasonably expect."[320] The court also recognized that "once the transmissions are received by another person, the transmitter no longer controls its destiny."[321] Thus, there is a limited circumstance (when the electronic method employed maximizes the users actual privacy) and a limited time period (where the e-mail has been sent but not yet opened by the intended recipient) in which the sender of an e-mail enjoys a reasonable expectation of privacy. But in the context of using government computer systems, *Maxwell* has little practical application, since Colonel Maxwell's Internet activities were conducted solely from his personal computer located in his home.[322]

In deciding, in *Maxwell*, that there is a limited reasonable expectation of privacy in e-mail, the CAAF analogized e-mail to two separate communications media where the Supreme Court has already recognized a legitimate expectation of privacy.[323] First, the court analogized e-mail to first class mail[324] and concluded, "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."[325] Of course, as with first-class mail, once the e-mail is received and opened by the intended recipient, the sender no longer has control over the contents.[326] The court also found that "[t]he fact that an unauthorized 'hacker' might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way."[327]

The court noted one significant difference from first-class mail: the fact that, because of the nature of Internet transmissions, the ISP can access the e-mail and see its contents before it is opened by the addressee.[328]

---

[319] *Id.*
[320] *Maxwell*, 45 M.J. at 417.
[321] *Id.* at 418.
[322] *Id.* at 411. *See also*, *Monroe*, 52 M.J. at 330-31 (finding no reasonable expectation of privacy in personal communications sent or received using government computer system).
[323] *Maxwell*, 45 M.J. at 417-418.
[324] *Id.* at 417 (citing *Gouled v. United States*, 255 U.S. 298 (1921) for the holding that sender of first-class mail has reasonable expectation of privacy in contents until received by the intended recipient).
[325] *Maxwell*, 45 M.J. at 418.
[326] *Id.* at 418.
[327] *Id.*
[328] *Id.*

Significantly, the court found that even this possibility did not destroy the legitimate expectation of privacy in the e-mail during transmission vis- -vis the police.[329] The court recognized one significant problem with this analogy, but did not devote a great deal of analysis to the issue.[330] If "the relationship of a computer network subscriber to the network is similar to that of a bank customer to a bank, [then] . . . there is no reasonable expectation that the records are private."[331] This could ultimately prove to be a critical issue in terms of Fourth Amendment analysis, but the ECPA does deal with this issue.[332]

The *Maxwell* court also analogized e-mail to telephone conversations.[333] While "the maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation . . . the conversation itself is held with the risk that one of the participants may reveal what is said to others."[334] In this type of analogy, the ISP would be more akin to a telephone operator. The fact that the telephone operator can listen in on the conversation does not vitiate the caller's legitimate expectation of privacy in the call.[335] The problem is that neither analogy translates smoothly to e-mail.

Various commentators have canvassed the problems in attempting to analogize e-mail to existing forms of communications.[336] The principle problem is the amorphous quality of cyberspace. The Fourth Amendment may protect "people, not places,"[337] but when it comes to cyberspace, courts, for lack of a better approach, tend to employ a "place-oriented approach."[338] Under this approach, "the degree of privacy protected by the Amendment depends on where . . . [a search] occurs."[339] The boundless nature of cyberspace is much more akin to "open fields" than to the privacy of a home or office under this approach, which does not bode well for finding a

---

[329] *Id.*
[330] *Maxwell,* 45 M.J. at 418.
[331] *Id.*
[332] See discussion on ECPA, *supra,* part II(B) (spelling out in detail what information can be disclosed, when, and to whom).
[333] *Maxwell,* 45 M.J. at 418.
[334] *Id. But see,* Watkins v. L.M. Berry & Co., 704 F.2d 577, 584 (11th Cir. 1983) ("The expectation of privacy in a conversation is not lost entirely because the privacy of part of it is violated.").
[335] California v. Greenwood, 486 U.S. 35, 36 (1988).
[336] *See e.g.*, Jackson, *supra* note 60; Katopis, *supra* note 103; Knopf, *supra* note 60; *and* 110 HARV. L. REV. 1591, *supra* note 276.
[337] Katz v. United States, 389 U.S. 347, 351 (1967).
[338] Knopf, *supra* note 60, at 86.
[339] 110 HARV. L. REV. 1591, *supra* note 276, at 1599.

reasonable expectation of privacy in e-mail.

The *Maxwell* court bravely applied the mail and telephone analogies, but these do not provide "a convincing analytical framework with which to govern Fourth Amendment jurisprudence in cyberspace."[340] One commentator analogized an e-mail message to a "cross between a telephone call and a postcard . . .", where the message body is the equivalent of a telephone conversation and the address portion is the equivalent of the postcard.[341] The principal problem with this analogy is that the address portion of an e-mail may also contain the subject line, which may equate to content.[342] But, if the postcard analogy holds, like the lack of any expectation of privacy in the contents of a postcard, the sender of an e-mail would not have a legitimate privacy interest in the subject line, regardless of whether it also contains "content."

The end result, with no viable analogy to e-mail, is that a risk analysis framework—the only remaining solution—largely vitiates any expectation of privacy in e-mail communications because "[e]-mail on the Internet is not routed through a central control point, and can take many and varying paths to the recipients. Unlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient."[343] Similarly, if analogizing communication via e-mail to telephone calls, under a risk analysis approach, the closer fit is to cordless telephone calls, which some lower courts have held do not enjoy a reasonable expectation of privacy because of the ease of interception.[344] However, when considering an issue as important as the privacy of our communications, there is something unsettling about allowing the protections of the Fourth Amendment to be supplanted by mere "ease of interception."[345]

---

[340] 110 HARV. L. REV. 1591, *supra* note 276, at 1599.
[341] Katopis, *supra* note 103, at 190-91.
[342] *Id*.
[343] ACLU v. Reno, 929 F. Supp. 824, 834 (1996). *See also*, 110 HARV. L. REV. 1591, *supra* note 276, at 1597.
[344] *See* McKamey v. Roach, 55 F.3d 1236, 1239-40 (6th Cir. 1995); *In re* Askin, 47 F.3d 100, 104-06 (4th Cir. 1995); United States v. Smith, 978 F.2d 171, 177-81 (5th Cir. 1992) ("No reported decision has concluded that a cordless telephone user has a reasonable expectation of privacy in his cordless phone conversations under Title III [of the ECPA] or the Fourth Amendment."); Tyler v. Berodt, 877 F.2d 705, 706-07 (8th Cir. 1989); and United States v. Carr, 805 F. Supp. 1266, 1271 (E.D. N.C. 1992) (ruling cordless phones not protected by the ECPA – "Those who use cordless telephones do so at their peril."). *See also*, 110 HARV. L. REV. 1591, *supra* note 276, at 1598.
[345] 110 HARV. L. REV., *supra* note 276, at 1598 ("Pure ease of interception cannot render an expectation of privacy unreasonable, however, because such a rule would remove well-settled Fourth Amendment protections[.]"); Jackson, *supra* note 60, at 105 ("Electronic communications vulnerability to interception is not a sound reason for giving it less protection[.]").

A final analogy is to a closed container.[346] While individuals generally retain a reasonable expectation of privacy in closed containers, including computers, under their control,[347] the analogy fails in the context of government computer systems. Government computers are not under the employee's control in the way their personal purse, luggage, or briefcase would be. Government computers are under the government's control. Though the court in *United States v. Villarreal*,[348] stated "[i]ndividuals do not surrender their expectations of privacy in closed containers when they send them by mail or common carrier . . .",[349] there must have been a reasonable expectation of privacy to start with.

An alternative solution is needed. One such solution could be based on *Katz's* "people, not places" approach.[350] *Katz* provides a standard that that might work if society is willing to recognize the reasonableness of an expectation of privacy: "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . , [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[351] Under this standard, despite the differences created by technology, the first-class mail analogy would work. The sender of an e-mail could expect a reasonable expectation of privacy in e-mail, at least until the recipient receives it, as with first-class mail. Once the recipient has it, of course, the sender no longer has any control over who it may be forwarded to or shown to. The sender's expectation of privacy in that e-mail thus diminishes incrementally to the extent that the recipient chooses to permit others to see it.[352]

Another proposed solution is to use the exceptions to the warrant requirement to identify factors that must be absent "in order to protect the privacy of one's communications."[353] The primary relevant exceptions are consent, disclosure to third parties, and open view.[354] In the context of government workplaces and government computer systems, the consent exception is unlikely to provide assistance, because use of government

---

[346] CCIPS MANUAL, *supra* note 2, at Part I (B)(2).
[347] *Id*.
[348] 963 F.2d 770 (5th Cir. 1992).
[349] *Id*. at 773-74.
[350] *Katz*, 389 U.S. at 351.
[351] *Id*.
[352] *Maxwell*, 45 M.J. at 417.
[353] 110 HARV. L. REV. 1591, *supra* note 276, at 1599-1600.
[354] *Id*.

computer systems constitutes consent to monitoring.[355] In terms of third-party consent, however, an unsettled issue is whether network or system administrators can lawfully consent to a search.[356] Resolution of the issue will depend on whether system administrators are viewed as more akin to landlords and hotel clerks, or to a person with "common authority."

As far as disclosure to third parties, the sender of an e-mail would have a reasonable expectation of privacy is the communication until it has reached the intended recipient. Once it is in the hands of the recipient, the sender no longer has a legitimate expectation of privacy, as well as no standing to object to a search of its contents, to the extent that the third party chooses to disclose the contents to anyone else.[357]

In *Smith v. Maryland*,[358] the Supreme Court recognized that the *Katz* analysis might not apply to every situation.[359] Cyberspace may very well turn out to be one of these situations. As the Court presciently observed, strict application of *Katz* may not always be appropriate.[360] The Court proposed two scenarios whereby an individual's subjective expectation of privacy may be nonexistent, but where there would nevertheless be a reasonable expectation of privacy because of society's firm belief that an objective expectation of privacy existed.[361]

> For 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. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such

[355] *See supra* note 6 for sample banner.
[356] *See* 110 HARV. L. REV. 1591, *supra* note 276, at 1600.
[357] *Id*. at 1600-01.
[358] 442 U.S. 735 (1979).
[359] *Id.* at 741.
[360] *Id*. at 741, n.5.
[361] *Id.*

> circumstances, where an 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.[362]

This provides a simple and workable standard in keeping with the spirit of the Fourth Amendment that all persons shall be "secure in their . . . papers."[363] E-mail, in so many ways, has replaced more traditional methods of correspondence, both personally and in business relations. Whereas our files and letters are widely recognized as "papers" protected by the Amendment, our newest form of communicating deserves no less protection.[364] The normative inquiry "requires a judgment about the kind of society in which we want to live; in determining 'reasonable expectations,' we cannot divorce the level of privacy that the Constitution does protect from a judgment about how much privacy our society ought to protect."[365] "As technology evolves so do societal expectations of reasonableness."[366]

The final inquiry is whether the search is reasonable.[367] "The Fourth Amendment commands that searches and seizures be reasonable."[368] The Fourth Amendment does not proscribe all searches and seizures by the Government, only those that are "unreasonable."[369] In the context of searches

---

[362] Smith v. Maryland, 442 U.S. at 741, n.5.
[363] U.S. CONST. Amend. IV.
[364] *See* Barrera & Okai, *supra* note 74 (discussing the "correspondence privacy paradigm" which questions whether electronic documents are any less worthy of privacy protections than physical documents).
[365] 110 HARV. L. REV. 1591, *supra* note 276, at 1607.
[366] Bayens, *supra* note 53, at 242.
[367] "The ultimate standard set forth in the Fourth Amendment is reasonableness." Cady v. Dombrowski, 413 U.S. 433 (1973).
[368] United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).
[369] Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The touchstone of the Fourth Amendment is reasonableness. The Fourth Amendment does not proscribe all state-initiated searches and seizures; it merely proscribes those which are unreasonable.").

within the government workplace, the seminal case is *O'Connor v. Ortega*.[370] The Court considered first whether there were circumstances in which there could be a reasonable expectation of privacy in a government workplace.[371] Finding that there could be, under the appropriate circumstances, the Court then provided the appropriate standard for determining when a workplace search is reasonable.[372]

A critical determination, particularly if there is even a remote hope of finding a reasonable expectation of privacy in personal e-mails sent through government computer systems, was the Court's finding that "[s]earches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the Fourth Amendment."[373] However, this is severely limited not only by the fact that users of government computer systems consent to monitoring, but also by the fact that "the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context . . . ."[374] Another important limitation expressly recognized by the Court is that this expectation of privacy "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[375] Regulation, to one extent or another, is standard in the military workplace.

The Court addressed the issue that although the workplace is the property of the employer, this does not mean that every item brought into it by employees is also the property of the employer.[376] For example, if an employee brings luggage, a handbag, or a briefcase to the office, "[w]hile whatever expectation of privacy the employee has in the existence and the outward appearance of the [item] is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* . . . is not affected in the same way."[377] This distinction may be important in the context of a government employee bringing a computer diskette with personal files to the workplace.

Turning to the standard of reasonableness for a workplace search by

---

[370] 480 U.S. 709 (1987).
[371] *Id.* at 711-12.
[372] *Id*. at 712.
[373] *O'Connor v. Ortega*, 48 U.S. at 715.
[374] *Id.*
[375] *Id*. at 716. (See the effect of this limitation in action in United States v. Simons, 206 F.3d 392 (4th Cir. 2000); Schowengerdt v. United States, 944 F.2d 483 (9th Cir. 1991); and Am. Postal Workers Union v. United States Postal Serv.. 871 F.2d 556 (6th Cir. 1989)).
[376] *O'Connor v. Ortega*, 48 U.S. at 715.
[377] *Id.* at 716.

the government as employer, the Court held that the government employer may intrude "on the constitutionally protected privacy interests of government employees" in two circumstances.[378] First, the government as employer may conduct noninvestigatory, work-related searches.[379] Second, the government employer may search pursuant to an investigation into work-related misconduct.[380] Such searches are constitutionally permitted so long as "both the inception and the scope of the intrusion [are] reasonable."[381]

The Court provided that the search of a government employee's office will be "'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file."[382]

Theoretically, this model could be applied to searches of e-mail. System administrators would be unimpeded in conducting noninvestigatory work-related searches, such as system maintenance. But searches of e-mail content beyond that would have to meet the reasonableness standard for suspected work-related employee misconduct.[383] Of course, if the employee is using a government computer system, any misconduct related thereto is clearly work-related, even if otherwise personal, because of the use of the government computer system. But this type of search assumes lack of consent. In the use of government computer systems, with the warning banners notifying users that use constitutes consent to monitoring, arguably there is consent for any search, content or otherwise, of the files and activity resident on a government computer, whether reasonable or unreasonable.

One final issue that must be considered under Fourth Amendment analysis is the impact of inevitable discovery. The United States Supreme Court formally recognized inevitable discovery as an exception to the

---

[378] *O'Connor v. Ortega*, 48 U.S. at 725. Note that in the context of government computer systems, the additional issue of consent and/or waiver is raised as a result of the log-on banner (or U.S. Air Force user agreement), thereby degrading or eliminating any reasonable expectation of privacy.

[379] *Id.*

[380] *Id.* Note that the misconduct must be "work-related." *See* United States v. Simons, 206 F.3d 392, 401 (4th Cir. 2000) ("This situation may be contrasted with one in which the criminal acts of a government employee were unrelated to his employment.").

[381] *O'Connor v. Ortega,* 480 U.S. at 726.

[382] *Id.*

[383] Admittedly, any use of a government computer system is "work related" and any misuse of a government computer system is a violation of the UCMJ art. 92. The threshold suggested implies some reasonable suspicion of misconduct prior to any investigatory search of e-mail.

exclusionary rule in *Nix v. Williams*.[384] Most state and federal courts, including every Federal Court of Appeals, already recognized the exception.[385] The CAAF (then called the Court of Military Appeals)[386] formally recognized the exception two years before *Nix* in *United States v. Kozak*.[387] The *Nix* Court set forth the prosecution's burden:

> If the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means . . . then the deterrence rationale has so little basis that the evidence should be received. Anything less would reject logic, experience, and common sense.[388]

In *Maxwell*, the issue was whether the files under Colonel Maxwell's other user names, in particular "Zirloc," would have been inevitably discovered absent AOL's voluntary disclosure of this information based on what it anticipated the search warrant would request.[389] The court rejected the assertion that the e-mails would have been inevitably discovered on the grounds that Air Force investigators "had ample, validly seized, evidence" under Colonel Maxwell's other screen name, indicating that he had been involved in sending and receiving child pornography.[390] The court assumed that this would have been enough "dirt" to satisfy the investigators and that they would have overlooked any additional misconduct found in their lawful search of Colonel Maxwell's computer.[391] This is a narrow view of criminal investigations. A search of Colonel Maxwell's computer would have turned up all of his screen names, including "Zirloc." It is not only likely, but probable, that Air Force investigators would have sought, and rightfully obtained, copies of the e-mails sent and received under the additional screen names to see if any additional child pornography activity existed.[392]

---

[384] 467 U.S. 431 (1984).
[385] *Id.* at 440-441 and n.2.
[386] On October 5, 1994, the National Defense Authorization Act for fiscal year 1995, Pub. L. No. 103-337, 108 Stat. 2663 (1994), renamed the United States Court of Military Appeals the United States Court of Criminal Appeals for the Armed Forces (the CAAF).
[387] 12 M.J. 389 (C.M.A. 1982).
[388] *Nix*, 467 U.S. at 444.
[389] *Maxwell*, 45 M.J. 406.
[390] *Id*. at 422.
[391] *Id.*
[392] Gilligan & Imwinkelried, *supra* note 61, at 341-42.

Compare the CAAF's rejection of inevitable discovery in *Maxwell* with the result in *Allen*, where the CAAF found that inevitable discovery did apply.[393] Because a warrant could—and clearly would—easily have been obtained in *Allen*, the CAAF found that the evidence would have been inevitably discovered.[394] In *Maxwell*, it appears that the CAAF was imposing some sort of "good faith" requirement on the ISP and was thus incorrectly decided. AOL clearly exceeded the scope of the warrant and, without the "bonus" information, OSI would have had to take extra investigatory steps to obtain the information. "Super Zippo," on the other hand, consulted with legal counsel prior to providing the information and, though the advice was wrong, the information provided would have ultimately been obtained anyway, because a warrant would have been secured if the OSI agent had been told it was required. However, the Supreme Court in *Nix v. Williams*[395] unambiguously rejected a good faith requirement in the context of inevitable discovery.[396]

One of the rare factual scenarios where inevitable discovery clearly would not apply is illustrated in *United States v. Hambrick*.[397] Hambrick was in a chat room called "Gay dads 4 sex."[398] An undercover New Hampshire police officer was observing the activity in the chat room and decided to find out the identity of the person using the screen name "Blowuinva."[399] He obtained a New Hampshire state subpoena and served it on Blowuinva's ISP.[400] The subpoena, though apparently valid on its face, was invalid because the justice of the peace who signed it was also a police officer who worked with the undercover officer.[401] The information provided by the ISP identified Hambrick, but he was a resident of another state. Thus, the New Hampshire officer turned the case over to the FBI.[402] The court correctly held that the inevitable discovery exception did not apply because, even though the same records were obtained by the FBI pursuant to a valid grand jury subpoena, the FBI would never have even known about the case but for the invalid New Hampshire warrant.[403]

---

[393] *Allen*, 53 M.J. at 409.
[394] *Id.* at 409.
[395] 467 U.S. 431 (1984).
[396] *Id.* at 445 ("[T]hat view would put the police in a *worse* position than they would have been in if no unlawful conduct had transpired. … We reject that view.").
[397] 55 F. Supp. 2d 504 (W.D. Va. 1999), *aff'd by* 225 F.3d 656 (4th Cir. 2000) *and cert. denied* 531 U.S. 1099 (2001).
[398] *Hambrick*, 55 F. Supp. 2d at 505.
[399] *Id.*
[400] *Id.*
[401] *Id.* at 506.
[402] *Hambrick*, 55 F. Supp. 2d at 509.
[403] *Id.*

The inevitable discovery exception has the potential to have enormous impact in cyberspace. Because of technological realities, there are conceivably very few circumstances in which inevitable discovery would not apply. In *Maxwell*, the CAAF found that inevitable discovery did not apply.[404] In *Allen*, without any meaningful discussion, the court found that inevitable discovery did apply.[405] The only substantial difference between the two cases is the issue of good faith. Yet, in *Nix v. Williams*,[406] the Supreme Court specifically stated that good faith was not relevant to the inevitable discovery inquiry. The operative facts in *Hambrick* represent a unique circumstance where inevitable discovery actually will not apply to cyberspace searches.

Where, then, does this leave us? Despite some well-presented arguments to the contrary, [407] on a constitutional level, principally because of user consent to monitoring and legitimate agency policies, a reasonable expectation of privacy is unlikely to be found with respect to the use of government computer systems. There is one possible exception that has not yet been adequately tested: privileged communications. While system administrators will still be able to view the content of these communications and files absent voluntary agency safeguards, it is likely that the courts will recognize the special nature of this type of information and not permit its exploitation and use in the same manner that non-privileged communications can be exploited.[408] As Lieutenant Colonel Coacher states, "[p]rotection for this kind of information does not cease simply because electronic communications are subject to monitoring."[409]

Some sort of system must be implemented to afford this type of

---

[404] *Maxwell*, 45 M.J. at 422.
[405] *Allen*, 53 M.J. at 409.
[406] 467 U.S. 431 (1984).
[407] *See e.g.*, Sundstrom, *supra* note 5.
[408] Regarding the attorney-client privilege for confidential communications, "[a] communication is 'confidential' if not intended to be disclosed to third persons other than those to whom disclosure is in furtherance of the rendition of professional legal services to the client *or those reasonably necessary for the transmission of the communication*." MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 502(b)(4) (2000) [emphasis added]. *See also*, ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) (Attorneys may use unencrypted e-mail to transmit information relating to representation of clients without violating the Model Rules of Professional Conduct. Opinion equates e-mail with commercial mail, land-line telephones and fax transmissions for purposes of privacy expectation with caveat that attorneys should consult with clients regarding use of e-mail and follow clients' instructions as to use of e-mail.) *But see*, United States v. Tanksley, 54 M.J. 169, 172 (2000) (addressing written attorney-client communication left in "plain view" on a computer monitor).
[409] Coacher, *supra* note 33, at 183.

communication additional protection.[410] Coacher advocates "[n]etwork professionals should be trained in the technical and legal responsibilities of systems administration to identify the types of communications that should receive additional protection. They should be taught not to disclose information discovered during monitoring activities, except for official purposes."[411] In fact, though, even this type of safeguard does not go far enough when the issue is privileged communications. There should be a method of flagging privileged communications in terms of context (for example, a distinctive flag, a distinctive symbol in the subject line, or by encoding the file), such that systems administrators are forbidden from viewing, or unable to view, the content of such communications absent a court order.

While the Fourth Amendment does apply to searches of government workplaces,[412] and the Supreme Court could theoretically extend this protection to content stored on government computers as well, two substantial obstacles remain in the way of establishing a legitimate expectation of privacy in e-mail when sending or receiving from government computer systems. First is the Supreme Court's decision in *O'Connor v. Ortega*,[413] adopting a relatively low standard for searches conducted in government workplaces. The second is the "risk analysis" approach ultimately engendered by the Court's framework for determining objective reasonableness in *United States v. Katz*.[414] Given the current susceptibility of Internet communications to easy interception and widespread eavesdropping,[415] under a risk analysis approach, a legitimate expectation of privacy is unreasonable.

B. The Electronic Communications Privacy Act

Though the ECPA establishes statutory privacy rights for electronic communications, it will not afford any meaningful relief to users of government computer systems. First, the ECPA does not legislatively establish a reasonable expectation of privacy where none exists under the

---

[410] *Id.*
[411] *Id.*
[412] O'Connor v. Ortega, 480 U.S. 709 (1987).
[413] *Id.*
[414] 389 U.S. 347, 361 (1967) (objects, activities or statements exposed to the "plain view" of outsiders are not protected; expectation of privacy in conversations "in the open" is unreasonable).
[415] *See generally*, Gilligan & Imwinkelried, *supra* note 61; Rogers, *supra* note 16; Skok, *supra* note 60; McTigue, *supra* note 74; Thompson, *supra* note 74; Wigod, *supra* note 74; Sessler, *supra* note 74; Barrera & Okai, *supra* note 74; *and* Schwartz, *supra* note 74.

Fourth Amendment.[416] Thus, the Fourth Amendment analysis is controlling. Second, as a non-public provider of electronic communications services, the government is simply not restrained by the statute.[417] Finally, ISPs are permitted to "intercept" communications if necessary in providing the service or protecting the rights of the ISP.[418] This provision grants broad latitude to the ISP to take whatever steps are necessary to conduct business. Additionally, "intercept" has been so narrowly interpreted by the courts as to be virtually meaningless.[419] In fact, the definition of intercept may be so narrow as to not even apply to e-mail communications, since the interception must occur at the precise moment that the e-mail is transmitted.[420] Once e-mails enter the government computer system, they become "stored" communications subject to the restraints of Title II of the ECPA.[421] Title II of the Act, governing stored communications, distinguishes between those ISPs who provide electronic communication services to the general public, and those who do not.[422] While the first category is restrained in disclosing the contents of stored communications, the latter is not restrained in any way.[423]

C. Maxwell, Monroe and *Allen*

In *Maxwell*, the CAAF stepped boldly into uncharted territory and applied the Fourth Amendment to the realm of cyberspace. While narrow and not binding outside the military, the court's holding established that there can be a reasonable expectation of privacy in e-mail. However, because *Maxwell* did not involve the use of government computer systems, it has limited benefit in determining whether there ever is, can be, or should be a reasonable expectation of privacy in the use of government computer systems. *Maxwell*'s value is that it establishes that there can be a reasonable expectation of privacy in e-mail under the proper circumstances and provides an initial framework for analyzing privacy interests in cyberspace.

Monroe comes very close to establishing that there is no hope for a reasonable expectation of privacy in the use of government computer systems. The foundation for this determination rests on both the Fourth Amendment and the ECPA. In terms of Fourth Amendment analysis, the insurmountable

---

[416] United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999), *aff'd* 225 F.3d 656 (4th Cir. 2000), *and cert. denied*, 531 U.S. 1099 (2001).
[417] CCIPS MANUAL, *supra* note 2, at Part III(E).
[418] 18 U.S.C. § 2511(2)(a)(i).
[419] Specific case law examples are provided in note 116.
[420] Coacher, *supra* note 33, at 174.
[421] *Id.*
[422] CCIPS MANUAL, *supra* note 2, at Part III(E).
[423] *Id.*

hurdle is consent. Users of government computer systems are on notice that use constitutes consent to monitoring. Such monitoring is not limited as to type (content or context) or purpose (system management, ensuring authorized use/preventing unauthorized use, maintaining system and operational security) or use (administrative, criminal and other adverse action are possible). In terms of the ECPA, the government is an electronic communications provider and, as such, is essentially unrestrained by the Act with respect to stored communications. However, the CAAF stops short of declaring that there is no reasonable expectation of privacy. Rather, the court limits this proclamation to no reasonable expectation of privacy *as to system administrators.* The court then relies on the inadvertent discovery provisions of the ECPA to permit disclosure of criminal activity to law enforcement personnel.

In *Allen,* the CAAF sidestepped the ultimate issue—whether there can be a reasonable expectation of privacy in the use of government computer systems—altogether by relying on the inevitable discovery doctrine. We are left with a limited reasonable expectation of privacy in e-mail where the use of government computer systems is not involved and an unlikely reasonable expectation of privacy in e-mail when government computer systems are used.

The CAAF has apparently retreated from its role of pioneer in *Maxwell* and is avoiding "bright-line" rules. Almost certainly this reflects uncertainty as to how to adapt old rules to emerging technologies that have radically changed our world. The more advanced the communications technology, the more susceptible it becomes to exploitation. Advances in technology are making actual privacy obsolete. The question for the legislatures and the courts then becomes what effect this has on our values and expectations of privacy. The old paradigms no longer fit and must be reassessed. "The Fourth Amendment 'is not an adjunct to the ascertainment of truth.' The guarantees of the Fourth Amendment stand 'as a protection of quite different constitutional values – values reflecting the concern of our society for the right of each individual to be let alone."[424] Do we permit technology to erode expectations of privacy in communications, or do the expectations persist, despite the reality that modern communications systems are eminently susceptible to eavesdropping? That is the ultimate puzzle, and the CAAF cannot be faulted for treading slowly into this new legal thicket.

IV. Conclusion

Monitoring of government computer systems is here to stay. Neither

[424] Schneckloth v. Bustamonte, 412 U.S. 218, 242 (1973).

the Fourth Amendment nor the ECPA, at least in its present form, will block the practice. In short, the place to look for a reasonable expectation of privacy online is not in any context that involves the use of government computer systems. The bottom line is that users of government computer systems are on notice from log-on banners and agency policies that their use of the system constitutes consent to monitoring. This monitoring clearly encompasses both context and content. Any expectation of privacy in context monitoring, despite arguments to the contrary,[425] is a lost cause from both Fourth Amendment and ECPA analyses. Content monitoring, on the other hand, is still open to considerable debate and further development of privacy-related parameters in this "new world."

Moreover, from a policy standpoint, it is operationally imperative to protect the Department of Defense (DoD) communications system and infrastructure from unlawful intrusions.[426] Systems protection monitoring also serves legitimate government interests.[427] The only unresolved issue is the extent to which the courts and DoD may be willing to go to protect from monitoring the content of certain communications stored on, or transmitted through, cyberspace from government computer systems. Context monitoring will not, and should not, go away. This is the most efficient and least intrusive method to make sure that service members are conducting themselves properly while online. Content monitoring, on the other hand, should be carefully scrutinized and judiciously utilized.

As Lieutenant Colonel Coacher suggests, changes need to be made.[428] "To the extent the purpose of monitoring shifts from protecting the system to uncovering criminal activity, the systems administrator becomes an agent of law enforcement."[429] Coacher proposes that network professionals receive additional training to recognize communications that should be protected and not disclose any such communications inadvertently viewed during routine monitoring.[430]

However, her proposed solution falls short of requirements. Systems administrators should not only receive the additional training suggested, but should also be carefully screened for professionalism and trustworthiness, similar to the screening conducted for granting of security clearances. At least

---

[425] *See generally,* Skok, *supra* note 60.
[426] Coacher, *supra* note 33, at 156-57.
[427] *Id.*
[428] *Id.* at 183-88.
[429] *Id.* at 182-83.
[430] Coacher, *supra* note 33, at 183.

for certain types of communications—notably those that are privileged, or coming from the highest levels in commands—the system administrators should either be restricted from viewing content absent a compelling, legitimate interest or, at the very least, we should put more senior people (E-7 and above) in charge of monitoring this type of communication. Where privileged communications are alleged, system administrators should not be granted the discretion to determine what can be disclosed for any purpose.

The following comprehensive solution is recommended. Context monitoring should always be permissible on government computer systems. Systems administrators should always be able to monitor and identify the sites visited by users of government computer systems to ensure that such use is in accord with the JER's ethical standards. Much of this can be done (and is being done) with software programs. Where problems are identified, system administrators can then take a more hands-on approach.

Content monitoring, on the other hand, should only be permitted in limited circumstances absent evidence that a particular user is engaging in inappropriate conduct. Content monitoring should be permitted for highly sensitive positions and those dealing with classified information on a routine basis. Content monitoring should be permitted in operational units when such units are actually engaged in operational missions to ensure that sensitive details, such as intended movement, is not intentionally or inadvertently disclosed. However, before a system administrator views the content of e-mail, some sort of programmed screening program should be in place to flag e-mails with certain words or phrases that might indicate the transmission of inappropriate material. Only when the flag raises a reasonable suspicion of wrongdoing should a system administrator read the actual content. System administrators should always be permitted to view any large attachments to e-mails and any JPEG (picture) or similar large files either sent or received by a user. However, systems administrators should not be have a license to snoop unchecked. They should not be able to read the private e-mails sent to and received from family members absent a reason to believe that the e-mail contains improper content. They should not be able to read e-mails protected by the attorney-client or clergy privilege. They should not be able to read e-mails containing sensitive command-related communications. They should not be able to read e-mails pertaining to patient medical treatment or records. They should not be able to read sensitive legal documents sent or received as part of the command's legal business. Ideally, except when operationally necessary or necessary to protect national security, content monitoring should not be permitted absent some indication that improper activity is taking place.

These recommendations seek to strike a balance between the Government's legitimate need to monitor e-mail and Internet usage, which at the same time giving some semblance of privacy to individual users.

APPENDIX A

COMPUTER USER AGREEMENT[431]

WHEREAS, I, the undersigned, in consideration of being given a computer user account on the_____ computer system (herein after referred to as "host"), which is a system owned and operated by the Department of Defense (DoD) covenant and agree as follows:

1. The individual computer workstations and host computer system are owned and operated by the Department of Defense (DoD).

2. DoD computers and computer systems are provided for the processing of official U.S. Government information only.

3. I have no expectation of privacy on any information entered, stored, or transferred through the DoD computers and host system except as specifically authorized by law or regulation.

4. Use of DoD computers and the host system are restricted to authorized users and I am responsible for all actions taken under my user account or identity. I will not permit anyone else to use the account given to me.

5. I will use the DoD computer and/or host system only as authorized. I understand that I am permitted to use this system for limited personal use that: (a) serves a legitimate public interest; (b) conforms with theater commander-in-chief (CINC) and MAJCOM policies; (c) does not adversely affect the performance of official duties; (d) is of reasonable duration and frequency, and whenever possible, is made during personal time (such as after-duty hours or lunch-time); (e) does not overburden the communications system with large broadcasts or group mailings; (f) does not create significant additional costs to DoD or the Air Force; and/or does not reflect adversely on DoD or the Air Force (such as uses involving pornography, child pornography, chain letters, unofficial advertising, soliciting or selling, violations of statutes or regulations, or other uses that are incompatible with public service).

6. I will not import any software or hardware to the system without authorization from the system administrator or my commander.

---

[431] OFFICE OF THE STAFF JUDGE ADVOCATE, AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS, COMPUTER CRIMES INVESTIGATOR'S HANDBOOK, Appendix 4 (May 1999, Updated Feb 2001) (modified slightly in form, not content, to fit format of this publication).

7. I will not attempt to access data, or use the operating systems programs, except as specifically authorized.

8. I will change my password at least every ninety (90) days.

9. I will not mask my identity or assume the identity of another user, nor shall I attempt to do so.

10. I will not enter data into the system if the data is of a higher classification level than the system. I will not enter data, which is proprietary, contractor excluded, or otherwise needs special protection, unless approved by the host computer security officer.

11. If I observe anything that indicates inadequate security or misuse of this system, I will immediately notify my immediate supervisor and the host system administrator.

12. I will follow office security procedures, official regulations, and policies applicable to computer systems operation.

13. I will not program any DoD computer to automatically forward electronic mail to a civilian computer user account.

14. I will not install any modem or remote access device without first obtaining the written permission of the host system administrator.

15. I will not use any DoD computer and/or the host system to gain unauthorized access, or attempt to gain unauthorized access, to other computers or computer systems, unless expressly authorized to do so by my commander. Further, I will not use any DoD computer and/or the host system to launch denial of service, or attempt to launch denial of service, attacks against other computers or computer systems, unless expressly authorized to do so by my commander.

16. The host system is monitored to ensure information security, system integrity, and the limitation of use for official purposes. By using the host system, I am expressly consenting to such monitoring and agree that any and all information derived from such monitoring, including connection logs between computers and my subscriber information may be used as a basis for administrative, disciplinary, or criminal proceedings.

17. I also hereby consent to the opening of any stored files and/or electronic mail that may be stored either on the host system or on any DoD computer workstation.

18. I hereby expressly authorize the system administrator to provide law enforcement with any and all information pertaining to my alleged misuse and abuse of any DoD computer and/or the host system.

19. Prior to my separation from the service, PCS, or retirement, I will notify the appropriate system administrator so that my account may be deleted.

20. I have been provided with a signed copy of this Agreement and understand that the system administrator will maintain the original.

Dated this ____ day of _____, 20__.

User:_____ User Organization:_____
(Printed name and rank)

User Location_____ User Phone Number:_____
(Rm, Bldg, Base)

Name of User Account:_____ Signature of User:_____
(e.g. "jonesRT")

Witnessed by:_____ Phone Number for SysAd:_____
(System administrator)

TO BE COMPLETED BY SYSTEM ADMINISTRATOR

Host system:_____ Server Location:_____

Designated Approval Authority:_____Phone:_____

Commander of Host System:_____Phone:_____

INNOCENT PACKETS? APPLYING NAVIGATIONAL REGIMES FROM THE LAW OF THE SEA CONVENTION BY ANALOGY TO THE REALM OF CYBERSPACE

Lieutenant Commander Steven M. Barney, Judge Advocate General's Corps, U.S. Navy*

Developments in information operations[1] have provoked considerable debate in

---

* *The positions and opinions stated in this article are those of the author and do not represent the views of the United States government, the Department of Defense, or the Department of the Navy. Lieutenant Commander Barney attended Suffolk University Law School, Boston, Massachusetts. Lieutenant Commander Barney earned his Juris Doctor degree in May 1990. In May 1990 Lieutenant Commander Barney was commissioned in the U.S. Naval Reserve. After completion of training at the Naval Justice School, Newport, Rhode Island, he reported to Naval Legal Service Office Detachment, Lemoore, California where he served as Senior Defense Counsel. In 1992 Lieutenant Commander Barney reported to Naval Air Weapons Station, Point Mugu, California as Staff Judge Advocate and was appointed as Special United States Attorney, for the Central District of California. In July 1994 Lieutenant Commander Barney reported to Naval Legal Service Office Detachment Roosevelt Roads, Puerto Rico as Officer-in-Charge. In July 1995 Lieutenant Commander Barney was assigned as Staff Judge Advocate, Commander Fleet Air Caribbean. Upon disestablishment of that command, his billet was initially assigned to Commander Western Hemisphere Group, Caribbean Area Coordinator, and finally transferred to U.S. Naval Station Roosevelt Roads, Puerto Rico. Lieutenant Commander Barney reported to the Naval Justice School in 1997 where he served as a Division Officer and Instructor until August, 2000. He then attended Naval War College, College of Naval Command and Staff where he earned his M.A. in National Security and Strategic Studies in 2001. After attending Naval War College, Lieutenant Commander Barney reported to Commander Cruiser Destroyer Group Eight, where he is currently assigned as Staff Judge Advocate*. This article was edited by Capt Andrew R. McConville, USMC.

[1] THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS, I-1, 1A. (1998).

> Information Operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems. Information Warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries[…]. Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include computer network attack. IO related activities

legal circles and raised concerns among operational commanders over the legal framework to be applied to information warfare. Initially, some U.S. government lawyers suggested the application of modern information systems technology to military purposes was so new that *no* law applied.[2] However, as lawyers and war fighters began to work with the rapidly emerging technology it was recognized that many traditional military activities included under the umbrella term of "information operations" were actually physical attacks on information systems by traditional military means. Applying international law to information operations involving physical attacks is less difficult for commanders and their lawyers because the laws regulating traditional military operations are reasonably well settled by international law and through the customary practice of States. On the other hand, it is more difficult to apply international law principles to information attacks involving the use of electronic means to gain access or change data in an enemy's computer system without necessarily causing damage to the computer itself or the telecommunications infrastructure to which it is attached.[3] This "void" in international law may be remedied over time through development of treaties. However, one scholar has observed,

> [G]iven Internet technology's exponential growth, it would seem extraordinarily useless to go through a lengthy treaty negotiation process to draft an agreement listing prohibited Internet behaviors or actions that would be as out of date as the computers that began to produce the treaty at the start of the drafting and negotiation process."[4]

This reason, as well as the lack of widespread experience in Cyberspace warfare, suggests that commanders and their lawyers must resort to drawing analogies from custom, treaties, and principles applied in the law of land, sea, air and space law to information warfare.

---

include, but are not limited to, public affairs (PA) and civil affairs (CA) activities.

Id. at I-1, 1.a.

[2] WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 5 (Aegis Research Corporation 1999) [hereinafter SHARP].

[3] U.S. DEP'T OF DEFENSE, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 4 (2d ed. 1999).

[4] George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1187 (2000) [hereinafter Walker].

If it is true that the realm of Cyberspace has a strong conceptual parallel to the realm of physical space, then the navigational regimes applied to physical space under the 1982 United Nations Convention on the Law of the Sea[5] (UNCLOS III) can be a useful and familiar conceptual framework when applied by analogy to planning and conducting operations in Cyberspace. This paper will explore how the UNCLOS III navigational regimes can be applied to information operations. It will suggest the rights of transit through Cyberspace under those regimes, and evaluate the advantages and disadvantages of applying the UNCLOS III concepts to information operations. Finally, it will suggest that the UNCLOS III analogy can address problems with r[outing information operations through the telecommunications infrastructure of neutral states.

The discussion of the legal implications of computer network attack begins with a scenario. It is 2005. In response to an unprovoked hostile act against citizens of State A by the armed forces of State Z, the national command authorities of State A authorize the use of force in national self defense, citing Article 51 of the Charter of the United Nations.[6] Because there remains a continuing threat from State Z military forces, the State A Joint Task Force commander is authorized by superiors to launch a computer network attack[7] (CNA) on a State Z military computer system. State A military forces launch the CNA from a military computer system in the territory of State A. Nearly instantaneously, the attack travels in electronic "packets" through the Internet, through communications networks in States B, C, D, E, F, and G before reaching the desired target in State Z. (Figure 1) As a result of the CNA, State Z military commanders are denied the use of their computer networks to communicate with units in the field.[8]

Under international law, did State A have the right to use the international telecommunications infrastructure to transmit a CNA on State Z?

---

[5] OCEANS L. & POLICY DEP'T, U.S. NAVAL WAR COLLEGE, U.S. NAVY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 1-14M, 1.1, 1-3 (1997) [hereinafter COMMANDER'S HANDBOOK] (noting that the 1982 United Nations Convention on the Law of the Sea, the third UN Convention on this subject, opened for signature 10 December 1982 and went into force November 16, 1994).

[6] U.N. CHARTER art. 51 (recognizing the "inherent right of individual or collective self defence" if an armed attack occurs against a Member of the United Nations).

[7] DEP'T OF DEFENSE, JOINT DOCTRINE FOR INFORMATION OPERATIONS, GL-5. A Computer Network Attack is "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."

[8] We will further assume the use of force in self defense by State A was lawful under the attendant circumstances, that disrupting State Z's computer network achieved a definite military advantage, and the use of force did not exceed what was necessary to prevent further attacks.

Was the territorial sovereignty of intermediate States violated by the CNA passing through their national telecommunications infrastructure? Did an act of force take place within their territory? Was the neutrality of those States violated? May State Z insist that neutral States prevent further CNAs from being routed through their telecommunications infrastructure? If the neutral States are willing but technologically unable to prevent further CNAs without shutting down their entire telecommunications infrastructure are the telecommunications nodes in those neutral states subject to attack by State Z? Discussion of these questions begins by examining how the purposes and language of the UNCLOS III can be adapted to operations in Cyberspace.

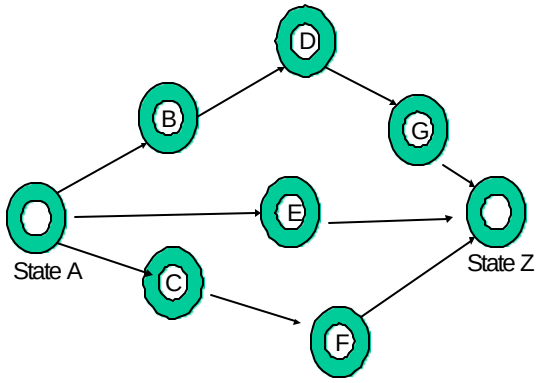


Figure 1: Hypothetical Computer Network Attack

Purposes of the UNCLOS III

The State Parties to the UNCLOS III desired to settle law of the sea issues "in a spirit of mutual understanding and cooperation [as an] important contribution to the maintenance of peace, justice, and progress for all peoples of the world."[9] The State Parties sought to resolve "problems of ocean space" through a regime that provides,

> [d]ue regard for the sovereignty of all States, a legal order for the seas and oceans which will facilitate international

[9] United Nations Convention on the Law of the Sea, Preamble, Dec. 10, 1982, 1833 U.N.T.S. 3 (entered into force Nov. 16, 1994) [hereinafter UNCLOS III].

> communication, and will promote the peaceful uses of the seas and oceans, the equitable and efficient utilization of their resources, the conservation of their living resources, and the study, protection and preservation of the marine environment.[10]

The State Parties expressly intended that the Convention benefit not only coastal States but also land-locked States and "contribute to the realization of a just and equitable international economic order which takes into account the interests and needs of mankind as a whole and, in particular, the special interests and needs of developing countries."[11] The principles of the Convention were premised on a United Nations (UN) General Assembly resolution which . . .

> [s]olemnly declared *inter alia* that the area of the seabed and the ocean floor and the subsoil thereof, beyond the limits of national jurisdiction, as well as its resources are the common heritage of mankind, the exploration and exploitation of which shall be carried out for the benefit of mankind as a whole, irrespective of the geographical location of States[…].[12]

From these oceans policy principles the UNCLOS III created an framework to balance and reaffirm the sovereignty of coastal States where necessary for safety and security while declaring international waters free for the use of all States. This notion of unimpeded high seas freedom of navigation is strikingly similar to the views of some who advocate similar rights to users of the Internet. But that freedom of Cyberspace navigation must be balanced against important national interests:

> Techno-purists feel that Cyberspace is borderless; there are no national or regional boundaries to inhibit anyone from communicating with anyone by phone, across the network, or across the universe. And from one perspective we must agree:

[10] UNCLOS III, *supra* note 9.
[11] *Id.*
[12] *Id.*

> If Cyberspace is "that place in between" the phones or the computers, then there are no borders. As we electronically project our essences across the network, we become temporary citizens of Cyberspace, just like our fellow cybernauts. By exclusively accepting this view, however, we limit our ability to create effective national information policies and to define the economic security interests of our country.[13]

A sound policy that balances international freedoms in Cyberspace with legitimate concerns about national security may be achieved by applying the navigational regimes of the UNCLOS III to the medium of Cyberspace. Fairly applied, such global Cyberspace policies could, borrowing from the language of the Convention,

- be an important contribution to the maintenance of peace, justice, and progress;
- resolve problems of Cyberspace;
- provide due regard for the sovereignty of all States;
- facilitate international communication;
- promote peaceful uses of Cyberspace and the equitable and efficient utilization of its resources;
- aid the study, protection, and preservation of the Cyberspace environment;
- contribute to the realization of a just and equitable economic order which takes into account the interests and needs of mankind as a whole and, in particular, the special interests and needs of developing countries;
- establish international Cyberspace as beyond the limits of national jurisdiction, as a common heritage of mankind, the exploration and exploitation of which shall be carried out for the benefit of mankind as a whole irrespective of the geographical location of States.

From the foregoing it is suggested that if the underlying purposes of the UNCLOS III were applied to the Cyberspace medium, it would have a desirable effect on international development of Cyberspace. A test of the

[13] WINN SCHWARTAU, INFORMATION WARFARE: CHAOS ON THE ELECTRONIC SUPER HIGHWAY 327 (Thunder's Mouth Press 1994) [hereinafter SCHWARTAU].

usefulness of this analogy in preserving national sovereignty is how well two important access rights under the UNCLOS III, "innocent passage"[14] and "transit passage,"[15] might be applied to military operations in Cyberspace.

Dividing Cyberspace

The analogy is premised on the identification of Cyberspace navigational regimes similar to the maritime navigational regimes from the UNCLOS III. To be recognized as valid, the Cyberspace analogy must be consistent with the underlying policy embodied in the UNCLOS III and be applied fairly, neither creating new rights for States nor infringing on preexisting ones. The analogy must use a balanced, rational approach to divide the intangible medium of Cyberspace into areas where sovereign rights of the individual State are preserved. It must also recognize that the Internet is part of an international telecommunication system where freedom of access benefits all States, and to which any artificially drawn boundaries would have to be consistent with legitimate issues of national sovereignty and customary international law. With those objectives in mind, the proposed analogy divides Cyberspace into regimes called national Cyberspace (Figure 2)--consisting of internal Cyberspace and territorial Cyberspace--and international cyberspace.

[14] *See generally* SCHWARTAU, *supra* note 13, Part II, § 3.
[15] *See generally Id.* Part III, § 2.

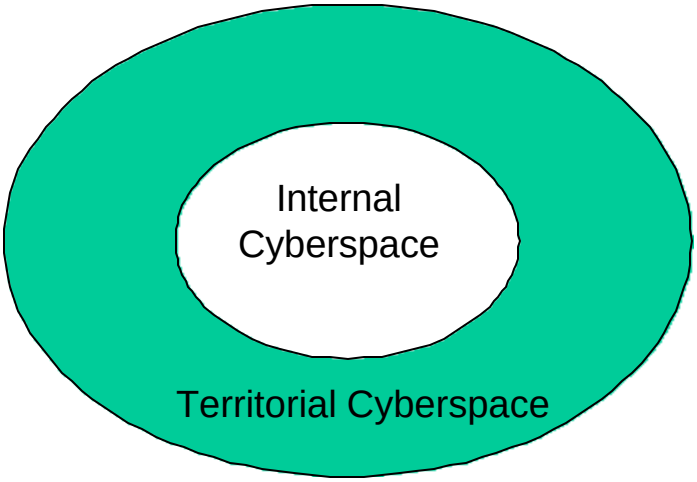


Figure 2: National Cyberspace

National Cyberspace.

National Cyberspace is the region of Cyberspace in which individual States require substantial sovereign rights to preserve the political and economic security of the State. National Cyberspace is further subdivided into internal Cyberspace and territorial Cyberspace. Understanding the distinction between internal and territorial Cyberspace is necessary to frame the overall rights and interests of national sovereignty that a State may exercise in national Cyberspace.

Internal Cyberspace

Internal Cyberspace is the region of Cyberspace where a State may exercise complete sovereignty; it is the Cyberspace equivalent to the land space, internal waters, and the air space above a State.[16] Internal Cyberspace is that medium serviced by the State's national telecommunications infrastructure[17] that is normally only accessible to authorized users (that is,

[16] UNCLOS III, *supra* note 9, art. 2 (declaring that the national airspace extends seaward from the land to the limit of the territorial sea).

[17] The term, "national telecommunications infrastructure" should be understood, in this context, to

persons with the specific permission of the computer system administrator). Internal Cyberspace includes the internal telecommunications systems of businesses and institutions that connect to the international telecommunications infrastructure by a combination of connections including cables, wires, microwave transmitters, and satellite ground stations. For example, the internal Cyberspace of the United States would include sensitive government telecommunication infrastructure and computer networks (e.g., the Department of Defense SIPRNET--Secret Internet Protocol Router Network--a computer network used for classified communications within the Department of Defense), and the equivalent internal communication networks used by businesses and organizations. Such networks, described as "critical infrastructure" by President Clinton in Executive Order 13010, include infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.[18] The President acknowledged that because so many of these critical infrastructures are owned and operated by the private sector "it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."[19] For this reason States may establish laws to prohibit unauthorized intrusion into internal Cyberspace. Moreover, as a matter of national security, the protection of internal Cyberspace becomes a matter that requires the combined efforts of military and civil authorities to establish a robust defense.[20]

Because States have interests in protecting their critical information infrastructure, the commander must evaluate the political and military risks associated with information operations that intrude into the internal Cyberspace of another State. Lawyers may provide guidance to the commander using analyses similar to that used when an intrusion of internal waters, land space, national airspace, or the territorial sea is contemplated. Depending on the circumstances of the operation, those lawyers would likely recommend a commander consult with superiors and seek permission, if possible, before

---

include both government and private telecommunications systems and not solely systems administered by and for the exclusive use of the State.

[18] Exec. Order No. 13,010, 64 Fed. Reg. 38,535 (Jul. 14, 1999) [hereinafter EO 13,010]. Signed on 15 July 1996. EO 13,010 identified the critical infrastructure into eight categories: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; including medical, police, fire and rescue; and continuity of government.

[19] SHARP, *supra* note 2, at 98.

[20] *See* Colonel James P. Terry, USMC (Ret), *Responding To Attacks On Critical Computer Infrastructure: What Targets? What Rules of Engagement?*, 46 NAVAL L. REV. 170 (1999) (providing an extensive discussion of operational considerations for computer network defense).

intruding into another State's internal Cyberspace.[21] Generally, an intrusion into another State's internal Cyberspace for the purpose of conducting military operations, including a use of force against that State to degrade, neutralize or destroy a computer network, will be lawful if the underlying use of force is authorized under Article 2 (4) or Article 51 of the Charter of the United Nations.[22]

It is more difficult to determine the appropriate response by a State to the discovery of an intrusion of its internal Cyberspace by a foreign State. An intrusion for the limited purpose of collecting intelligence, without more, is probably not a "use of force" that would immediately entitle the aggrieved State to respond with force in self defense. In such a case the most appropriate response by the aggrieved State would be to lodge a diplomatic protest of the unauthorized intrusion with the offending State as is frequently done by nations in response to discovering another State conducting espionage within its sovereign territory. However, if a State determines the intrusion constitutes a grave breach of the States national security, then use of force may be among the range of response options. An example of such a grave breach of national security would be the act of inserting a computer virus into a military command and control computer network. Assuming the intruder could be identified, any response involving the use of force by the aggrieved state must be premised on self-defense, and limited in scope to what is necessary and proportional to negate the danger posed by the intrusion.[23]

Without clear demarcation of borders or boundaries it may be difficult to determine when an information operation is at the point of intruding into internal Cyberspace. However, the practice among Internet users has begun to suggest virtual boundaries that may help avoid unintentional intrusions of internal Cyberspace. For example, some Internet sites are restricted to authorized users who register, obtain a password, or pay a fee to view materials or buy products or services on the site. Commanders conducting information operations should probably consider these types of owner/operator restrictions, by password or otherwise, as *prima facie* evidence that the site is within the internal Cyberspace of a State. The decision to intrude upon the site without authorization should be subjected to the risk analysis described above.

---

[21] *See generally* THE JOINT CHIEFS OF STAFF, CJCSI 3121.01A, CHAIRMAN OF THE JOINT CHIEFS OF STAFF STANDING RULES OF ENGAGEMENT FOR US FORCES, CJCSI 3121.01A (15 January 2000) (giving guidance on the use of force).

[22] U.N. CHARTER art. 2 (4) expressly prohibits the use of force in international relations except as authorized by the United Nations Security Council under Chapter VII or in national or collective self-defense under article 51.

[23] SHARP, *supra* note 2, at 100.

The mere use of a warning screen "banner,"[24] indicating access to the site is limited to authorized users, is probably not sufficient to indicate the site is within a States' internal Cyberspace. However the Department of Defense Office of General Counsel suggests it may be possible to specify certain information systems or Internet sites as "vital to national security," both to give those systems high priority for security measures or to warn an intruder

---

[24] *See, e.g.*, Message, 131256Z May 97, Chief of Naval Operations, subject: Communications Security (COMSEC) and Information Systems Monitoring Requirements; Message, 191445Z May 97, Commandant, Marine Corps, C4I-CIO, subject: Computer Notice and Consent Log-On Banner (Warning Screen) (19 May 1997) (citing Memorandum, Department of Defense General Counsel, subject: Communications Security (COMSEC) and Information Systems Monitoring (27 Mar. 1997)). The typical Department of Defense banner notice contains language similar to the following:

> 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. . . . DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Id.

that an attack on the system could trigger an active defense in response that could damage the intruder's computer.[25] A prudent commander will conduct a risk analysis based on the specific warning language on the site and consult with qualified counsel before authorizing the intrusion to determine whether an unauthorized intrusion might trigger a defensive response or diplomatic protest, if detected.

Territorial Cyberspace

Territorial Cyberspace is that portion of national Cyberspace through which, and to which, governments, commercial enterprises, or private organizations allow generally unrestricted access. An example of territorial Cyberspace of the United States government is the new Internet site, *http://WWW.FirstGov.gov*.[26] Developed as a single point of access to scores of government web sites, *FirstGov* enables anyone with access to the World Wide Web to "surf" for information about agencies of the United States Government. Using this web site a potential adversary could lawfully use its national intelligence capabilities to collect open-source intelligence (OSINT) information about the United States government. Similarly, hundreds of thousands of businesses and non-commercial organizations maintain web sites on the World Wide Web and provide access to users from all over the world. There are currently no restrictions on agents or employees of government agencies, corporations, noncommercial organizations and individual persons to "surf" those web sites, send electronic mail, and transfer files and funds within the territorial Cyberspace of a State.[27]

Taken together, internal Cyberspace and territorial Cyberspace

---

[25] U.S. DEP'T OF DEFENSE, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 47 (1999).

[26] Government Services Administration, Office of Governmentwide Policy, *FirstGov, at* http://WWW.FirstGov.gov (last visited 1 Feb. 2001). Visitors to the site are welcomed with the following:

> Welcome to FirstGov — the first-ever government website to provide the public with easy, one-stop access to all online U.S. Federal Government resources. This cutting-edge site gives the American people the "Information Age" government they deserve. By using the wonders of information technology to bring government closer to the American people, we can expand the reach of democracy and make government more responsive to citizens.

[27] The possible economic restriction, that a user must first have a computer with a connection to the Internet, does not change the underlying fact that once connected to the Internet the user is free to go anywhere.

comprise the national Cyberspace of a State. Within this area, States may promulgate laws to govern access to national Cyberspace and exercise police power, including the power to initiate criminal prosecution against individuals who violate State laws and who are subject to personal jurisdiction of the State.[28] States may exercise judicial authority over activities in national Cyberspace, including laws to prohibit criminal acts (such as threats to harm the person or property of another), promote consumer protection, and enforcement commercial contracts (again, subject to the requirement of having jurisdiction over a party).[29] Unlike OSINT activities in territorial Cyberspace, which are entirely lawful, a person who conducts intelligence collection activities that involve an unauthorized intrusion into internal Cyberspace may be subject to criminal jurisdiction in the State where the penetration occurred.[30]

International Cyberspace

The regime of international Cyberspace is more difficult to define because there is no physical space counterpart specifically defined in the UNCLOS III. The U.S. Navy *Commander's Handbook on the Law of Naval Operations* defines international waters "for operational purposes...[as] all ocean areas *not* subject to the territorial sovereignty of any nation."[31] Similarly, the UNCLOS III identifies the high seas as comprising "all parts of the sea that are *not included* in the exclusive economic zone, in the territorial sea, or in the internal waters of a State."[32] The "not subject" and "not

---

[28] *See* Terrence Berg, *The Impact of the Internet on State Power to Enforce the Law*, 2000 BYU L. REV. 1305 (analyzing, in depth, contemporary problems with states exercising personal jurisdiction in criminal and civil cases involving the Internet). Generally a person must be physically present within the jurisdiction of the court before being tried. *See* International Shoe v. Washington, 326 U.S. 310 (1945); Shaffer v. Heitner, 433 U.S. 186 (1977); World-Wide Volkswagen v. Woodson, 444 U.S. 286 (1980); Helicopteros Nacionales de Colombia v. Hall, 466 U.S. 408 (1984) (establishing the legal requirements for *in personam* , or personal, jurisdiction in civil cases). *See* Strassheim v. Daily, 221 U.S. 280 (1911) (recognizing the "detrimental effects" test for exercising extraterritorial criminal jurisdiction).

[29] The question of personal jurisdiction for activity in Cyberspace is beyond the scope of this paper. The discussion of jurisdiction is merely intended to show the extent of national sovereignty that a State may exercise over activities conducted in national Cyberspace.

[30] *See generally* Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 68 U.S. NAVAL WAR COLLEGE INT'L L. STUDIES, 1978-1994 (1995). While international law does not prohibit States from conducting espionage, it is well settled that State's may prosecute individual persons who conduct espionage if they are found within the physical territorial jurisdiction of the State.

[31] COMMANDER'S HANDBOOK, *supra* note 5, at 1.5. For the purposes of this paper the term "nation" in the COMMANDER'S HANDBOOK is the equivalent of "State." [Italics in original.]

[32] UNCLOS III, *supra* note 9, Part VII, § 1, art. 86 [Italics added]. The regime of exclusive economic zones (EEZ) is unique to physical space. Although coastal States retain specific rights over the resources found within the water column in the EEZ, those rights do not otherwise

included" language in both definitions is significant in several respects. First, it reflects the primary approach taken in the UNCLOS III to specifically define those waters subject to the national jurisdiction of coastal States, and leave all other waters outside the jurisdiction of any State. Second, by defining international waters and the high seas in the negative--"not subject" to, and "not included," in coastal State jurisdiction, respectively--it reinforces the notion that, except for areas of the ocean in which coastal States have clearly identifiable and protected interests, no State has the right to declare jurisdiction over international waters. Finally, it suggests that the approach advocated for defining navigational regimes in Cyberspace is consistent with the intent of the UNCLOS III because it reinforces the underlying principle that outside national Cyberspace, commanders may move Cyber Forces with freedom from restrictions by other States, giving due regard for the rights of others.[33] Therefore, international Cyberspace is not a physical place; it is a *characteristic* of Cyberspace by which a data packet is not physically present anywhere but is merely in transit within the international telecommunications infrastructure and therefore not subject to the territorial sovereignty of any State.[34]

Under this analogy, since States would have authority to exercise jurisdiction over national Cyberspace, it may be possible for a State to close its national Cyberspace to information operations. While possible, it is not probable because one of the characteristics of the Internet is that no single organization controls access to the World Wide Web, "nor is there any centralized point from which individual Web sites or services can be blocked from the web."[35] To close national Cyberspace would require the State to cut off virtually all access to its own domestic telecommunications network, a measure that would be extremely disruptive and unsuitable except in the most grave threats to national security. However, if access to national Cyberspace is merely restricted, and telecommunication nodes are still accessible to international Cyberspace the UNCLOS III analogy provides two exceptions to the sovereignty of coastal States over national waters: innocent passage and transit passage.[36] These transit rights could be exercised to "move" Cyber

---

restrict the freedom of all States within the international waters, provided those freedoms are exercised with due regard to the rights of the Coastal State. *See id*. art. 58.

[33] SHARP, *supra* note 2, at 15.

[34] Walker, *supra* note 4, at 1104.

[35] *Id*. at 1099.

[36] Horace B. Robertson, *The New Law of the Sea and the Law of Armed Conflict at Sea,* 68 U.S. NAVAL WAR COLLEGE INT'L L. STUDIES, 1978-1994 286 (1995) (discussing the EEZ and quoting Ambassador Elliott Richardson):

Forces through national Cyberspace without the obligation to notify the State or any intermediate States, as suggested in the hypothetical scenario at the beginning of this paper.

Innocent Passage and Transit Passage in Cyberspace

The rights of innocent passage and transit passage under the UNCLOS III are exceptions to the general rule that Coastal States may limit access by foreign ships to national waters. While both innocent passage and transit passage may be exercised by warships, both passage rights have specific limitations which must be considered by the operational planner seeking to employ either or both passage rights as a legal basis to move forces through physical space. For Cyberspace navigation, it will be seen that Cyberspace transit passage is the preferred, though not the exclusive, mode that could be employed. The following brief analysis demonstrates that the right of transit passage gives the commander superior flexibility as compared to the right of innocent passage.

The right of innocent passage gives the ships of all States the right to traverse the territorial sea in a continuous and expeditious manner, so long as that passage is not prejudicial to the peace, good order, or security of the coastal State. Certain actions by a warship or State vessel may be considered "not innocent" and thus inconsistent with the right of innocent passage through the territorial sea of a coastal State under Article 19 of the Convention. Those limitations, coupled with the right of coastal States to temporarily suspend the right of innocent passage when necessary for the security of the coastal State, reduce the value of innocent passage to the operational planner. Applying those same limitations to the right of innocent passage through the territorial Cyberspace (Figure 3), an operational planner may be unable to rely on unfettered use of Cyberspace innocent passage if the Cyber Force could be characterized as violating any of the proscribe activities listed in Article 19 of

---

> In the group which negotiated this language it was understood that the freedoms in question…must be *qualitatively* and *quantitatively* the same as the traditional high-seas freedoms recognized by international law: they must be qualitatively the same in the sense that the nature and extent of the right is the same as the traditional high-seas freedoms; they must be quantitatively the same in the sense that the included uses of the sea must embrace a range no less complete--and allow for the future uses no less inclusive--than traditional high-seas freedoms.[119]

the Convention.[37]

[37] UNCLOS III, *supra* note 9, Part II, § 3, art. 19(2). The activities proscribed under Article 19(2) include:

> (a) any threat or use of force against the sovereignty, territorial integrity, or political independence of the coastal state, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations;
>
> (b) any exercise or practice with weapons of any kind;
>
> (c) any act aimed at collecting information to the prejudice of the defense or security of the coastal State;
>
> (d) any act of propaganda aimed at affecting the defense or security of the coastal State;
>
> (e) [omitted];
>
> (f) the launching, landing or taking on board of any military device;
>
> (g) the loading or unloading of any commodity, currency or person contrary to the customs, fiscal, immigration or sanitary laws and regulations of the coastal State;
>
> (h) the act of willful and serious pollution contrary to this Convention;
>
> (i) [omitted];
>
> (j) the carrying out of research or survey activities;
>
> (k) any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State;
>
> (l) any other activity not having a direct bearing on passage.

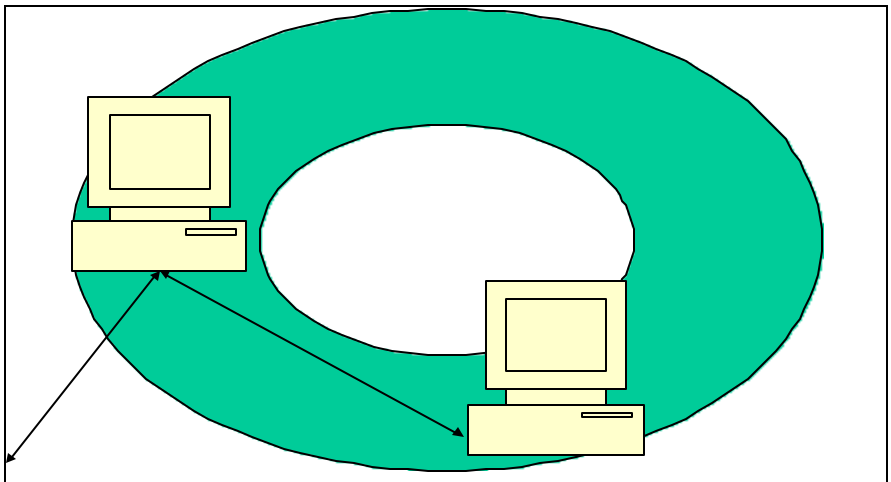


Figure 3: Cyberspace Innocent Passage, State B

Analysis of the factors listed in the Convention as "prejudicial to the peace, good order or security of the coastal State" if conducted in the territorial sea suggests that any right of innocent passage would be at least as limited in territorial Cyberspace as that enjoyed by physical ships. In particular, restrictions under Article 19(2)(a) and (k) could directly impact a military operation involving CNA if the effect of the threat or use of force actually interferes with communications, facilities, or installations of the transited state.[38] However, if no action or use of force is intended to be used

[38] It may be argued that the remainder of the limitations under UNCLOS III art. 19(2) could further limit the right of innocent passage in Cyberspace, but a complete discussion of those limitations is beyond the scope of this article. Some problem areas include the following sub articles: (a) the question of when a military operation in Cyberspace constitutes a use of force requires applying the legal restraints on the use of force imposed by Article 2(4) of the Charter of the United Nations [*See* SHARP, *supra* note 2, at 137 ("What constitutes a prohibited 'threat or use of force' in Cyberspace and elsewhere is a question of fact that must be subjectively analyzed in each and every case in the context or all relevant law and circumstances.")] (c) the ordinary use of the Internet to collect open-source intelligence (OSINT); (g) the loading or unloading of a computer sniffer program, virus, logic bomb, or Trojan horse as a "commodity" contrary to the laws and regulations of the coastal State; (h) any action, willfully targeted toward another State which results in serious pollution contrary to the Convention, affecting the coastal State; (j) research or survey activities intended to identify features and vulnerabilities of the telecommunications infrastructure of the State; (k) the broad proscription on interfering with "any

against the transited State, then Cyber innocent passage may be authorized. A more thorny problem with using innocent passage to justify movement of force through Cyberspace is the proscription against "any threat or use of force against the sovereignty, territorial integrity, or political independence of the coastal State, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations."[39] Even assuming no threat or use of force is directed against the *transited* State, there still remains the issue of whether innocent passage through Cyberspace may be limited if the use of force is targeted against a *third* State. The U.S. view of military use of innocent passage has been that "cargo, destination, or purpose of the voyage cannot be used as a criterion for determining that the passage is not innocent," and that "possession of passive characteristics, such as the innate combat capabilities of a warship, do not constitute 'activity'" within the territorial sea in regard to the enumerated list.[40] Applying that rationale to Cyberspace innocent passage, the fact that a Cyberspace transmission contains an information "weapon" with destructive capability does not render passage "non-innocent."

Therefore, the maritime navigational regime of transit passage provides significantly greater flexibility to the commander than does innocent passage and, when applied by analogy to Cyberspace operations, more closely matches how the international telecommunications infrastructure supports information operations (Figure 4). In maritime navigation, the right of transit passage allows all ships and aircraft freedom of navigation and overflight solely for the purpose of continuous and expeditious transit of the international strait between one part of the high seas or an exclusive economic zone and another part of the high seas or an exclusive economic zone. Ships and aircraft exercising the right of transit passage may proceed without delay through or over the strait, in their normal mode of operations, and must refrain from the threat or use of force against the sovereignty, territorial integrity or independence of States bordering the strait.[41] Therefore it would violate the rights of all States to exercise transit passage if, for example, Spain or

---

systems of communication" of the coastal State may be invoked if actions directed against a third State have a foreseeable collateral effect on the Coastal State; (l) the "other activity not having a direct bearing on passage" language points to the underlying assumption of innocent passage, being specifically a limited waiver of territorial sovereignty only when passing through the territorial sea or Cyberspace.

[39] UNCLOS III, *supra* note 9, Part II, § 3, art. 19(2)(a).

[40] COMMANDER'S HANDBOOK, *supra* note 5, § 2.3.2.1, 2-8 n.27 (summarizing testimony of Professor (Rear Admiral) H.B. Robertson, *Before the House Merchant Marine & Fisheries Comm.*, 97th Cong., *Hearing on the Status of the Law of the Sea Treaty Negotiations*, 27 July 1982, Ser. 97-29, at 413-14 and Professor B. Oxman, ¶ 2.1.1, 2-1 n.2 at 853, respectively.

[41] UNCLOS III, *supra* note 9, Part III, § 1, art. 34-39.

Morocco closed the Straits of Gibraltar to ships and aircraft transiting between the Atlantic Ocean and the Mediterranean sea. The right of transit passage through these *physical* international straits is important to the international economy, communication, and to national and collective self defense. In a like manner States and their people must use their national telecommunications infrastructure to access international Cyberspace. Therefore the State's national telecommunications infrastructure is the Cyberspace equivalent of an international strait.

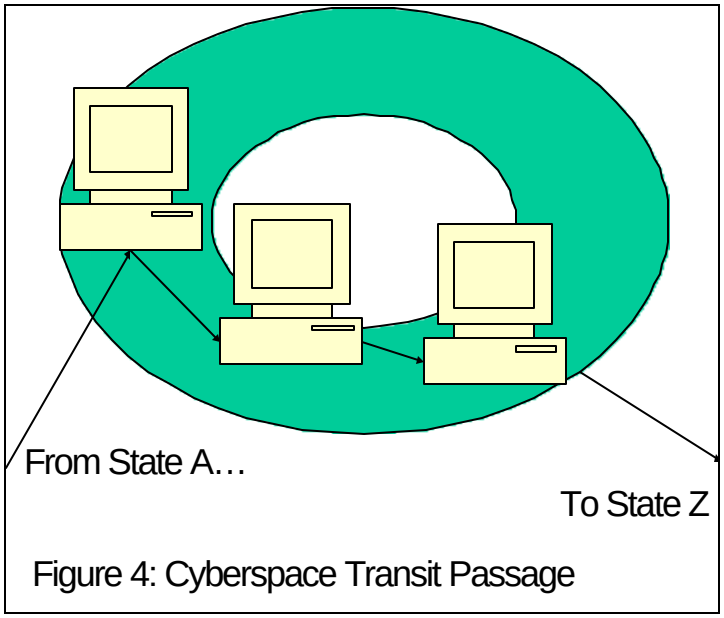


Figure 4: Cyberspace Transit Passage

When navigating Cyberspace international straits, users behave much like ships and aircraft engaged in transit passage: they proceed without delay, in the normal mode of continuous and expeditious transit, and refrain from any threat or use of force against the national Cyberspace through which their communication is routed. The nature of telecommunications means Cyber Forces transit Cyberspace almost instantaneously and without delay except as limited by system bandwidth during periods of peak demand. The high speed of transmission is valuable to the commander as well as the State through which the Cyber Force is transmitted. The combination of speed and volume of Internet traffic means most States have limited capability to intercept and monitor Cyberspace communications. This limited ability to intercept and monitor traffic through Cyberspace is important to maintaining the neutrality

of states that are mere intermediaries in information warfare, as in our opening scenario, because the transited State is unlikely to be aware of the transmission.

In summary, transit passage provides the commander two major advantages over innocent passage: forces may transit in their normal mode of operation[42] and bordering States may not suspend the right of transit passage through international straits. When applied to Cyberspace the proscription against suspending transit passage is a strong argument for applying the UNCLOS III by analogy to Cyberspace. While governments, corporations and private organizations may choose to suspend access to their internal Cyberspace for various reasons, as global economies become more dependent on the international telecommunications infrastructure it is unlikely that States could or would entirely close national Cyberspace. Even if a State tried to close national Cyberspace it would have little effect on the ability to transfer CNA packets through international Cyberspace because if intermediate routers are not available the packet will be automatically rerouted. Finally, if a belligerent State, like State A in the opening scenario, were to specifically route a CNA through the Cyberspace of a neutral intermediate state that act alone would be insufficient to violate the neutrality of the transited State if the Cyberspace transit passage analogy is used.

Neutrality in the Era of CyberWarfare

Codification of the navigational regimes in the UNCLOS III had an immediate impact on the application of customary international law of armed conflict to the maritime environment. One scholar, Rear Admiral Horace B. Robertson, JAGC, U.S. Navy (retired), observed that the navigational regimes of the UNCLOS III directly impacted the rights of neutral States. Admiral Robertson noted,

> [o]ne of the advantages of the new transit passage concept is that it keeps the littoral States bordering straits with great strategic value out of the vicious circle of escalation in times of tension and crisis. If transit through such straits were subject to the discretion of the coastal States, they would unavoidably become involved even if the

[42] *See* UNCLOS III, *supra* note 9, Part III, § 2 (Transit Passage), art. 39. The normal mode for submarines, submerged; for aircraft carriers, while conducting flight operations; for aircraft, while flying defensive cover for transiting surface ships.

> discretionary power were to be exercised evenhandedly[…]. The escalation preventing quality of transit passage in times of tension and crisis--i.e. in time of fragile peace---are even more important for neutral States in times of armed conflict.[43]

This is a particular advantage to States that are neutral in international armed conflict and is equally applicable to both traditional military operations and information operations.

The right of states to remain neutral in international armed conflict is well established under international law. The Hague Convention No. XIII, *Concerning the Rights and Duties of Neutral Powers in Naval War* (Hague XIII),[44] comprises the latest expression in treaty form of the respective rights and duties of neutrals and belligerents with respect to hostile activities within neutral "maritime territory" (that is, internal waters and the territorial sea) and may be used as a starting point for discussion of these issues for our UNCLOS III analogy.[45]

The UNCLOS III and the international law of armed conflict created special challenges for neutral States that must be reconciled with Hague XIII.[46]

---

[43] Robertson, *supra* note 36, at 282 quoting RAUCH, THE PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS FOR THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS AND THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA: REPERCUSSIONS ON THE LAW OF NAVAL WARFARE 32 (1984) [hereinafter RAUCH].

[44] HAGUE CONVENTION NO. XIII, THE HAGUE, 18 October 1907, 36 Stat. 2415, 2 Am. J. Int'l L. (Supp) 202. [hereinafter HAGUE XIII). Hague XIII has not received universal ratification, but most of its provisions are considered to be a statement of customary international law.

[45] Robertson, *supra* note 36, at 276. [Footnote omitted.]

[46] *Id.*

The significant provisions of HAGUE XIII are as follows:

> Belligerents are required to respect the sovereign rights of neutral States and to abstain from acts that would constitute a violation of neutrality (article 1); […]
>
> Belligerents cannot use neutral ports or waters as a base of operations nor erect any apparatus to communicate with belligerent forces at sea (article 5);
>
> **A neutral Government must employ the "means at its disposal"** to prevent the fitting out or arming of vessels within its jurisdiction which it believes are

Hague XIII uses the terms "neutral waters" or waters "within its jurisdiction," or similar terms to refer "either to the internal waters or the territorial waters (territorial sea) of the neutral State", since those were the only areas of the oceans recognized at that time as being within the jurisdiction or sovereignty of the coastal State.[47] The cardinal principle of the law of neutrality is that belligerents may not conduct hostilities in neutral territory, land, or sea. Neutral states have an obligation to use the means at their disposal to conduct surveillance of their waters to ensure that belligerents do not violate their neutrality and to take preventive or corrective action if they detect such violations.[48] As the application of the law of neutrals has evolved through state practice over time, so too the changes in technology, including information warfare, do not cause states to discard those aspects of international law concerning neutrals which have become customary.

Robertson concluded that since the same rules apply to the post UNCLOS III territorial sea that formerly applied in the narrow territorial sea,

> …[a]s a matter of principle belligerents are bound to respect the sovereignty of neutral

---

> intended for cruising or engaging in hostile operations and to prevent departure from its jurisdiction of such vessels (article 8);
>
> A Neutral State must apply its rules and restrictions impartially to the belligerents may forbid the entry of vessels which have violated its rules or its neutrality (article 9);
>
> The "mere passage" of belligerent warships or prizes through a neutral's territorial sea does not affect the neutral's neutrality (article 10);
>
> Unless the neutral's regulations provide otherwise, belligerent warships may remain in neutral ports, roadsteads or territorial waters no more than 24 hours (article 12);
>
> A neutral State must exercise such surveillance "as the means at its disposal allow" to prevent violation of its territorial waters (article 25); and
>
> The exercise of its rights under the Convention by a neutral cannot be considered an unfriendly act by a belligerent (article 26).

[47] Robertson, *supra* note 36, at 276.
[48] *Id*. at 278.

> powers and to abstain, in neutral territory or neutral waters from any act of warfare. Any act of hostility, including capture and the exercise of the right of search, committed by belligerent warships in the territorial waters of a neutral power, constitutes a violation of neutrality and is strictly forbidden.[49]

Counterbalancing this requirement for belligerents to refrain from violating neutrality is the obligation of the neutral State to conduct surveillance in their territorial waters to ensure belligerents comply. In an observation that immediately illustrates the difficulty of conducting surveillance of national Cyberspace, Robertson notes the perils created for the neutral State under the UNCLOS III:

> The emergence of a "new" peacetime regime for the oceans, with its expansion of existing zones subject to national jurisdiction and the creation of new zones also subject to the same or similar forms of jurisdiction, has created problems of adaptation of the traditional rules of armed conflict at sea to these new developments…. As has been suggested by the foregoing analysis, however, the geographic and operational factors that determine the nature and scope of naval operations in time of armed conflict, and, in particular, the relationships between belligerent and neutral forces, render it uncertain as to whether such mechanical application of prior rules to new or expanded areas of national jurisdiction serves the best interests of either neutrals or belligerents or the humanitarian objectives of the rules. Massive expanses of waters that are denied to belligerents for hostile operations and for which neutral States have burdensome duties of surveillance and

[49] *Id*. at 279 citing RAUCH, *supra* note 43.

> control are likely to increase beyond belligerents' power to resist the temptation to violate such waters and to overtax the capabilities of neutral States to enforce their duties within them. The result may well be increased tension between neutral and belligerent States with the consequent danger of widening the area of conflict and drawing neutral States into it.[50]

Robertson's recommendations for reformulating the rules of naval warfare that are affected by the emergence of new zones in the "new" law of the sea may be readily adapted by commanders and their lawyers to the emerging requirements for the new zones of Cyberspace described in this paper. [51] Those recommendations, found in pertinent part at Appendix A, could serve as a useful policy to protect the rights of neutrals by guaranteeing that the mere transit of a computer network attack through a neutral States' national Cyberspace would not cause the loss of neutral status.

Conclusion

This paper has proposed that the navigational regimes under the 1982 United Nations Law of the Sea Convention could be applied by analogy to information operations involving a computer network attack. It was suggested that the CNA described in the scenario at the beginning of the paper may be lawfully transmitted through the international telecommunications infrastructure, including Internet routers physically located in neutral States, by applying Cyberspace analogies of innocent passage or transit passage. The concept of Cyberspace transit passage gives commanders greater flexibility for information operations than does Cyberspace innocent passage, because under the UNCLOS III States have the right to temporarily suspend innocent passage. During the near instantaneous transmission of the CNA to the intended target in the opening hypothetical, the CNA passed through international Cyberspace. The territorial sovereignty of those intermediate States was therefore not violated, nor did an act of force take place within their territory. For that reason, and because most States lack the technological

[50] Robertson, *supra* note 36, at 302.

[51] The author has substituted the Cyberspace terminology developed in this paper for the traditional UNCLOS III maritime terms, and eliminated those sections of Rear Admiral Robertson's analysis that do not apply to our analogy, such as maritime zones of archipelagic waters and exclusive economic zones.

means to detect, intercept, and identify the CNA as it passes through the Internet, those neutral States had no obligation to prevent the transit of their national Cyberspace and their status as neutrals was not violated. Perhaps this analogy will provide a future Joint Task Force Commander with the conceptual tools needed to more effectively plan and conduct operations in and through Cyberspace with greater certainty that the courses of action involving the use of force in Cyberspace will comply with international law.[52]

[52] A prudent commander will seek and obtain the assistance of qualified legal counsel at the earliest planning stages. Qualified counsel must be consulted to determine whether, if at all, the analogy proposed in this paper comport with customary international law under the specific circumstances.

Appendix A

A Proposal to Adopt Selected Principles from The Hague Convention No. XIII, Concerning the Rights and Duties of Neutral Powers in Naval War to Information Operations

3. Neutral [Cyberspace] consist of the internal [Cyberspace], territorial [Cyberspace], and where applicable, the [national Cyberspace], of a State which is not a party to the armed conflict.

4. Within neutral Cyberspace, hostile acts by belligerent forces are forbidden. A neutral State must exercise such surveillance and enforcement measures as the means at its disposal allow to prevent violation of its neutral Cyberspace by belligerent forces.

5. Hostile acts within the meaning of paragraph 4 include […. e.] Use [of neutral Cyberspace] as a base of operations.

6. Subject to the duty of impartiality, and under such regulation as it may establish, a neutral State may, without jeopardizing its neutrality, permit the following acts within its neutral [Cyberspace]:

a. Innocent passage […]

7. A belligerent [may not cause a transmission with offensive information operation capability to] extend its stay in neutral [Cyberspace] [….]

8. Belligerent [States] may exercise the right of transit passage through neutral international straits [in Cyberspace]. While within neutral [Cyberspace] comprising an international strait […] belligerent […] forces are forbidden to carry out any hostile act.

9. Should a neutral State be unable or unwilling to enforce its neutral obligations with respect to hostile military activities by belligerent […] forces within its neutral [Cyberspace], the opposing belligerent may use such fore as is necessary within such neutral [Cyberspace] to protect its own forces and to terminate the violation of neutral [Cyberspace].

10. A neutral State shall not be considered to have jeopardized its neutral status by exercising any of the foregoing neutral rights nor by allowing a belligerent State to exercise any of the privileges permitted to a belligerent State."[53]

[53] Robertson, *supra* note 36, at 302.

Appendix B

Innocent Packets? Applying Navigational Regimes from the 1982 UNCLOS III to the Realm of Cyberspace…Additional Thoughts by the Author.

Since submitting this article, other ideas have come up as I have further considered operations in Cyberspace:

1. The analogy is useful to help commanders and their staffs develop a common operational picture during initial planning. As the time for the operational use of an information weapon approaches, especially review of proposed targets, evaluation of the operation shifts more toward traditional law of armed conflict considerations of necessity, proportionality, and humanity.

2. As a fundamental principle of law, express obligations under international and domestic law will always take precedent over use of the proposed analogy. For that reason, the excellent treatment of specific legal requirements described in the DoD Office of General Counsel paper, *An Assessment of International Legal Issues in Information Operations, Second Edition, November 1999,* is a valuable resource for planning information operations.

3. There are likely to be circumstances where the analogy simply does not work. Information operations typically involve special access programs and application of highly sensitive capabilities and technology. Because this paper was written to stimulate general discussion in an unclassified academic environment, no classified material was used. In planning an actual operation, capabilities of specific information weapons must be carefully reviewed with a view toward identifying specific legal requirements. In sum, slavish application of the analogy is neither advocated nor intended.

4. My bias in evaluating this topic is toward enabling the consideration and use of information weapons where they can provide a definite military advantage. To that end, I suggest using this analogy to help propel the discussion of information weapons beyond the "it can't be done" stage, if that response is based solely on the fact that no specific law enabling the proposed use can be found.

5. The navigational regimes under UNCLOS III apply to both military and commercial vessels. But, in practice, some coastal States view use of the

regime of innocent passage by warships passing through their territorial seas with great suspicion. Some States impose limitations on innocent passage by warships that are inconsistent with UNCLOS III and are rejected by the United States and other maritime nations. With that in mind, a prudent commander will always consider the effect on international relations of a legitimate exercise of navigational rights under UNCLOS III if it would create tension with a coastal State. For example, the regime of innocent passage allows, among other things, vessels to stop and anchor within the territorial seas. This is considered consistent with the continuous and expeditious passage so long as anchoring is consistent with prudent navigation. On the other hand, stopping and anchoring a warship in the territorial seas may be considered unacceptably provocative by the coastal State, even if it is expressly authorized under UNCLOS III. Just as commanders regularly apply their good judgment to the implications of an assertion of rights under UNCLOS III on the seas, their best judgment must also be applied when conducting operations in Cyberspace.

6. The logical linkage between physical and Cyberspace innocent passage is difficult to grasp. Once again, examination of the practice of innocent passage under UNCLOS III can help illustrate application of the analogy. In the case of UNCLOS III innocent passage, the choice to navigate through the territorial sea of a coastal State is ordinarily related to a specific purpose. In most cases, the choice of innocent passage indicates the captain or master of the transiting vessel has specifically determined that passage through the territorial seas of a coastal State produces a definite advantage over the alternative, that is, avoiding passage through the territorial seas and remaining in international waters thereby enjoying largely unrestricted high seas freedom of navigation. In most cases that advantage may be no more than the desire to reduce distance traveled, yielding savings in time and fuel consumption. But it is also true that the reason for choosing innocent passage could be any reason at all, so long as it does not cause the passage to become "non-innocent." In the Cyberspace realm, by analogy, the rationale supporting the choice of Cyberspace innocent passage may be any reason so long as it, too, does not cause the passage to become non-innocent. In contrast, the transit passage regimes of both physical and Cyberspace do not require the same degree of specific intent to pass through territorial seas as in the case of innocent passage. Under transit passage, the specific intent is merely to navigate from high seas on one side of an international strait to the high seas on the other side. Passage through the overlapping territorial seas of the coastal States bounding the international straits is of less importance and is merely incidental to the general intent underlying transit passage. Returning to our analogy for operations in Cyberspace, the distinction between innocent passage and transit

passage are ultimately related to the more specific intent *to enter* national Cyberspace in the former, and the more general intent *to transit* in the latter. Indeed, one might argue it does not stretch the analogy too far to suggest that, as in physical space, a decision to "stop and anchor" in territorial Cyberspace is permissible as long as the stop is "incidental to ordinary [Cyber] navigation."

TOO MUCH OF A GOOD THING? FEDERAL SUPREMACY & THE DEVOLUTION OF REGULATORY POWER: THE CASE OF THE COASTAL ZONE MANAGEMENT ACT

Lieutenant Patrick J. Gibbons, JAGC, USN*

I. Introduction

Contemporary federalism debates have increasingly focused on environmental policy.[1] After years of expanding federal regulatory power, authority now seems to be shifting back toward the states.[2] Federal environmental regulation, a frequent source of federal-state friction[3] may be broadly characterized under two schemes.[4] One approach is the abandonment of state involvement in favor of federal control, such as the regime of the Toxic Substances Control Act.[5] Another approach is "cooperative federalism," in which the federal government delegates administrative and enforcement responsibilities to the states in varying degrees.[6] This is often described as "layered cake" federalism because each level of government is

---

* *LT Patrick Gibbons (B.A., University of Virginia, 1992; M.A., University of Virginia, 1993; J.D., University of Virginia 2001) is currently assigned as Trial Counsel at Trial Services Office Southeast, Jacksonville Detachment. Prior to serving as a Judge Advocate, LT Gibbons served as Division Officer onboard, USS STOUT (DDG 55); aide to Director, Naval Reserve (OPNAV NO95); and as a student at the University of Virginia School of Law through the Law Education Program.* This article was edited by LCDR Karen M. Somers, JAGC, USN.

[1] *See* Robert V. Percival, *Environmental Federalism: Historical Roots and Contemporary Models*, 54 MD. L. REV. 1141, 1141 (1995)[hereinafter Percival I].

[2] *See Id.* at 1142.

[3] *See Id.* at 1144.

[4] One commentator has identified three approaches to environmental regulation, differentiating between arrangements in which the federal government sets standards for the states to enforce, and those in which the states are free to set their own standards subject to federal approval. *See id* at 1141- 44. For purposes of this Article, the distinction is unimportant and only two classes are necessary.

[5] *See Id.* at 1176.

[6] *See Id.* at 1173-76.

assigned a distinct role within the whole scheme.[7] Cooperative federalist statutory arrangements purport to return to the states some of the regulatory power that the federal government has assumed in the last sixty years, and give the states a greater voice in allocating the costs of regulation.

One cooperative federalist regime which is often held up as a model for the devolution of regulatory power to the states is the Coastal Zone Management Act (CZMA),[8] where the federal government provides incentives to the states to encourage them to establish their own regulatory schemes.[9] Although the incentive is often financial, in the case of the CZMA Congress offered the additional carrot of federal consistency.[10] In a departure from federal supremacy, Congress effectively assimilates a state's law as codified in its coastal management plan and applies it to federal agencies.[11] Once a state coastal management plan is approved by the Secretary of Commerce, all federal agency activities directly affecting or within the coastal zone must be consistent with the state plan "to the maximum extent practicable,"[12] or must be of such overriding national importance that the President exempts them from the consistency requirement.[13] Consistency neither wholly waives nor wholly preserves federal supremacy, but does subject agencies to stricter controls than intergovernmental coordination requirements.[14] "[I]t is clear that federal development projects in the coastal zone . . . are subject to state coastal management policies and may be substantially modified at the insistence of the states to conform to these policies."[15] Federal agencies are required to do more than consider state programs and coordinate their activities with state agencies, yet they are not totally subordinated to state law.[16] Although an attempt to restore the balance of state-federal power, this departure from traditional federalism paradoxically undermines the federal system by

---

[7] *See* Ronald J. Rychlak, *Coastal Management and the Search for Integration*, 40 DEPAUL L. REV. 981, 987 (1991) [hereinafter Rychlak].
[8] *See* 16 U.S.C.A. § 1451 et *seq.* (West 2001).
[9] *See* Percival I, *supra* note 1, at 1173. "While the [CZMA's] collaborative framework is not without its limitations, it holds considerable promise. . . ." TIMOTHY BEATLEY ET AL., AN INTRODUCTION TO COASTAL ZONE MANAGEMENT, 196 (1994)[hereinafter BEATLEY].
[10] *See* 16 U.S.C.A. §§ 1454-56 (West 2001).
[11] *See* William C. Brewer, *Federal Consistency and State Expectations*, 2 COASTAL ZONE MANAGEMENT J. 315, 321 (1976)[hereinafter Brewer].
[12] 16 U.S.C.A. § 1456 (West 2001).
[13] *See Id.* at § 1456(c) (West 2001).
[14] *See* Richard L. Kuerstein & Paul M. Sullivan, *Coastal Federalism: the Role of the Federal Supremacy Doctrine in Federal and State Conflict Resolution*, 33 JAG J. 39, 42 (1984)[hereinafter Kuerstein & Sullivan].
[15] BEATLEY, *supra* note 9, at 69.
[16] *See Id.* at 41.

restricting agencies acting under authority explicitly given to the federal government by the Constitution, such as national defense.

In general, courts are sensitive to the Constitutional and practical limitations on judicial involvement in the national security arena, and consequently defer to defense agencies when required to mediate between defense and environmental concerns.[17] This generality does not apply to activities subsumed under the Coastal Zone Management Act, however, because of the Act's requirement that federal agency actions within the coastal zone be consistent with approved state plans to the maximum extent practicable.[18] This potentially subordinates national defense interests to state and local land use and environmental regulatory interests. National security is mentioned explicitly only once in the Act, and then only in the context of federal licensing and permitting.[19]

This article explores the potential subversion of federalist concerns in environmental schemes that were designed to further the federalist arrangement by looking at the tensions between what is perhaps the most "federal" (i.e. most broadly national) of federal concerns, national security, and the CZMA's federal consistency requirement. This article argues that in pursuing an arrangement that purports to restore traditional federal-state distributions of power, the Coastal Zone Management Act inadvertently goes too far and gives the states excessive power. Section II traces the history of federal involvement in coastal environmental regulation and the movement leading up to the passage of the CZMA. It then examines the main provisions of the Act and how it has evolved through several reauthorizations and amendments. Section III takes a closer look at current environmental federalism debates, the federalist distribution of state and national power, and the consistency provisions of the Act. Section IV examines the only three judicial decisions rendered in consistency disputes involving a defense agency. The cases illustrate the federalism concerns discussed in Section III. The final Section discusses possible solutions to the difficulties inherent in delegating regulatory power to the states while still preserving federal supremacy over matters of national concern.

---

[17] *See* STEPHEN DYCUS, NATIONAL DEFENSE AND THE ENVIRONMENT, 154 (1996)[hereinafter DYCUS].
[18] *See* 16 U.S.C.A. § 1456(c) (West 2001).
[19] *See Id.* at § 1456(c)(3) (West 2001); *see also* Richard L. Kuerstein, et al., *Protecting Our Coastal Interests: a Policy Proposal for Coordinating Coastal Zone Management, National Defense, and the Federal Supremacy Doctrine*, 8 B.C. ENVTL. AFF. L. REV. 705, 715 (1980).

II. The Coastal Zone Management Act

The Coastal Zone Management Act was enacted by Congress after three years of negotiation and debate, as part of a larger legislative effort to pass laws to protect and improve the environment. Since then it has been reauthorized five times, and amended almost as often, to mirror changes in the nation's environmental priorities. The fact that it still exists reflects, in itself, the continued commercial and environmental importance of the nation's coastlines. This section examines the background context of the CZMA and the regime it has created. Subsection A. surveys generally the history of regulation to preserve the coasts and the effort to create federal legislation to protect the resources of the shore. Subsection B. then describes the legislative history of the Act and the subsequent amendments that have resulted in the Act's present form.

A. Historical Context

Prior to the rise of modern regulation, land use, real estate development, and pollution abatement were controlled through the common law of nuisance.[20] To the extent that the federal government regulated land use at all, it was usually to promote development, such as grants to railroads and the commercial development of inland waterways.[21] The first federal erosion control activity occurred in 1829, when the government acted to restore the ground beneath Fort Moultri in South Carolina.[22] In 1899, Congress enacted the Rivers and Harbors Act, banning discharges into the nation's waters. This was intended not to protect water quality but to ensure unimpeded navigation.[23] Legislation concerning public health and environmental preservation were largely absent.[24] Even the rapid expansion of federal regulation that accompanied the New Deal had minimal environmental content.[25]

---

[20] *See* Percival I, *supra* note 1, at 1152-55; ROBERT V. PERCIVAL ET AL., ENVIRONMENTAL REGULATION, 87-89 (2d ed. 1996) [hereinafter PERCIVAL II]. *See also, e.g.,* Missouri v. Illinois, 200 U.S. 496 (1906)(holding that Missouri failed to establish that Chicago's sewage caused an increase in typhoid fever in St. Louis); New York v. New Jersey, 256 U.S. 296 (1921)(holding that New York failed to demonstrate the New Jersey sewage discharges into New York harbor created a nuisance); New Jersey v. City of New York, 283 U.S. 473 (1931)(holding that New York City's at-sea garbage dumping created a nuisance for New Jersey).
[21] *See* Percival I, *supra* note 1, at 1147-49.
[22] *See* Rychlak, *supra* note 7, at 984.
[23] *See* PERCIVAL II, *supra* note 20, at 105.
[24] *See* Percival I, *supra* note 1, at 1147-49.
[25] *See Id.* at 1155.

The economic boom that followed World War II in the United States contributed to a rapid expansion of activity in the coastal zone.[26] The Truman Proclamation[27] focused attention on the coastal zone in 1945,[28] and in the subsequent effort to expand America's exploitation of the oceans' wealth, Congress provided research and financial aid to the states.[29] From 1945 until the emergence of the environmental movement in the 1960s, federal environmental policies generally placed responsibility with state and local governments to regulate and protect their resources.[30] For example, the 1948 Water Quality Act provided grants to the states to fund water pollution control and limited federal involvement to financial and research assistance.[31] The then-existing, decentralized scheme, while successful in encouraging the exploitation of the coastal zone, failed to capture the environmental costs of that development.[32] The increases in use and exploitation were consequently accompanied by a rapid decline in coastal resources and water quality.[33] The 1960s witnessed technological innovations which increased access to and development in the coastal zone.[34] Investment was particularly focused on military and commercial uses.[35] While the federal government continued to place regulatory responsibility with state and local government, appreciation nevertheless grew as to the interstate character of the resulting pollution.[36] This awareness coincided with the general spread of grassroots support for the environment in the 1960s.[37] It was a period of re-evaluation of the effectiveness of environmental protection and land use planning.[38] Although the federal government was experimenting with cooperative efforts with the states such as the Water Resources Planning Act of 1965 and the Intergovernmental Cooperation Act of 1968,[39] initial federal land regulation of environmental impacts was aimed at federal agencies.[40]

---

[26] *See* Judith Kildow, *The Roots and Context of the Coastal Zone Movement*, 25 COASTAL MANAGEMENT 231, 233 (1997)[hereinafter Kildow].
[27] *See* Exec. Order No. 9633, 10 C.F.R. § 12305 (1945).
[28] *See* Kildow, supra note 26, at 232.
[29] *See* Percival I, *supra* note 1, at 1155.
[30] *See Id*. at 1156.
[31] *See* PERCIVAL II, *supra* note 20, at 104.
[32] *See* Kildow, *supra* note 26, at 232.
[33] *See Id*. at 232.
[34] *See Id*. at 234.
[35] *See Id*.
[36] *See* Percival I, *supra* note 1, at 1156.
[37] *See Id*. at 1159.
[38] *See* David R. Godschalk, *Implementing Coastal Zone Management: 1972-1990*, 20 COASTAL MANAGEMENT 93, 97 (1992)[hereinafter Godschalk].
[39] *See* Brewer, *supra* note 11, at 316.
[40] *See* PERCIVAL II, *supra* note 20, at 105-6. *See also* National Historic Preservation Act, 16 U.S.C.A. § 470 (West 2001) et seq.; National Environmental Policy Act, 42 U.S.C.A. § 4321(West 2001) et seq.

By the middle of the decade, a coastal crisis was recognized.[41] Advocates of outdoor recreation, marine resource development, estuarine protection, and land use policy were calling for some form of federal action.[42] These advocacy groups reflected the increased type and extent of coastal zone usage in the twenty years since the Truman Proclamation. Outdoor recreation was among the United States' top ten economic activities in the 1960s.[43] The outdoor enthusiasts' lobbying was rewarded by the passage of the Land and Water Conservation Fund Act of 1964.[44] Advocates to protect estuarine areas argued that the coastline was more than a mere place for fun.[45] Congressional efforts on the preservationists' behalf began in 1965, with a House bill proposing the creation of a wetlands preservation area on Long Island which, although it failed, inspired a subsequent bill for a national preservation program.[46] The Clean Water Restoration Act of 1966 passed, authorizing among other things a comprehensive National Estuarine Pollution Study.[47] Through continued effort and negotiation, the Estuary Protection Act passed in 1968.[48]

While the recreational and protectionist movements advanced in more or less successive chronological order, the two other advocacy efforts were essentially concurrent.[49] Ocean development proponents succeeded in attaining the passage of the Marine Resources and Engineering Development Act.[50] Nearly simultaneously, land use control advocates pushed to enact legislation that would subsume coastal zone management into a larger national land use scheme.[51] Their effort was a logical progression from the earlier work of the recreational activists, extending national estuaries protections to the whole of the coastal zone.[52]

Several studies recommended federal action in the coastal zone, including two Department of the Interior estuary studies, and studies by the American Law Institute and the Marine Sciences Council, a Cabinet-level

---

[41] *See* Godschalk, *supra* note 38, at 97.
[42] *See Id.*
[43] *See* Zigurds L. Zile, *A Legislative-Political History of the Coastal Zone Management Act of 1972*, 1 COASTAL ZONE MANAGEMENT J. 235, 237 (1974)[hereinafter Zile].
[44] *See Id.* at 240.
[45] *See Id.* at 241.
[46] *See Id.* at 245-47.
[47] *See Id.* at 253.
[48] *See* Zile, *supra* note 43, at 247-53.
[49] *See Id.* at 267.
[50] *See Id.* at 256.
[51] *See Id.* at 268.
[52] *See* Zile, *supra* note 43, at 269.

group led by Vice President Hubert Humphrey.[53] But arguably the most important was *Our Nation and the Sea*, the report of the Commission on Marine Science, Engineering, and Resources, commonly known as the Stratton Commission.[54] The Stratton Commission was formed in 1966 pursuant to the Marine Resources and Engineering Development Act.[55] Chaired by and named for Julius Stratton, President of the Massachusetts Institute of Technology, the Commission was charged with undertaking a comprehensive study of American ocean interests.[56] While the report's scope spans the spectrum of U.S. oceans interests,[57] it was particularly influential in its recommendations for the coastal zone.[58] Julius Stratton actually coined the term "coastal zone" to describe the area in which the ocean interfaces with land.[59]

The report recognized the economic and ecological importance of the nation's coastal resources and its unique characteristics,[60] and highlighted the special management challenges it presented because of the fragmentation of authority on the federal and state levels and the disarray into which the coastal zone had descended.[61] In pursuing its objective, the Commission considered the interests of the groups that brought coastal zone concerns to the fore: advocates of outdoor recreation, marine resource development, estuarine protection, and land use policy. Of these four, the development and land use interests ultimately proved most influential in the Commission's report.[62] The Commission suggested a regulatory regime focused on the states, with the federal government's regulatory role limited to encouraging the states to adopt plans with promises of grants as an incentive.[63] The Commission also recognized the federal government's unique interests and responsibilities in the coastal zone, including its roles as both a polluter and a developer.[64] To reconcile its proposal to give states the lead and yet accommodate these federal roles, the Commission posited a scheme under which the federal government would review and approve proposed state plans; after approval, federal agencies would be bound to ensure their activities were conducted in a manner

---

[53] *See* DEP'T. OF COMMERCE, U.S. OCEAN POLICY IN THE 1970S: STATUS & ISSUES, IV-7 (1978).
[54] *See generally* COMM'N ON MARINE SCIENCE, ENGINEERING AND RESOURCES, OUR NATION AND THE SEA (1969)[hereinafter COMM'N ON MARINE SCIENCE].
[55] *See* Kildow, *supra* note 26, at 235.
[56] *See Id*.
[57] *See generally* COMM'N ON MARINE SCIENCE, *supra* note 54.
[58] *See* Zile, *supra* note 43, at 259-60.
[59] *See* Godschalk, *supra* note 38, at 97.
[60] *See Id*; Kildow, *supra* note 26, at 235.
[61] *See* Kildow, *supra* note 26, at 235; Godschalk, *supra* note 38, at 97; COMM'N ON MARINE SCIENCE, *supra* note 54, at 56.
[62] *See* Godschalk, *supra* note 38, at 97.
[63] *See* COMM'N ON MARINE SCIENCE, *supra* note 54, at 56.
[64] *See Id*. at 60.

consistent with that plan.[65] The Commission also proposed the formation of the National Oceanic and Atmospheric Administration (NOAA), which it envisioned as a sort of "wet NASA" to explore and exploit the oceans' wealth.[66] Administration of the coastal zone management plans would be one of NOAA's responsibilities.[67] The Commission made its report in 1969 after three years of study. As will be seen below, its results would profoundly influence the final structure of the Coastal Zone Management Act.

The ninety-first Congress considered the first coastal zone management bills in 1969.[68] The Nixon administration followed through on Vice President Spiro Agnew's promise to offer a draft coastal zone management bill by submitting one prepared by the Department of the Interior, which was closer in emphasis and philosophy to the findings of the more environmentalist-oriented National Estuarine Pollution Study than the Stratton Commission report.[69] Although no coastal zone management bills were enacted, the ninety-first Congress still adjourned with a consensus as to the state management approach the Commission suggested.[70] The ninety-second Congress witnessed the growing interest among congressional committees in the coastal zone management proposals, which reflected the increased importance of coastal development and environmental concerns.[71] One important aspect of the debate was whether the eventual regime would fall within the purview of the Department of Interior or the Department of Commerce; the result was felt likely to determine the orientation of the Act toward either environmental or development concerns.[72]

The final form of the Coastal Zone Management Act was passed following a Senate-House compromise in 1972.[73] The coastal zone management debate was overshadowed by land use proposals, and in the Act's final form, the coastal zone was given to Commerce, on the assumption that the Secretary would delegate his powers to the Administrator of NOAA.[74] The next subsection describes the Act itself and its evolution over the last twenty seven years.

---

[65] *See Id*. at 61.
[66] *See Id*. at 230; *see also* Zile, *supra* note 43, at 257-58.
[67] *See* COMM'N ON MARINE SCIENCE, *supra* note 54, at 61.
[68] *See* Godschalk, *supra* note 38, at 98.
[69] *See* Zile, *supra* note 43, at 261.
[70] *See* Godschalk, *supra* note 38, at 98-99.
[71] *See* Zile, *supra* note 43, at 270.
[72] *See Id*. at 262.
[73] *See* Zile, *supra* note 43, at 273.
[74] *See Id.*; *see also* Godschalk, *supra* note 38, at 99

B. The CZMA Regime

Since its inception, the Coastal Zone Management Act[75] has been distinguished by its voluntary nature.[76] It proposes a series of incentives to the states rather than penalties, and accords them broad latitude to define their priorities in undertaking a Coastal Zone Management Plan (CZMP), through a process one commentator has called "co-production."[77] In addressing the spectrum of environmental challenges faced in the coastal zone, the Act embodies the federal government's first major effort at an integrated environmental program, considering pollution in all its varied forms.[78] Indeed, the term "coastal zone" implies integration across geographic bounds.[79] The Act functions through a "layered cake" approach to federalism, assigning distinct roles to each discreet layer of government as part of the whole regime: the local government is to assess and decide issues such as land use and zoning, while the state and federal governments provide financial and research assistance.[80]

Congress declared a four-part national policy in the Act:

> (a) to preserve, protect, develop, and where possible, to restore, to enhance, the resources of the Nation's coastal zone for this and succeeding generations,
>
> (b) to encourage and assist the state to exercise effectively their responsibilities in the coastal zone through the development and implementation of management programs to achieve the use of the land and water resources of the coastal zone giving full consideration to ecological, cultural, historic, and esthetic values as well as to needs for economic development,

---

[75] *See* 16 U.S.C.A § 1451 (West 2001) *et. seq*.
[76] *See* Godschalk, *supra* note 38, at 111.
[77] *See Id*.
[78] *See* Rychlak, *supra* note 7, at 983.
[79] *See Id.* at 985.
[80] *See Id.* at 987.

> (c) for all Federal agencies engaged in programs affecting the coastal zone to cooperate and participate with state and local governments and regional agencies in effectuating the purposes of this title, and
>
> (d) to encourage the participation of the public, of Federal, state, and local governments and of regional agencies in the development of coastal zone management programs.[81]

The Act goes on to prescribe the three major characteristics of the regime it created: grants to fund the development of state CZMPs in § 1454;[82] grants to underwrite the cost of administering approved CZMPs in § 1455;[83] and federal consistency requirements in § 1456.[84]

Section 1454 provided that the Secretary of Commerce could grant funds to any coastal state for the purpose of developing and implementing a CZMP.[85] Grants would be contingent upon the state incorporating in its plan certain requirements, including a definition of the boundaries of the coastal zone, identification of the means by which the state proposed to exert control over the land and water uses, and guidelines for priority of uses.[86] Grants were limited to only eighty percent of the state's total costs, and were renewable for only four years.[87] Plans already in development at the time of the CZMA's enactment were eligible for grants if the state was in the process of bringing the plan into compliance with the Act.[88]

Section 1455 provided administrative grants to states with approved CZMPs to administer their programs.[89] The administrative grants program and § 1454 are the financial part of Congress' two-pronged inducement to develop a plan. Once a CZMP is developed, the federal government will subsidize a portion of the Plan's execution costs.[90] In order to qualify for administrative

---

[81] Godschalk, *supra* note 38, at 99 (quoting 16 U.S.C. § 1452 (1972)).
[82] *See* 16 U.S.C.A. § 1454 (West 2001).
[83] *See Id*. at § 1455.
[84] *See Id*. at § 1456.
[85] *See Id*. at § 1454(a).
[86] *See Id*. at § 1454(b).
[87] *See Id*. at § 1454(c).
[88] *See* 16 U.S.C.A. § 1454(d) (West 2001).
[89] *See Id*. at § 1455 .
[90] *See Id.*

grants, however, the state must satisfy § 1455(c).[91] First, it must demonstrate that it has provided the relevant federal agencies the opportunity to participate in developing the plan.[92] Second, it must demonstrate that it has followed the prescribed enactment procedures, including holding public hearings and designating a single agency with the authority to implement the program and to receive and administer the grants.[93]

The requirements of §§ 1454 and 1455 were construed in *API v. Knecht* to afford NOAA and the enacting state broad discretion in establishing the CZMP.[94] The American Petroleum Institute and other plaintiffs initiated the suit seeking declaratory and injunctive relief against the Commerce Department's acceptance of California's Coastal Management Plan (CCMP), contending that the proposed plan failed to satisfy the Act's requirements for two reasons: the CCMP was not a "management plan" as defined by § 1455 of the Act, and the procedures followed to develop the plan violated the Act.[95] After summarizing the plaintiffs' argument in detail, the court interpreted their complaint as essentially contending that the CCMP lacked sufficient specificity.[96] If the plaintiffs' allegations were correct, then in the absence of the relief sought they would be required to spend money to determine whether their projects, primarily development of the oil and gas resources of the Outer Continental Shelf, were consistent with the CCMP without any reasonable assurance of state approval.[97] The trial court was not happy with the Act or with the issues it was required to sort out; it characterized them as:

> [Q]uestions of the highest importance, greatest complexity, and highest urgency. They arise as a result of high legislative purpose, low bureaucratic bungling, and present inherent difficulty in judicial determination. In other words, for the high purpose of improving and maintaining felicitous conditions in the coastal areas of the United States, the Congress has undertaken a legislative solution, the application of which is so complex as to make it almost wholly unmanageable. In

[91] *See Id.* at § 1455(c).
[92] *See Id.* at § 1454(d) (West 2001).
[93] *See Id.* at § 1455(c)(2);(d).
[94] 456 F. Supp. 889 (C.D. Cal. 1978)
[95] *See Id.* at 893.
[96] *Knecht*, 456 F.Supp. at 896.
[97] *See Id.* at 896-97.

> the course of the legislative process, there obviously came into conflict many competing interests which, in typical fashion, the Congress sought to accommodate, only to create thereby a morass of problems between the private sector, the federal bureaucracy, the state legislature, the state bureaucracy, and all of the administrative agencies appurtenant thereto.[98]

Later, the court expressed further frustration:

> [T]he Court sits in review of agency action which stretches over a long period of time, includes non-transcribed public hearings, not essentially adversary in nature, and in fact, quite the contrary . . . . At times the Court has the sense that the record by its very nature permits only an occasional brief glance into the workings of the administrative decision-making process in this instance.[99]

Despite these irritations, the court held that Congress intended that management programs need only be specific enough "to guide public and private uses."[100] The Act, the court continued, was first and foremost concerned with the environment, a concern not changed by the 1976 Amendment, which expressed a national interest in the siting of energy facilities.[101] The "adequate consideration" provision, according to the court, was intended to achieve an equitable balance between federal and state concerns, not to impose an affirmative burden on the states in crafting their plans.[102] Provided that the development and decision-making process of creating a management plan took place within the context of cooperation, coordination, and information sharing among the local, state, and federal agencies that Congress intended, the states were free to make their own

---

[98] *Knecht*, 456 F.Supp. at 895-96.
[99] *Id.* at 899, n. 6.
[100] *Knecht*, 456 F.Supp. at 919 (quoting 16 U.S.C.A. § 1453(12) (West 2001)(defining "management plan")).
[101] *See Id.*
[102] *Knecht*, 456 F.Supp. at 925.

decisions.[103] The guarantee against arbitrary state decisions provided to a consistency applicant is the option to appeal to the judiciary or the Secretary of Commerce.[104] The latitude permitted states by the Act in crafting their plans reverberates in the federalism question; as will be discussed in Section IV below, some states use that discretion to force federal benefits rather than merely to prevent harm to the coast.

Section 1456 required federal agency consistency with an approved state coastal management plan.[105] Consistency requirements fall into two categories: first, actions by federal agencies must be consistent "to the maximum extent practicable;"[106] second, applicants for federal permits or licenses to conduct activities in the coastal zone must provide a certification with their application that their activities are consistent with the state CZMP, and must provide a copy of the certification to the state.[107] The state then notifies the agency at the earliest practicable time, but within six months, of its concurrence in or objection to the proposed activity, and no license or permit may be issued without the state's concurrence.[108] The Act provides, however, that the Secretary of Commerce may override a state's objection should he determine that the activity is consistent with the objectives of the Act or is otherwise necessary in the interest of national security.[109] The consistency provision and its implications are addressed in Section III below.

The CZMA was not enacted without criticism: "Critics . . . described the act as 'poorly drafted, deficient in substantive standards, vague on policy, and uncertain regarding agency responsibility' . . . . Environmentalists would have preferred an act with a stronger federal role . . . ."[110] Despite these criticisms, the Act has survived almost thirty years, undergoing amendments and revisions to reflect the national mood and changes in the priorities of different Presidents. The ninety-fourth Congress reauthorized and amended the Act in 1976 in response to the energy crisis of the mid-1970s.[111] The Act as amended sought to advance national energy self-sufficiency by funding state needs for new energy activities through the Coastal Energy Impact Program (CEIP).[112] The amendment also attempted to

---

[103] *See Id.* at 923-24.
[104] *See Id.* at 926.
[105] 16 U.S.C.A. § 1456 (West 2001).
[106] *Id.* at § 1456(c)(1).
[107] *See Id.* at § 1456(c)(3).
[108] *See Id.*
[109] *See Id.*
[110] Godschalk, *supra* note 38, at 100 (quoting Zile, *supra* note 43, at 235-36.)
[111] *See* BEATLEY, *supra* note 9, at 70.
[112] *See Id.* at 70; *see also* Godschalk, *supra* note 38, at 102

clarify the states' role in Outer Continental Shelf development.[113] Additionally, it provided a mediation process to resolve state/federal disagreements of state programs.[114] The 1980 reauthorization was an attempt to guide the states' implementation process, and was captioned the "Coastal Zone Management Improvement Act."[115] It outlined nine areas of national interest that states would be required to address: natural resource protection, hazards management, major facility siting, public access for recreation, redevelopment of urban waterfronts and ports, simplification of decision procedures, coordination of affected federal agencies, public participation, and living marine resource conservation.[116] The amendment also required a written assessment of the extent to which a state addressed the national interest needs, and provided for a reduction in funding in the absence of progress to address them.[117] The amendment added § 1455a, which provided grants to states to fund construction and beach access improvement projects.[118]

The ninety-ninth Congress passed the 1986 Coastal Zone Management Reauthorization Act to continue the Act's programs, albeit under a tighter budget.[119] The 1990 Reauthorization, however, strengthened the environmental aspects of the Act in several ways. First, it reinstated the development grants for states without CZMPs, which had been allowed to lapse,[120] and it established a non-point source pollution control requirement to be implemented through the CZMA and the Clean Water Act.[121] Most significantly, it revised the consistency provisions to overturn *Secretary of Interior v. California*,[122] making all federal activities inside or outside the coastal zone subject to consistency determinations if they affected the coastal zone.[123] In 1984, the Supreme Court ruled that the sale of Outer Continental Shelf oil and gas leases by the Department of the Interior did not require a consistency determination because it did not "directly affect" the coastal zone, since the federal lands exclusion extended to OCS submerged lands.[124] California had brought suit against Interior to force it to make a consistency determination prior to selling

---

[113] *See* Godschalk, *supra* note 38, at 102.
[114] *See Id.* at 102.
[115] *See* BEATLEY, *supra* note 9, at 70-71; *see also* 16 U.S.C.A. § 1451(West 2001).
[116] *See* 16 U.S.C.A. § 1452 (2) (West 2001); *See also* Godschalk, *supra* note 38, at 105; BEATLEY, *supra* note 9, at 71.
[117] *See* 16 U.S.C.A. § 1461 (West 2001); *see also* Godschalk, *supra* note 38, at 105.
[118] *See* 16 U.S.C.A. § 1455a (West 2001); *see also* Godschalk, *supra* note 38, at 105-6.
[119] *See* BEATLEY, *supra* note 9, at 72; *see also* Godschalk, *supra* note 38, at 108.
[120] *See* 16 U.S.C.A § 1454 (West 2001); *see also* Godschalk, *supra* note 38, at 110.
[121] *See* 16 U.S.C.A. § 1455 (West 2001); *see also* Godschalk, *supra* note 38, at 110; BEATLEY, *supra* note 9, at 71-72
[122] 464 U.S. 312 (1984).
[123] *See* 16 U.S.C.A. § 1456 (c)(3) (West 2001); *see also* Godschalk, *supra* note 38, at 110.
[124] *See Secretary of the Interior*, 464 U.S. at 315.

leases to explore for oil and gas on the Outer Continental Shelf, on the theory that leasing sales set off a chain of events culminating in the development of OCS resources.[125] Examining the Congressional record, the Court interpreted Congress' intent to be that state regulation under the CZMA reached some but not all federal activities;[126] since a lessee did not acquire the right to explore fully or to develop OCS oil and gas, lease purchasing was exempt from consistency requirements.[127] The 1990 Reauthorization broadened the scope of consistency to include any affect, direct or indirect, on the coastal zone, even if the activity occurred on federal lands excluded from the coastal zone by definition.

The Coastal Zone Management Act thus creates a regime in which states are encouraged to plan how their coasts are used in a rational and environmentally-sound manner. Congress induced states to participate in this regime through offers of financial assistance and federal consistency. The consistency provisions, by submitting federal agency action to state review and approval, present a challenge to the federal system. The implications of that challenge are the subject of the next section.

III. Federalism, National Security, and the Consistency Provision

A. Environmental Regulation and the Federalists

The federal environmental legislation of the 1970s has as its hallmark the "cooperative federalism" approach to dividing state and federal responsibility and authority.[128] Cooperative federalism was Congress's answer to the challenge of finding the best possible fit between environmental problems and regulatory responses.[129] The goal of cooperative federalism is to preserve state autonomy and responsibility while providing a level of uniformity to environmental programs.[130] Generally, states are given the opportunity to assume all or a portion of the responsibility for a regulatory program provided they meet standards set by Congress or a designated

---

[125] *See Id.* at 317-19.
[126] *See Id.* at 323.
[127] *See Id.* at 317.
[128] *See* Mark Squillace, *Cooperative Federalism Under the Surface Mining Control and Reclamation Act: Is This Any Way to Run a Government?* ENV. L. REP. (Envtl. L. Inst.) February, 1985[hereinafter Squillace].
[129] *See* Daniel C. Esty, *Revitalizing Environmental Federalism*, 95 MICH. L. REV. 570, 574 (1996)[hereinafter Esty I].
[130] *See* Katheryn Kim Frierson, Comment, *Arkansas v. Oklahoma: Restoring the Notion of Partnership Under the Clean Water Act* 1997 U. CHI. LEGAL F. 459 (1997)[hereinafter Frierson].

agency.[131] As an additional incentive, the federal government usually funds at least part of the program.[132] The resulting scheme balances the "general perception that groups seeking better levels of environmental quality are relatively more effective at the federal level, and, therefore, federal regulation is likely to be more protective of the environment"[133] against the argument that the states are the more appropriate vehicle of regulation.[134]

Cooperative federalism offers some distinct advantages over more or less-centralized systems. Ideally, it moves decision-making to the lowest level of government that can internalize all the economic consequences of a decision and still conform to central government policies.[135] Varieties of cooperative federalism such as the Coastal Zone Management Act also provide state oversight of federal compliance; the federal government, as the Stratton Commission recognized, is itself a major polluter.[136] With cooperative federalism, "United States environmental policy makers have established a clear trend towards independent oversight of all governmental polluters."[137]

There are however strong arguments in favor of centralizing some environmental decisions. Professor Daniel Esty points out that the psychological externalities of local decisions may not be captured by a decentralized system, particularly when the boundaries of a resource or problem are not fixed.[138] "[D]ecentralized decision-making may exclude from representation, albeit passively, the views of significant numbers of citizens."[139] His proposed solution to this "choice of public"[140] problem is to set decision-making power at the appropriate community (rather than political) level, defined by citizenship instead of geographic boundaries.[141] For example, management decisions related to the Grand Canyon should arguably reflect the

---

131 *See* Squillace, *supra* note 128.
132 *See Id.*
133 Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race-to-the-Bottom" Rationale for Federal Environmental Protection*, 67 N.Y.U. L. REV. 1210, 1223 (1992)[hereinafter Revesz].
134 *See generally Id.*
135 *See* Daniel L. Rubinfield, *On Federalism and Economic Development*, 83 VA. L. REV. 1581, 1588 (1997)[hereinafter Rubinfield].
136 *See* COMM'N ON MARINE SCIENCE, *supra* note 54, at 56.
137 *See* Adam Babich, *Our Federalism, Our Hazardous Waste, and Our Good Fortune*, 54 MD. L. REV. 1516, 1549 (1995)[hereinafter Babich].
138 *See* Esty I, *supra* note 129, at 595-96.
139 *See Id.* at 649.
140 Esty distinguishes "choice of public," meaning choice of the appropriate community to make a decision, problems from "public choice" issues. *See Id.* at 597.
141 *See Id.* at 596.

value all Americans place on the Grand Canyon and not just that of Arizonans.[142]

How community is defined is a case-by-case judgment; environmental "success" may conflict with other social goals.[143] "Optimal environmental governance must therefore be understood to be both relevant and contextual."[144] Sub-optimal governance may not take full cognizance of other social values.[145] "Special interest groups often try to use the regulatory process to advance their own . . . position. As a result, environmental policymakers frequently do not have the public interest fully (and only) in mind when they make policy decisions."[146] One interest that would potentially be undervalued by local or state decision-makers is national defense.

In arguing for the adoption of the Constitution, the Federalist papers make a compelling case for the supremacy of the federal government over the states in issues of overarching national concern, and for the exemption from state control of federal activities pursuant to those concerns. National defense is one of the areas with regard to which Hamilton makes a case most strongly for supremacy. In Federalist XXIII, he maintained that:

> The authorities essential to the care of the common defense are these: to raise armies; to build and equip fleets; . . . to direct their operation; to provide for their support. These powers ought to exist without limitation; because it is impossible to foresee or define the extent and variety of national exigencies, or the correspondent extent and variety of the means which may be necessary to satisfy them. The circumstances that endanger the safety of nations are infinite; and for this reason no constitutional shackles can wisely be imposed on the power to which the care of it is committed.[147]

---

[142] *See Id.* at 639.
[143] *See* Daniel C. Esty, *Toward Optimal Environmental Governance*, 74 N.Y.U. L. REV. 1495, 1572 (1999)[hereinafter Esty II].
[144] *Id.*
[145] *See* Esty II, *supra* note 143.
[146] *Id.* at 1514.
[147] THE FEDERALIST No. 23 (Alexander Hamilton).

Should the states control defense issues, "[t]he security of all would thus be subject to the parsimony, improvidence, or inability of a part."[148] James Madison argued for the importance of supremacy in maritime defense particularly:

> The palpable necessity of the power to provide and maintain a Navy, has protected that part of the Constitution against a spirit of censure, which has spared few other part. It must, indeed, be numbered among the greatest blessing of America, that as her Union will be the only source of her maritime strength, so this will be a principal source of her security against danger from abroad.[149]

If the Federalists were writing today, their eighteenth-century eloquence would likely be replaced by such modern, drier economic terms as free-riders and holdouts: "because one state can protect itself simply by relying on a neighbor's defense, none of the states will undertake defense itself, even though each prefers a nation with defense to a nation without defense."[150] "Such interjurisdictional problems present a serious structural challenge and generally can only be addressed by authorities acting from a more overarching perspective, bringing within the ambit of the regulatory calculus all cost bearers and beneficiaries."[151] A central government's coercive power to resolve these issues is the Federalists' answer to the collective action problem.[152] The consistency provisions of the Coastal Zone Management Act illustrate the potential cost to the Nation hidden in the cooperative federalism scheme.

B. Federal Consistency

The Coastal Zone Management Act is concerned with an area of state control but national importance. In crafting the Act, Congress sought to effect a "more equal partnership" between the states and the federal government in

---

[148] THE FEDERALIST No. 25 (Alexander Hamilton).
[149] THE FEDERALIST No. 40 (James Madison).
[150] Note, *To Form a More Perfect Union?: Federalism and Informal Interstate Cooperation*, 102 HARV. L. REV. 842, 845 (1989)[hereinafter Note].
[151] Esty II, *supra* note 143, at 1513.
[152] *See* Note, *supra* note 150, at 846.

coastal zone issues.[153] Through the Stratton Commission and other studies, Congress identified threats to coastal zone resources from increasing population and development.[154] It then created a cooperative-federalist arrangement to induce the states to manage and plan their coastal zone development in a manner that protected the unique ecology and resources of the coastal zone. States were chosen over local governments because they were thought to be more likely to consider the national interest.[155] Additionally, states' wider geographic jurisdictions were assumed to lend themselves to a more integrated approach, and states were considered not as subject to short-term economic pressures.[156] At the other end of the spectrum, state authorities were chosen over a federal regulatory scheme because it seemed unlikely that one federal agency could be put together to address the myriad of coastal zone interests and issues.[157] States have traditional authority over zoning and wetlands preservation, and are generally closer to regional problems than the federal government.[158] Unlike other cooperative federalist schemes such as the Clean Air Act and Clean Water Act, there was no threat of federal program management should the states decline to participate. State participation would be voluntary, but the offer of federal consistency, in addition to federal funding, was intended to be a carrot to bring states into the Act's plan.[159] Of the two, however, consistency was felt to be the heart of the Act.[160]

Architects of state coastal zone management plans (CZMPs) are not unbounded in how consistency will impact federal agencies. CZMPs must be approved by the Secretary of Commerce, and it is in this approval process that the federal government theoretically has the opportunity to limit the reach of state plans.[161] In preparing their CZMPs, states must demonstrate to the Secretary that they have given adequate consideration to national interests.[162] Problems and potential conflicts between state and federal agencies are

---

[153] *See* Tim Eichenberg & Jack Archer, *The Federal Consistency Doctrine: Coastal Zone Management and "New Federalism,"* 14 ECOLOGY L.Q. 9, 11 (1987)[hereinafter Eichenberg and Archer].
[154] *See Id.* at 13.
[155] *See* Jeffrey L Beyle, Note, *A Comparison of the Federal Consistency Doctrine Under FLPMA and the CZMA*, 9 VA. ENVTL. L.J. 207, 207-08 (1989)[hereinafter Beyle].
[156] *See* Beyle, *supra* note 155 at 208; *see also* Rychlak, *supra* note 7, at 1004.
[157] *See* Beyle, *supra* note 155, at 208.
[158] *See Id.*
[159] *See* Eichenberg & Archer, *supra* note 153, at 14.
[160] *See* Major Richard M. Lattimer, Jr.,USMC, *Myopic Federalism: the Public Trust Doctrine and Regulation of Military Activities*, 150 MIL. L. REV. 79, 123 (1995)[hereinafter Lattimer].
[161] *See* Beyle, *supra* note 155, at 211.
[162] *See Id.* at 212.

expected to be ironed out during the drafting and approval stages.[163] Thus, provisions with which agencies will have difficulty conforming should be negotiated and modified prior to approval and implementation; the resulting CZMP is assumed to provide adequate protection of national interests.[164] State authority should be further inhibited in that, at least with respect to federal agency actions, the agency itself makes the initial consistency determination.[165] Finally, if a state's CZMP limits an agency's activity to the detriment of a paramount national interest, the President may exempt the agency action from consistency.[166]

In bifurcating the consistency requirement between federal agency activities and federally-licensed or permitted activities, Congress created two levels of consistency activity.[167] In the case of federal agency activity, federal lands are specifically excluded from the state coastal zone and the state CZMP.[168] Nevertheless, activities which "directly affect" the coastal zone must be consistent with the state CZMP to "the maximum extent practicable."[169] "Directly affecting" is an expansion of state authority from the earlier "in the coastal zone" language of the 1972 Act which Congress amended to address *Secretary of the Interior v. California*.[170] "To the maximum extent practicable" is intended to ensure a high level of compliance while still allowing for unforeseen changes in circumstance.[171] The fact that activity takes place on federal lands limits the state's ability to interfere directly with the activity but does not exempt it from a consistency determination.[172] It is intended to impact only those activities which the federal agency has undertaken within its discretion, i.e. activities it is not otherwise required to undertake.[173]

---

[163] *See* Eichenberg & Archer, *supra* note 153, at 24.
[164] *See Id.* at 57.
[165] *See* Lattimer, *supra* note 160, at 137.
[166] *See* J. Christopher Martin, Comment, *The Use of the CZMA Consistency Provisions to Preserve and Restore the Coastal Zone in Louisiana*, 5 LA. L. REV. 1087, 1103 (1991)[hereinafter Martin].
[167] *See* Martin, *supra* note 166 at 1093; *see also* Eichenberg & Archer, *supra* note 153, at 14; Beyle, *supra* note 155, at 209-10.
[168] *See* 16 U.S.C.A. § 1456(e) (West 2001).
[169] *Id*. at § 1456 (West 2001).
[170] *See* 464 U.S. 312 (1984)(holding that the sale of oil and gas leases on the Outer Continental Shelf did not directly affect the coastal zone); *see also* Eichenberg & Archer, *supra* note 153, at 16-17.
[171] *See* Beyle, *supra* note 155, at 210 (quoting 16 U.S.C.A. § 1456(c)(1) (West 2001)).
[172] *See* Eichenberg & Archer, *supra* note 153, at 58.
[173] *See* Martin J. LaLonde, *Allocating the Burden of Proof to Effectuate the Preservation and Federalism Goals of the Coastal Zone Management Act*, 92 MICH. L. REV. 438, 455 (1993)[hereinafter LaLonde].

In the arena of federally-licensed or permitted activities, states have more direct power. The person or organization petitioning for a permit or license must attach a certification to the application stating that the activity is consistent with the state CZMP.[174] It must submit a copy to the state as well for its review,[175] and the burden is on the applicant to prove that its proposed activity is consistent.[176] Within the prescribed time for action, the state may object to the activity and prevent it.[177] This effectively results in state veto power over activity that would otherwise be federally controlled.[178] States are limited in this respect only as to matters of overriding national interest.[179] In *California Coastal Comm'n v. Granite Rock Co.*, the Supreme Court decided the question of whether the federal lands exemption pre-empted state regulatory authority over private activities conducted on federal land.[180] Granite Rock was a mining company with a permit to mine federal land.[181] They sued on the theory that mining federal land should be exempt from state regulation under the federal lands exclusion of § 1456(c)(3).[182] The Court disagreed, citing the Senate Report: "There is no attempt to diminish state authority through federal preemption. The intent of this legislation is to enhance state authority by encouraging and assisting the states to assume planning and regulatory powers over their coastal zones."[183] State regulations not in conflict with the operation or objectives of federal law are consequently not categorically pre-empted by the CZMA.[184]

While consistency gives states veto over federal and federally-licensed activity, Congress has provided no automatic exemptions for defense-related activities under the CZMA.[185] States are required to consider the national interest, but are under no affirmative obligation to accord their plans with it.[186] Without aligning their plans with the national interest, states are free to consider federal concerns nominally and then try to force federal actions to conform to state priorities. "By according states important participating roles, by providing them with procedural protections, and by providing for judicial

---

[174] *See* 16 U.S.C.A. § 1456 (West 2001).
[175] *See Id.*
[176] *See* Martin, *supra* note 166, at 1102.
[177] *See* 16 U.S.C.A. § 1456 (West 2001).
[178] *See* Beyle, *supra* note 155, at 211; Martin, *supra* note 166, at 1091.
[179] *See* Kuersteiner & Sullivan, *supra* note 14, at 49.
[180] 480 U.S. 572, 575 (1987).
[181] *See Granite Rock Co.*, 480 U.S. at 576.
[182] *See Id.* at 589-90.
[183] *See Id.* at 592 (quoting S.Rep. No. 92-753 at 1 U.S.C.C.A.N. 4776 (1972)).
[184] *See Granite Rock Co.*, 480 U.S. at 593.
[185] *See* Eichenberg & Archer, *supra* note 153, at 58 (quoting S. Pac. Transp. Co. v. Cal. Coastal Comm'n., 520 F. Supp 800, 802 (N.D. Cal. 1981)).
[186] *See* Kuerstein & Sullivan, *supra* note 14, at 48.

review, the state's political and bargaining powers were strengthened considerably . . . ."[187] States may therefore influence defense agencies' behavior in the coastal zone through threat of delay and litigation.[188] These obstructions would result in unanticipated expenditures or compromise of mission requirements and performance standards.[189] Should the states incorporate land use practices such as state public trust doctrine in the CZMPs, defense agencies would be subject to state public trust law in their development activity.[190] Subjecting defense agencies to state public trust law, or any state land use regime, forecloses opportunities and restricts the choices available to the agencies in pursuing their missions.[191] One commentator has noted that North Carolina and California incorporate their public trust doctrines in their CZMPs, using language sufficiently vague as to allow those states to interfere with military live-fire training in the coastal zone.[192] The result is that in fields subject to agency discretion, the states may limit the exercise of that discretion.[193]

In the event that a state determination is adverse to the national interest, appeal to the Secretary of Commerce is an option open to the agency. The Secretary has the discretion to override a state's consistency veto of a permit application either because the proposed activity is consistent with the purposes of the Act, or because the activity is in the national interest.[194] Should the activity "directly support" defense or other essential national security activities, the state's consistency objection may be overridden.[195] Based on appeals submitted to the Secretary through 1987, however, the Secretary appears to avoid making decisions on substantive grounds where a political or procedural solution was available.[196] Where alternative development scenarios are available, override was significantly less likely; no overrides for national security reasons were granted.[197] Curiously, the national security overrides which have been pursued have come not from the Defense Department, but from the Departments of Interior and Energy in their efforts

---

[187] Edward L. Strohbehn, Jr. *The Basis for Federal/State Relationships in Environmental Law*, 12 ENVTL L. REP. 15074 (1982)[hereinafter Strohbehn].
[188] *See* Kuerstein & Sullivan, *supra* note 14, at 40.
[189] *See Id*. at 41.
[190] *See* Lattimer, *supra* note 160, at 134.
[191] *See Id*. at 135.
[192] *See Id*. at 136.
[193] *See* Kuerstein & Sullivan, *supra* note 14, at 55.
[194] *See* Eichenberg & Archer, *supra* note 153, at 15.
[195] *See Id*. at 34.
[196] *See Id*. at 41.
[197] *See Id*.

to shelter Outer Continental Shelf development under the umbrella of energy self-sufficiency and the enhancement of strategic energy reserves.[198]

Unlike licensed activities, federal agencies are not required to seek state approval, and are not bound to defer should states object to their activities in the coastal zone. Instead of appealing to the Secretary, states are likely in this event to turn to the judiciary, the other option available. The threshold inquiry for the court in such a case is whether the activity "directly affects;" if not the case ends there.[199] Courts are reluctant to allow national security concerns as a government defense because of the statutory mechanism available to address those concerns, which they tend to view as the only legitimate means of protecting national security interests.[200] Courts therefore interpret state consistency influence liberally, assuming that federal-state conflicts are smoothed over during the approval process.[201]

When states take court action against federal agency activities directly affecting the coastal zone, the agency may similarly pursue a Presidential override of the consistency requirement if the override is in the "paramount interest" of the United States.[202] Presidential exceptions to environmental laws are rare, however.[203] Additionally, politics and policies of local accommodation make it difficult for military leaders to advance their arguments effectively in favor of their proposed activity.[204] The paramount interest exception is thus unlikely because of the visibility and political considerations of any such decision.[205] As a former NOAA General Counsel has noted:

> [E]very effort . . . must be made to reach an accommodation, but in the final analysis, if the issue cannot be resolved, the state decision will prevail -- a significant provision from the standpoint of the states. Lack of accommodation would not appear

---

[198] *See Id.* at 45.
[199] *See Id.* at 47.
[200] *See* Melinda R. Kassen, *The Inadequacies of Congressional Attempts to Legislate Federal Facility Compliance with Environmental Requirements*, 54 MD. L. REV. 1475, 1479 (1995)[hereinafter Kassen].
[201] *See* Kuersteiner & Sullivan, *supra* note 14, at 51-52.
[202] *See* 16 U.S.C.A. §1456(c) (West 2001).
[203] *See* Kassen, *supra* note 200, at 1479.
[204] *See* Lattimer, *supra* note 160, at 151.
[205] *See Id.* at 123.

> to be adequate ground for refusal by the Secretary to grant . . . approval.[206]

Even when the judiciary or the executive has acted to support activities in the coastal zone against state claims, Congress has adjusted the balance back in favor of the states, as in the 1990 amendments to the Act.[207] In 1984, the Supreme Court ruled that Outer Continental Shelf oil and gas leases sold by the Department of the Interior did not "directly affect" the coastal zone because the federal lands exclusion[208] extended to Outer Continental Shelf submerged lands.[209] Writing for the Court, Justice O'Connor held that,

> [a] broader reading of [the CZMA] is not compelled by the thrust of other CZMA provisions. . . . [I]t is clear beyond peradventure that Congress believed that CZMA's purposes could be adequately effectuated without reaching federal activities conducted outside the coastal zone. Both the Senate and House bills were originally drafted, debated, and passed, with [the CZMA] expressly limited to federal activities in the coastal zone. Broad arguments about CZMA's structure, the Act's incentives for the development of state programs, and the Act's general aspirations for state-federal cooperation thus cannot support the expansive reading . . . urged by respondents.[210]

Congress moved to overturn *Secretary of the Interior* in the 1990 Reauthorization of the CZMA.[211] The new provision reads:

> Each Federal agency activity *within or outside the coastal zone that affects any land or water use or natural resource of* the coastal zone shall *be carried out* in a

---

[206] *See* Brewer, *supra* note 11, at 317.
[207] *See* Lattimer, *supra* note 160, at 150; 16 U.S.C.A. § 1456 (West 2001). *Compare* Secretary of the Interior v. California, 464 U.S 312 (1984).
[208] *See* 16 U.S.C.A. § 1453(1) (West 2001).
[209] *See* Secretary of the Interior v. California, 464 U.S. 312 (1984).
[210] *See* Secretary of the Interior v. California, 464 U.S. 312, 331 (1984).
[211] *See* Godschalk, *supra* note 38, at 110.

> manner which is consistent to the maximum extent practicable *with the enforceable policies of approved State management programs*. . . .[212]

An examination of the legislative materials related to the passing of the 1990 Reauthorization supports this hypothesis.[213] The Report of the House Committee on Merchant Marine and Fisheries noted that "[a]s CZM programs have matured, and competition for coastal resources has increased, the federal consistency requirements have grown in significance as a management tool."[214] The Report described the "problem areas"[215] in federal consistency that the amendment was intended to remedy: "Since [*Secretary of the Interior*], other federal agencies have broadly interpreted the case in a manner that would exclude their activities from undergoing a federal consistency review."[216] The Report supported the states' assertion that "they are granted the authority, through the federal Coastal Zone Management Act, to implement coastal management requirements and that *these requirements are binding on all federal agencies*."[217]

The Report of the Senate Committee on Commerce, Science, and Transportation[218] accorded with the House Report:

> The [proposed amendment] strengthens the Federal consistency provisions of the CZMA by reversing the 1984 Supreme Court decision, *Secretary of the Interior v. California*. . . . The [amendment] would clarify that *all Federal agency activities* . . . within or outside the coastal zone must be consistent to the maximum extent practicable with federally approved State management programs if such activity

---

[212] 16 U.S.C.A. § 1456(c)(1)(A) (West 2001)(as amended by Pub. L. 101-508, § 6208(a))(emphasis added to highlight substituted language).
[213] *See* H.R. REP. NO. 101-535 (1990); S. REP. NO. 101-445 (1990); H.R. CONF. REP. NO. 101-964 (1990), *reprinted in* 1990 U.S.C.C.A.N. 2673-80; 136 CONG. REC. 26030-67 (1990).
[214] *See* H.R. REP. NO. 101-535, at 13.
[215] *See Id.*
[216] *See Id.*
[217] *See* H.R. REP. NO. 101-535, at 13 (emphasis added).
[218] *See* S. REP. NO. 101-445 (1990).

> affects, or will lead to effects on, the coastal zone.[219]

The responsible Committees of both the House and Senate, then, clearly intended that all federal agency activities that may have some effect on the coastal zone are subject to consistency determinations. No mention was made of national security or defense agency actions in the Reports, leaving the door open to state frustration of such activity executed in accordance with the agencies' missions.

When the debate moved to the floor of the House, the Congressional intention to include all federal agencies was made even more clear.[220] One Member commented that the Amendment intended to clarify that the relevant factor in consistency determinations would not be the location of agency activity, but on the effect, including reasonably foreseeable indirect affects.[221] The chair of the Merchant Marine and Fisheries Committee added that the Committee's intent was that "the effects test should be broadly construed to include the direct and indirect effects of a Federal activity."[222] While some Representatives cautioned of the Amendment's potential impact on federalism concerns such as national security and interstate commerce,[223] those concerns were dismissed with a quick reference to the national security exemption: "[the national security exemption] allows the President to override a State's objection to a Federal agency activity . . . ."[224] The debate overlooked the protests of a small minority, as the House focused mainly on the effects of other federal activities, particularly ocean dumping and the sale of oil and gas leases.[225] The House indisputably intended to subject any Federal activity that could conceivably affect the coastal zone to the possibility of a state consistency objection,[226] on the belief that "Federal agencies should be required

---

[219] *See Id.* at 6 (emphasis added).
[220] *See generally*, 136 Cong. Rec., *supra* note 213.
[221] *See Id.* at 26043 (statement of Mr. Paneta).
[222] *See Id.* (statement of Mr. Jones).
[223] *See* 136 Cong. Rec, *supra* note 213, at 26046 (statement of Mr. Shumway)("the [amendment] expands the so-called consistency provision so that a whole host of Federal activities will now be covered . . . . I would suggest to the Members that [the amendment] . . . skews . . . the Federal-State balance . . . ."), 26049 (statement of Mr. Strangeland)("[i]n particular situations . . . overriding Federal interests, such as national security and interstate commerce, argue for a balanced sharing of authority among jurisdictions . . . . [I]f we give broad deference to State coastal agencies, we must be sure not to unduly restrict [sic] the Federal . . . programs.").
[224] *See generally*, 136 Cong. Rec., *supra* note 213, at 26044 (statement of Mr. Paneta).
[225] *See generally*, *Id* . at 26043 (statement of Mr. Paneta); 26046 (statement of Mr. Shumway); 26049 (statement of Mr. Strangeland); 26063 (statement of Mr. Goss).
[226] *See Id.* at 26044 (statement of Mr. Hertel).

to tailor their activities to mesh as much as possible with State efforts to protect the coast."[227]

The House Conference Report detailed the results of the Senate and House's compromise on the amendment.[228] With regard to the consistency requirement, the Report states:

> The amended provision establishes a generally applicable rule of law that *any* federal agency activity (regardless of its location) is subject to the CZMA requirement for consistency if it will affect any natural resources, land use, or water uses of the coastal zone. No federal agency activities are categorically exempt from this requirement.
>
> Whether a specific federal agency activity will be subject to the consistency requirement is a determination of fact based on an assessment of whether the activity affects natural resources, land uses, or water uses in the coastal zone of a state with an approved management program. This must be decided on a case-by-case basis by the federal agency conducting the activity.[229]

The report goes on to direct that "the term 'affecting' is to be construed broadly."[230] As for the Presidential exemption in the event of a paramount interest of the United States, "[t]he exemption authorized . . . is not applicable to a class of federal agency activities but only to a specific activity."[231] Congress was united, then, in its intent to expand state power in the coastal zone, potentially at the expense of federal defense interests.

Some commentators believe that the balance in favor of state authority that Congress seems to strike should be pursued to further the states'

---

[227] *Id.* at 26046 (statement of Mr. Studds).
[228] *See* H.R. CONF. REP. NO. 101-964 (1990), *reprinted in* 1990 U.S.C.C.A.N. 2673-80.
[229] *See* H.R. CONF. REP. NO. 101-964 (1990)), *reprinted in* 1990 U.S.C.C.A.N. at 2675.
[230] *See Id.*
[231] *See Id.* at 2676.

interests.[232] One notes that the CZMA requires states to balance the costs and benefits of coastal protection with the costs and benefits of development.[233] This balancing will require conceptual value judgments difficult to quantify.[234] The resulting variety, however, does not undermine Congress' expectation that each state strike its own balance.[235] The resulting coastal management plans encode state cost considerations, and the consistency requirement forces federal agencies to consider the cost of their activity on the locality where it takes place.[236] Another commentator goes beyond this cost-internalization analysis to argue that states should act to force positive effects from federal agencies, and not mere non-damage.[237] Initial state action should always take a hard line, so that future actions with regard to the proposed activity are not estopped.[238] Since the burden of proving consistency is on the federal agency, states should set the consistency bar high in order to force benefits, and then pursue litigation if unsatisfied.[239] California and Delaware already pursue such a hold-out strategy.[240]

With respect, then, to federal-state interaction regarding issues of national concern, the Coastal Zone Management Act potentially turns federalism on its head, giving the states influence over federal action, if not an outright veto, that the federal system was intended to prevent. The consistency provision of the CZMA give states leverage to hold out in granting their consent in order to force concessions from federal agencies carrying out their missions in the coastal zone. Some commentators even advocate this type of strategic behavior in an effort to wring benefits from the federal government which might not otherwise accrue to the state.[241] How that strategic behavior impacts perhaps the most crucial of federal activities, providing for the common defense, is examined in the next section.

IV. Illustrative Cases

---

[232] *See* Martin, *supra* note, 166 at 1099; *see generally* Kassen, *supra* note 200; LaLonde, *supra* note 173.
[233] *See* LaLonde, *supra* note 173, at 471.
[234] *See Id.*
[235] *See Id.* at 472.
[236] *See Id.*
[237] *See* Martin, *supra* note 166, at 1099.
[238] *See Id.* at 1098.
[239] *See* Martin, *supra* note 166, at 1102.
[240] *See Id.* at 1100.
[241] *See generally Id.* at 1100; Kassen, *supra* note 200.

The national security concerns of defense agencies have fortunately rarely come into conflict with states' coastal management regimes thus far.[242] The Navy has been the only service forced to defend consistency determinations in court, and the results have reflected the Federalists' concern for local veto over actions that are national in their importance. This section examines those three controversies in detail. The litigation was expensive for the nation, both in terms of actual litigation costs, and in the impact the ensuing delays had on the projects.

A. Friends of Earth v. United States Navy

In 1988, the Ninth Circuit heard an appeal of a denied motion to enjoin the Navy's construction project to support homeporting a *Nimitz*-class aircraft carrier in Everett, Washington in a dispute over the state dredging permitting requirement.[243] The Navy had planned to dredge 3.4 million cubic yards of material, one third of which was contaminated with heavy metals and organic compounds, in order to build the base it required for the homeporting plan.[244] The Navy proposed to dispose of the spoils using a method designed to prevent damage from the contaminants. But the efficacy of the method was unproven at the depths the spoils would be placed.[245] In March, 1987, the Navy applied to the city of Everett for a state permit to conduct the dredging under Washington's statutory coastal zone management plan, the Shoreline Management Act (SMA).[246] Everett approved the permit in June, 1987, and the Washington Department of Ecology reviewed and approved the permit in July, 1987.[247] In July, 1987, Friends of Earth and other groups requested a review of the approval in accordance with SMA provisions.[248] Under the SMA, permitted activities may not be commenced until the conclusion of all

---

[242] Communication with attorneys at the Offices of General Counsel of NOAA, the U.S. Coast Guard and the Department of the Navy reveals that no defense agency has ever invoked the national security exception of the CZMA. The three cases below are the only actions against a defense agency over a consistency dispute. *See* electronic mail message from David Kaiser, Federal Consistency Coordinator, NOAA, Office of Ocean and Coastal Resource Management, to author, 1 (Oct. 19, 1999)(on file with author); electronic mail message from Ron Borro, Department of the Navy Office of General Counsel, Installations & Environment, to author, 1 (Oct. 27, 1999); electronic mail message from MAJ Craig D. Jensen, USMC, Assoc. Counsel for the Commandant, Environment and Land Use, to author, 1 (Nov. 2, 1999)(on file with author); telephone interview with Thomas M. Hayes, Office of Chief Counsel, Environmental Law, U.S. Coast Guard (Oct. 25, 1999).

[243] *See* Friends of Earth v. United States Navy, 841 F. 2d 927, 928- 30. (9th Cir.1988).

[244] *See Id.* at 929.

[245] *Friends of Earth*, 841 F.2d at 929.

[246] *See Id.* at 930 (citing WASH. REV. CODE §§ 90.58.010-.930 (West Supp. 1987)).

[247] *See* Friends of Earth v. United States Navy, 841 F.2d 927, 928-30 (9th Cir. 1988)(citing WASH. REV. CODE § 90.58.140(12)).

[248] *See Id.* (citing WASH. REV. CODE § 90.58.140(5)).

reviews initiated within thirty days of application approval by state authorities.[249] By September, 1987, the Navy had accepted bids for the dredge work and awarded the contract.[250] The contract specified that no "in-water" work would begin until July, 1988, providing sufficient time for the conduct of Friends of Earth's review.[251] The dispute centered around the definition of "in-water" in the contract; the Navy wanted to begin excavation work on land that was occasionally submerged at high tide.[252]

The trial court refused to grant the injunction, agreeing with the Navy that the land was exempt from the SMA because it was on federal land and beyond Washington's reach.[253] The Navy argued that SMA is a land use law, not an environmental law, and that it was merely required to satisfy the requirements of the Clean Water Act in carrying out its activities.[254] Consequently, SMA did not address the activity Navy wished to conduct while awaiting the Friends of Earth review, and Navy would be free to proceed. The Ninth Circuit disagreed, contending that SMA is a mixed land use and environmental protection statute.[255] As such, the dredging and water quality regulations of the permit applied to the Navy project regardless of whether the activity was conducted on federal or non-federal land.[256] As a result, the court enjoined the Navy from any further activity until after completion of the review process.[257]

The court relied in part on *Cal. Coastal Comm'n. v. Granite Rock*[258] in reaching its decision.[259] In that case, involving an attempt by a mining company licensed to excavate federally-owned land to resist being subject to the California Coastal Commission's regulations, the Supreme Court held that the Coastal Zone Management Act does not pre-empt state permitting requirements or diminish state environmental regulatory authority on federal land.[260] Relying on the Congressional record and the federal regulations governing mineral exploration on federal land, the Court stated that as long as the Commission's permitting requirements were not in direct conflict with

---

[249] *See Id.* (citing WASH. REV. CODE § 90.58.180).
[250] *See Id.*
[251] *See Id.*
[252] *See Id.*
[253] *See Friends of Earth*, 841 F.2d at 930-31.
[254] *See Id.* at 935.
[255] *See Friends of Earth*, 841 F.2d at 935 (citing Cal. Coastal Comm'n. v. Granite Rock, 480 U.S. 572 (1987)).
[256] *See Friends of Earth*, 841 F.2d at 935.
[257] *See Id.* at 937.
[258] 480 U.S. 572 (1987).
[259] *See Friends of Earth*, 841 F.2d at 936.
[260] *See Granite Rock*, 480 U.S. at 592.

federal regulations, Granite Rock was subject to state regulation.[261] Since the permit required by the Commission was for environmental protection and not land use, the exemption of federal land from CMZP regimes did not apply.[262] The Ninth Circuit took the *Granite Rock* decision a step further, by applying the Court's distinction of environmental versus land use regulation to federal activity instead of a federally-permitted activity. Under *Friends of Earth*, any activity on federal land is subject to state environmental controls even if the land is covered by the CZMA's federal lands exemption.

The goals of the CZMA appeared to have been met in this case. Federal, state, and local governments had reviewed and approved the planned activity. The project was planned deliberately, after considering the ecological impact of the project on Everett's shoreline. Nevertheless, a local activist group successfully delayed the project, incurring additional costs, which were borne by the nation. In this instance, the CZMA's consistency requirement functioned to allow an interest group opposed to defense-related activity to obstruct a federal project that had passed the consistency test.

B. Cal. Coastal Comm'n v. United States

In the mid-1990s, The Navy planned to move a *Nimitz*-class aircraft carrier to San Diego in order to balance the allocation of forces between the Atlantic and Pacific Fleets following the decommissioning of three carriers and the Base Realignment and Closure (BRAC) decisions.[263] In 1995, the Navy submitted a consistency determination to the California Coastal Commission with regard to its plan to deepen the channel into San Diego as part of the carrier's relocation to Naval Air Station North Island on the Coronado peninsula.[264] The proposed dredging would deepen the channel to allow a fully-loaded aircraft carrier to transit in and out of the harbor without waiting for high tide.[265] The 7.9 million cubic yards of sand from the dredging were to be used for beach nourishment in accordance with California's coastal management plan, and the remaining 2 million cubic yards would be dumped at an approved Army Corps of Engineers' site four and a half miles off Point Loma.[266] The California Coastal Management Plan calls for all appropriate

---

[261] *See Id.* at 594.
[262] *See Id.* at 587-88.
[263] *See* Defs' Mem. of P. & A. in Opp'n to Pls.' Mot. for Prelim. Inj., 3 [hereinafter Defs' Mem.].
[264] *See* Cal. Coastal Comm'n. v. United States, 5 F. Supp. 2d 1106, 1108 (S.D. Cal. 1998).
[265] *See* Defs' Mem., *supra* note 263, at 3.
[266] *See Id.*

spoils to be used for beach nourishment.[267] At the time of the proposal and review, there was no record of munitions being present in the sand the Navy intended to dredge based on past excavation of the channel and extensive bottom-material testing in preparation of the proposal.[268] The channel was to be prepared in time for the carrier to relocate in August, 1998.[269] The Commission approved the plan in November, 1995, and in September, 1997 the Navy began dredging operations.[270] In the course of dredging operations, munitions of various sizes and ages were found in the spoils.[271] In October, the Navy requested the Commission to approve modifications to the plan to permit 2.5 million cubic yards intended for beach replenishment to be dumped instead at the Corps of Engineers' site, citing the risk to public safety posed by the discovered ammunition.[272] While considering its options, the Navy commissioned a consultant to study alternatives to the ocean dumping scheme.[273] The resulting "Harris Report" was the basis of the Commission's argument that alternatives to dumping the spoils at sea had been insufficiently explored.[274] The Navy contended that straining the sand so as to ensure that no munitions were inadvertently placed on the beach would be prohibitively expensive and would delay the project.[275] In its brief opposing a motion for preliminary injunction, the Navy contended that it had attempted to continue negotiations to work out a plan that would satisfy the needs and concerns of both sides, and that dumping all the material at sea was the worst-case scenario.[276] Based on the ammunition found, the Corps of Engineers issued a new dredging permit in October, 1997, which mandated the at-sea dumping of all spoils from the ammunition-contaminated site.[277] The Navy in the same month submitted a new consistency determination to the Commission, outlining a plan to dump all remaining spoils from the project at sea, and using instead sand from another inner harbor dredge project for beach replenishment.[278] The unexplored alternatives cited in the Harris Report were the basis of the Commission's claim that the operation was not consistent "to the maximum extent practical."[279] Despite the Commission's protests, the

---

[267] *See* Pls' Mem. of P. & A. in Supp. of Mot. for Prelim. Inj., 15[hereinafter Pls. Mem.] (citing CAL. PUB. RES. CODE § 30233(b)); *see also* Defs' Mem., *supra* note 263, at 8.
[268] *See* Defs' Mem., *supra* note 263, at 4.
[269] *See Id.* at 1.
[270] *See* Defs' Mem., *supra* note 263, at 9.
[271] *See Id.* at 10-11.
[272] *See Id* at 12.
[273] *See* Defs' Mem., *supra* note 263, at 12.
[274] *See* Cal. Coastal Comm'n. v. United States, 5 F. Supp. 2d 1106, 1109 (1998).
[275] *See Id.*
[276] *See* Defs' Mem., supra note 263, at 12.
[277] *See Id.* at 15.
[278] *See Cal. Coastal Comm'n.*, 5 F. Supp. 2d at 1109.
[279] *See Id.* at 1109.

Navy indicated that it would proceed without concurrence, citing the mounting expense of delay and the pressing need to prepare the channel for the carrier's arrival.[280] In December, 1997, the Commission met with Navy representatives, including Assistant Secretary of the Navy Robert Pirie, and two San Diego area congressmen, Congressman Ron Packard and Congressman Duke Cunningham.[281] At that meeting, Congressman Packard, Chair of the House Military Construction Subcommittee, offered to reprogram the Navy's appropriation to pay for the more expensive beach replenishment with cleaned sand.[282]

The Commission initiated action to prevent the Navy from not replenishing the beaches, and sought a preliminary injunction.[283] The Commission's motion alleged three reasons for the injunction: not depositing the spoils would damage property owners and the public by not repairing beach erosion; the California Coastal Commission (CCC) would be injured by its inability to enforce the California Coastal Management Plan; and alternatives to dumping the spoils at sea available to the Navy had not been fully explored.[284] Continued beach erosion would limit the public's ability to use the beaches, lower property values along the beach, and potentially risk public safety because of wave action.[285] The CCC argued that Congress had entrusted to it in the CZMA the authority to ensure that federal agencies complied with state environmental law.[286] In response to the Navy's contention that alternative plans were fiscally impossible to undertake, the CCC asserted that inadequate funding was not an excuse for non-compliance with the CCMP.[287]

The Navy countered that state agreement or disagreement with a federal consistency determination was not the test of whether an agency had complied to the maximum extent practicable.[288] The CCMP no longer applied, because: (1) the munitions-contaminated spoils were unusable for beach nourishment; (2) the new dredging permit prevented using the spoils as beach material, and demonstrated the Corps of Engineers' concurrence with the Navy's opinion; and (3) finding the ordnance was an unforeseeable event

---

[280] *See Id*; *see also* Defs' Mem., *supra* note 263, at 14.
[281] *See* Pls' Mem., *supra* note 267, at 8.
[282] *See Id.* at 9.
[283] *See Id.*
[284] *See* Pls' Mem., *supra* note 267, at 2.
[285] *See Id.* at 16.
[286] *See Id.* at 12.
[287] *See Id.* at 9, 19.
[288] *See* Defs' Mem., *supra* note 263, at 20.

allowing deviation from the plan with which the Commission had concurred.[289] The Navy pointed out that it had proposed a reasonable, feasible alternative in using spoils from another, uncontaminated section of dredging for beach nourishment.[290] Additionally, the Navy argued that to grant the injunction would imperil national security by restricting carrier operations to coincide with high tide and forcing refueling at sea rather pierside, a safer alternative.[291]

The court disagreed, citing *Friends of Earth v. United States Navy*[292] as controlling precedent for the Ninth Circuit that Congressional intent under the Act is given greater weight than traditional deference to the reasonableness agency action.[293] The court reasoned that the injunction was only for the period required for the California Coastal Commission to evaluate the feasibility of other dredging alternatives, and that national security would not be damaged.[294] The court pointed out that aircraft carriers had negotiated the transit into and out of San Diego for some time without benefit of the deeper channel.[295]

Ultimately the case was settled out of court through a political solution. Congressman Packard reprogrammed the Navy's construction budget as he had promised, providing enough money to carry out the more expensive spoils cleaning procedure discussed in the Harris Report and to cover the costs incurred by delay.[296] The channel was dredged, the carrier relocated to San Diego, and area beaches were replenished. Using the CZMA consistency provisions, the CCC was able to hold out to force a more expensive solution to the Navy's unexpected dredging difficulty. Despite the availability of other dredge material to replenish San Diego's beaches, the Commission pursued and achieved local gain at national expense.

C. *Barcelo v. Brown* and Vieques Island

In 1978, the government of Puerto Rico and various non-profit Puerto Rican citizens' organizations filed suit against the United States in federal court, alleging violations of many federal and commonwealth environmental

---

[289] *See Cal. Coastal Comm'n.*, 5 F. Supp. 2d at 1109-10.
[290] *See* Defs' Mem., *supra* note 263, at 22.
[291] *Id.*
[292] 841 F.2d 927 (9th Cir. 1988).
[293] *See Cal. Coastal Comm'n.*, 5 F. Supp. 2d at 1111.
[294] *See Cal. Coastal Comm'n.*, 5 F. Supp. 2d at 1112.
[295] *See Id.*
[296] *See* electronic mail from Ron Borro, Department of the Navy Office of General Counsel, Installations & Environment, to author, 1 (Sep. 23, 1999)(on file with author).

laws, including the Coastal Zone Management Act, by the Navy in the operation of its training facility on Vieques Island.[297] Vieques is an island of thirty-three thousand acres located approximately six miles off the southeast coast of Puerto Rico.[298] It became a United States territory along with Puerto Rico following the Spanish-American War.[299] Politically, it is a municipality of Puerto Rico.[300] According to the 1970 census, Vieques had a population of 7,767, of whom 2,998 lived in the island's two towns, and the balance lived in rural areas.[301] In the early 1940s, the island's economy was based primarily on sugar farming, livestock, and fishing.[302] Between 1939 and 1944, the Navy acquired title to twenty-six thousand acres in two sections, which were bisected by the remaining civilian area.[303] The eastern sector had been developed into an airstrip, a Marine Corps garrison, an ammunition depot, and an observation complex.[304] Additionally, the eastern sector contained beaches used for amphibious assault exercises and target areas designated for live-fire (i.e., actually discharged or released ordnance, whether inert or explosive, as opposed to simulated fire) ship-to-shore gunnery and aerial bombardment training.[305] It is one of four firing ranges in the Caribbean sea which make up the Atlantic Fleet Weapons Training Facility.[306] The western sector was used for ammunition storage, administrative offices, a non-firing, small-unit infantry training area, and another amphibious assault beach.[307] The plaintiffs' complaint was based on the use of Vieques for the live-fire and amphibious training exercises.[308]

The plaintiffs alleged *inter alia* that the Navy's activities were inconsistent with Puerto Rico's approved Coastal Zone Management Plan.[309] The Navy defended by arguing that it acted consistently "to the maximum extent practicable."[310] Following a three-month trial,[311] the court held that the plaintiffs' contentions were inappropriate for a variety of reasons,

---

[297] *See* Barcelo v. Brown, 478 F. Supp. 646, 650 (D.P.R. 1979).
[298] *See Id.* at 652.
[299] *See Id.* at 654.
[300] *See Id.* at 652.
[301] *See Id.* at 654.
[302] *See Id.*
[303] *See Barcelo*, 478 F. Supp. 654.
[304] *See Barcelo*, 478 F. Supp. 654.
[305] *See Id.*
[306] *See Id.* at 655.
[307] *See Id.* at 654-55, 709-10.
[308] *See Id.* at 656.
[309] *See Id.* at 680. For Coastal Zone Management Act purposes, Puerto Rico, the Virgin Islands, Guam, the Commonwealth of the Northern Marianas, and the Trust Territories of the Pacific Islands and American Samoa are considered "coastal states." *See* 16 U.S.C.A. § 1453(4) (West 2001).
[310] See *Barcelo*, 478 F. Supp. at 680.

> "[n]ot least of which [was] that the 'CZMA' and the Commonwealth's Plan [were] inapplicable to the Defendant Navy's lands in Vieques. . . ."[312] because "'*[e]xcluded from the coastal zone are lands the use of which is by law subject solely to the discretion of or which is held in trust by the Federal Government, its officers or agents*.'"[313]

The court supported its interpretation of the exclusion of federal lands from the definition of "coastal zone" with the Congressional Record:

> Of particular importance is the definition of "Coastal zone." The coastal zone is meant to include the *non-Federal* coastal waters and the *non-Federal* land beneath the coastal waters, and the adjacent *non-Federal* shore lands including the waters therein and thereunder. . . .All federal agencies conducting or supporting activities in the coastal zone are required to administer their programs consistent with approved state management program[s]. However, *such requirements do not . . . extend state authority* to land subject solely to the discretion of the Federal Government such as national parks, forests and wildlife refuges, Indian reservations and *defense establishments*. . . .[314]

The court found the plaintiffs' complaint to be groundless.[315] In fact, the court opined that the Navy's control of the area was probably ecologically beneficial; the presence of many species not found on civilian parts of the island was *res ipsa loquitor* of the Navy's exemplary stewardship.[316] The court

---

[311] *See Id.* at 652.
[312] *Id.* at 680.
[313] *Id.* at 680-81 (quoting 16 U.S.C.A. § 1453(1)) (West 2001)(emphasis supplied by the court).
[314] *See Barcelo*, 478 F.Supp. at 681 (quoting Senate Rep. No. 92-753, 1972 U.S. Code Cong. and Admin. News, 4783)(emphasis supplied by court).
[315] *See Id.* at 682.
[316] *Id.*

went into significant detail supporting its findings regarding the Navy's ecological impact[317] before ruling that the plaintiffs had failed to state a claim under the CZMA.[318]

Barcelo is thus an instance in which federalism concerns overruled state environmental interests, including the Puerto Rican Coastal Management Plan. In determining the remedy for those allegations the plaintiffs had proven,[319] Judge Torruella wrote:

> Lastly, we have not the slightest doubt but that the granting of the injunctive relief sought would cause grievous, and perhaps irreparable harm, not only to Defendant Navy, but to the general welfare of this Nation. It is abundantly clear from the evidence in the record, as well as by our taking judicial notice of the present state of World affairs, that the training that takes place in Vieques is vital to the defense of the interests of the United States.[320]

The freedom of national defense matters from state influence was thus affirmed in *Barcelo*.

If *Barcelo* were tried today, however, the result would likely not be the same. *Barcelo* was litigated in 1978 and 1979. The relevant consistency provisions of the Coastal Zone Management Act had not yet been amended from their original form: "Each Federal agency conducting or supporting activities directly affecting the coastal zone shall conduct or support those activities in a manner which is, to the maximum extent practicable, consistent with approved state management programs."[321] The new language removes the foundation of Judge Torruella's *Barcelo* opinion by subjecting any federal agency activity directly affecting the coastal zone to the state coastal zone management plan, regardless of the site of the activity. Absent a national security exemption from the Secretary of

---

[317] *See Id.* at 682-88.
[318] *See Id.* at 692.
[319] The Navy was to have violated the Federal Water Pollution Control Act (33 U.S.C. §§ 1251-1376), Executive Order 11,593 (38 Fed. Reg. 34,793), and the National Environmental Policy Act (42 U.S.C.A. § 43325) (West 2001). *See Id.* at 705.
[320] *Barcelo*, 478 F.Supp. at 707.
[321] 16 U.S.C.A. § 1456 (c) (1) (West 2001).

Commerce, Navy Department live-fire training on Vieques Island would be subject to Puerto Rican consistency objections under a plain-language reading of the amended Act.

The courts have not yet had the opportunity to address the expansion of state consistency power over federal lands within the national defense context. The case may present itself in the near future, however, as the Navy's training activities on Vieques Island have again been challenged. On April 19, 1999, a Marine pilot on an evening training mission at the Vieques live-fire range became disoriented as dusk settled, and released his two five-hundred pound bombs on the wrong target.[322] Four people were injured and one, a civilian security guard named David Sanes Rodriguez, was killed as a result.[323] Shortly thereafter, activists trespassed onto the bombing ranges and set up camp to protest the use of the range and Rodriguez's death.[324] Puerto Rican Governor Pedro Rossello appointed a commission to study the issue.[325] The Commission concluded that the Navy's activity had caused "disastrous economic and environmental damage" to the island.[326] As press coverage continued, military officials argued that the Vieques facility was an "'irreplaceable' national asset worth billions of dollars" and the "only site in the Atlantic where the military can stage integrated sea and air training."[327]

> To fully prepare for war, Navy officials . . . said, they need Vieques, the only place where they can count on nearly 200,000 square miles of uncongested air and sea space and some land for target and amphibious assault practice, allowing all battle components to come together in a realistic scenario.[328]

---

[322] *See 4 Hurt in Military Accident*, N.Y. TIMES, Apr. 20, 1999, at A20; *Navy Attributes Fatal Bombing to Mistakes*, N.Y. TIMES, Aug. 3, 1999, at A12; Karl Ross, *Death at Navy Bombing Range Resonates Through Puerto Rico*, WASHINGTON POST, Aug. 19, 1999, at A10.
[323] *See 4 Hurt in Military Accident*; *Death at Navy Bombing Range Resonates Through Puerto Rico*, *supra* note 322.
[324] *See Puerto Ricans Protest Fatal Bomb Accident*, N.Y. TIMES, May 10, 1999, at A16.
[325] See Mireya Navarro, *Uproar Against Navy War Games Unites Puerto Ricans*, N.Y. TIMES, Jul. 10, 1999, at A8.
[326] Mireya Navarro, *Uproar Against Navy War Games Unites Puerto Ricans*, N.Y. TIMES, Jul. 10, 1999, at A8; *see also* Ross, *supra* note 322, at A10.
[327] Ross, *supra* note 322, at A10.
[328] Navarro, *supra* note 326, at A8.

In June, 1999, President Clinton appointed a panel of officials to review Puerto Rico's complaints and alternatives to training there.[329] In October, 1999, it reported that live-fire training should continue in order adequately to prepare Navy and Marine Corps forces, but recommended that an alternate site be found in order to cease training on Vieques within five years.[330] Governor Rossello rejected that recommendation in Senate testimony the day after the panel report's release.[331] Rossello argued that "[t]he bottom line is that the Navy has repeatedly been a shabby steward of the delicate ecology of what was once one of the most uniformly beautiful islands in the Caribbean Sea."[332]

Although no party has initiated legal action as of this writing, "the [Puerto Rican] government is preparing for legal action as a last resort."[333] Should further discussion regarding future uses of Vieques fail,[334] a suit seems almost inevitable. In the event of litigation, CZMA violations are sure to be among the allegations. Although the plaintiffs in *Barcelo* failed to state a claim under the CZMA in their suit, the amended Act would be more helpful in a new suit. The expansion of the consistency provision's reach puts potential plaintiffs in a stronger position to argue that the Navy's activity is inconsistent with Puerto Rico's coastal zone management plan. A plain-language reading of the amended provision, coupled with the legislative history of the amendment, presents a powerful argument that such a suit is exactly what Congress had in mind with the 1990 Reauthorization: an exertion of state power over a federal agency to enforce state policy objectives. National defense activities would thus be subject to state veto in a manner more direct and potentially more harmful than the litigation delays of either *Friends of Earth* or *California Coastal Comm'n*.

V. Recommendations

The Coastal Zone Management Act, in delegating to the states the authority to review federal agency actions, sets up exactly the situation with

---

[329] Elizabeth Becker, *Panel Backs Firing Exercises in Puerto Rico*, N.Y. TIMES, Oct. 19, 1999, at A1.
[330] *See Id.*
[331] Elizabeth Becker, *Puerto Rico Governor Faces Senators Over Firing Range*, N.Y. TIMES, Oct. 20, 1999, at A25.
[332] Elizabeth Becker, *Puerto Rico Governor Faces Senators Over Firing Range*, N.Y. TIMES, Oct. 20, 1999, at A25. The President ultimately did not follow the recommendations of the Navy and the Panel he appointed. *See* Elizabeth Becker, *President Halts Target Practice by Navy on Puerto Rican Island*, N.Y. TIMES, Dec. 4, 1999, at A1.
[333] *See* Navarro, *supra* note 326.
[334] *See* Roberto Suro, *President Intervenes on Vieques*, WASHINGTON POST, Nov. 17, 1999, at A29.

regard to defense activities that concerned the Founders in the Federalist Papers. In order to act in the best interest of the nation as a whole, the Founders intended that with regard to national security, the federal government should be free to act independent of parochial matters. The consistency provisions of the Coastal Zone Management Act undermine that intent and leave the states free, should they structure their plans accordingly, to put their own objectives above those of the nation as a whole, and to require the national government to spend more money, to delay or cease important activities, and potentially to fall short of its obligations in order to further state and local concerns.

Past commentators have proposed solutions to this federal challenge. One early comment suggested that states be required to adopt relevant federal agencies' definitions of "national interest" where those interests demand federal action under the supremacy clause.[335] Unless the agency's views were an arbitrary or capricious abuse of discretion, states would be required to defer to agency definitions.[336] The "adequate consideration" the Act requires would thus be clarified in a manner consistent with federal supremacy.[337] In order to effect the proposal, "activities subject to supremacy" and "relevant federal agency" would have to be sufficiently defined.[338] "Activities subject to supremacy" would obviously include those concerns that are exclusively federal responsibilities, such as defense and navigation.[339] "Relevant federal agency" for purposes of defining the national interest would be the agency responsible for carrying out that interest in the coastal zone.[340] Such an assignment would be made based on common practice or relevant statutory provisions.[341] National defense is one area that would for the most part be clearly assigned to the Defense Department; areas of overlap with other agencies or departments could be resolved within the Executive Branch.[342] Once these two conditions are met, then deference would be shown to the agency's definition of national interest, since the agency is best positioned to define practical limitations on coastal management programs related to its concerns.[343] Not every agency would set the same limits, and even within one agency the bounds would vary; not every defense activity is as vital as every

---

[335] *See* Kuesteiner, et al., *supra* note 19, at 733.
[336] *See Id.*
[337] *See Id.*
[338] *See Id.* at 734.
[339] *See Id.*
[340] *See Id.* at 735.
[341] *See* Kuesteiner, et al., *supra* note 19, at 735.
[342] *See Id.*
[343] *See Id.*

other defense activity.[344] This proposal would not affect already-existing compliance requirements federal agencies currently face, such as those of the Clean Water Act, Clean Air Act, or the National Environmental Policy Act.[345] By affording the agency affected the opportunity to carve out a reasonable area of traditional federal supremacy free of state veto, the national interest in that area would be protected from the sway of local and state self-interest.

Another commentator has suggested a form of condemnation to create "defense areas" in the coastal zone within which the Armed Forces would be free to train and operate without state interference.[346] Defense agencies would still be subject to the oversight of other federal agencies, and to statutorily-imposed environmental duties, such as those deriving from the National Environmental Policy Act.[347] Because such an action would garner little political support, that commentator suggests the development of a "federal public trust doctrine" as an alternative.[348] The public trust doctrine is a common law concept under which the sovereign owns tidal and riparian lands as a public trustee.[349] Owners of land bordering public trust lands do not hold the entire fee, but own it subject to a dominant servitude held by the sovereign.[350] The sovereign may thus influence or control property uses as part of its responsibility as trustee for the waters and riparian lands regardless of private ownership opposition.[351] Exercise of the doctrine does not constitute an unconstitutional taking because land held in trust for the public is used for the public benefit.[352] A federal public trust doctrine would ensure that government agencies, including the nation's defense organization, would be able to carry out their missions as part of their responsibility to the nation as a whole by affording leaders greater flexibility in making land use decisions.[353] Such a federal doctrine would enhance rather than make irrelevant current environmental law, since courts would be able to force responsible stewardship interstitially on federal agencies as trustees where current regulation falls short of influencing such stewardship.[354] Federal public trust doctrine would overcome the challenge to federalism presented by the consistency determination, because it would provide a fairly simple legal mechanism by

---

[344] *See Id.* at 735-36.
[345] *See Id.* at 737.
[346] *See* Lattimer, *supra* note 160, at 151.
[347] *See Id.*
[348] *See Id.* at 151-64.
[349] *See Id.* at 182.
[350] *See Id.*
[351] *See Id.* at 182-85.
[352] *See* Lattimer, *supra* note 160, at 184.
[353] *See Id.* at 162.
[354] *See Id.* at 158.

which national security agencies could execute their responsibilities in the face of state opposition.

Both articles present interesting and innovative suggestions to resolve the tension between the consistency provisions and the mission requirements of defense agencies. Both would prove difficult if not impossible to implement, however. Subjecting states' plans to a federally-determined definition of national interest would likely face substantial opposition in Congress, particularly in light of Congress's tendency to favor state control in coastal zone issues, as evidenced by the implicit re-affirmation of state control in the 1990 reauthorization and amendment of the Act. The threat of delay and obstruction would not be eliminated, so long as local activist groups and states are still free to challenge the reasonableness of agency definitions in court.

Congressional opposition is but one hurdle obstructing the enactment of a federal public trust approach to restoring the federal balance to coastal zone management. As a common law doctrine, a federal public trust doctrine must result from judicial action. The judiciary, as evidenced by *Friends of Earth* and *Cal. Coastal Comm'n.*, is unlikely to favor increased federal flexibility in adjudicating consistency disputes. Were the judiciary to take the necessary steps to establish firmly a federal public trust doctrine, it would nevertheless be subject to Congressional action. As with all federal common law, Congress would be free to reverse judicial initiatives in later amendments to the Act. Congress has already done so in overturning the result of *Secretary of the Interior v. California.* Given Congress's repeated expression of support for the notion of state control over the coastal zone, it is unlikely that a federal public trust doctrine could be enacted, however appealing the notion may be.

This Article suggests a more modest remedy to the consistency/federalism dilemma. Appendix A is a proposed amendment to the CZMA's consistency provisions to restore the balance of state interests and federal defense concerns in the coastal zone. The provisions in their current form, included for comparison as Appendix B, require all appeals to go to or through the Secretary of Commerce.[355] In the event of a judicial decree against an agency pursuing the paramount interest of the United States, the Secretary may certify the existence of that paramount interest in writing and ask the President to exempt the agency's action from consistency.[356] In the case of defense agencies acting in the paramount interest of national security, a modification of the consistency procedure would streamline the process and restore the federal balance. Rather than submit national security questions to

[355] *See* 16 U.S.C.A. § 1456(c) (West 2001).
[356] *See Id.* at § 1456(c)(1)(B) (West 2001).

the Department of Commerce, consistency conflicts arising from defense agency actions should be submitted to the Secretary of Defense. Appeal to the judiciary would be prohibited in order to prevent the kind of strategic behavior displayed in *Friends of Earth* and *Cal. Coastal Comm'n.* Nonetheless, the Secretary would be subject to the same Congressional reporting requirements that the Secretary of Commerce now bears. Consistency exemption power would be non-delegable. This provision would only apply to agencies of the federal government tasked by law with national security missions. Non-defense agency attempts to claim the national security exemption, such as past appeals by oil and gas interests, would still go to the Secretary of Commerce.

This amendment would have three positive effects. First, by entrusting the consistency override power exclusively to the Secretary of Defense, override actions would be subject to the full force of the political process. State and local governments and public interest groups could still challenge national security actions through their Congressional delegations and by direct appeals to the White House. In this way, the integrity of state management plans would be protected by the high visibility an exemption would carry, guaranteeing that only those actions of the highest national importance be exempt. Second, the added expense of delay and litigation would be eliminated. Once states expressed opposition to a defense agency action, the agency would be free to go up its chain of command to the Secretary. The Secretary would then either grant or not grant the exemption; either way, the parties would have a definitive answer as to where in the hierarchy of national priorities the project fell. Whatever the outcome of the appeal to the Secretary, the decision will have been made by the national political process as the Constitution envisions, rather than through local obstruction and the unpredictability of judicial interpretation. Third, Congressional reporting requirements would provide the process with legislative oversight. Should exemptions become routine or clearly against Congressional determinations of the national interest, the Secretary would be accountable to Congress for consistency exemption decisions. Congressional exercise of the power of the purse, displayed for example in *Cal. Coastal Comm'n.*, provide one avenue to control actions meeting with Congressional disapproval.

The federal imbalance codified by the Coastal Zone Management Act is easily remedied by minor changes to § 1456. By returning control of national security actions in the coastal zone to the Defense Department, federal concerns with local holdouts and state control over defense activities are abated. By subjecting the Secretary's decisions to Congressional review and scrutiny, the protective functions of the Act would still be in place. The

balance between state interests and national defense concerns would be struck by the political branches of the government, guaranteeing that local land use and environmental concerns are addressed within a framework that nevertheless insures that the interests of the whole nation are protected.

APPENDIX A

Proposed Amendment to the Consistency Provision of the Coastal Zone Management Act, 16 U.S.C.A. § 1456(c)

Changes are indicated by the use of italics.

§ 1456 Coordination and cooperation

(c) Consistency of Federal activities with State management programs; Presidential exemption; certification

(1)(A) Each Federal agency activity within or outside the coastal zone that affects any land or water use or natural resource of the coastal zone shall be carried out to the maximum extent practicable with the enforceable policies of approved State management programs. A Federal agency shall be subject to this paragraph unless it is subject to paragraph (2), *(3) or (4).*

(B) [Paragraph (1)(B) addresses appeal provisions for non-Defense Federal agencies. No change is recommended.]

(C) (Paragraph (1)(C) addresses scheduling the consistency certification of non-Defense Federal agencies. No change is recommended.]

(2) [Paragraph (2) requires consistency certification for non-Defense Federal development projects in the coastal zone. No change is recommended.

(3)(A)(i) *Except as provided in paragraph 4(c),* after final approval by the Secretary of a State's management program, any applicant for a required Federal license or permit to conduct activity, in or outside of the coastal zone, affecting any land or water use or natural resource of the coastal zone of that State shall provide in the application to the licensing or permitting agency a certification that the proposed activity complies with the enforceable policies of the State's approved program and that such activity will be conducted in a manner consistent with the program. At the same time, the applicant shall furnish to the State or its designated agency a copy of the certification, with all necessary information and data. Each coastal State shall establish procedures for public notice in the case of all such certifications and, to the extent it deems appropriate, procedures for public hearings in connection therewith. At the earliest practicable time, the State or its designated agency shall notify the Federal agency concerned that the State concurs with or objects to the applicant's certification. If the State or its designated agency fails to furnish the required notification within six months after receipt of its copy of the

applicant's certification, the State's concurrence with the certification shall be conclusively presumed. No license or permit shall be granted by the Federal agency until the State or its designated agency has concurred with the applicant's certification or until, by the State's failure to act, the concurrence is conclusively presumed, unless the Secretary, on his own initiative or upon appeal by the applicant, finds after providing a reasonable opportunity for detailed comments from the Federal agency involved and from the State, that the activity is consistent with the objectives of this chapter or is otherwise necessary in the interest of national security.

(B) [Paragraph (3)(B) addresses consistency certification requirements for exploration or development of, or production from the resources of the Outer Continental Shelf. No change is recommended.]

(4)(A) *Any Department of Defense activity within or outside the coastal zone, including any development project undertaken, that affects any land or water use or natural resource of the coastal zone shall be carried out in a manner which is consistent to the maximum extent practicable with the enforceable policies of approved State management plans. The Defense agency carrying out such activity shall provide a consistency determination to the relevant State agency designated under section 1455(d)(6) of this title and to the Office of the Secretary of Defense at the earliest practicable time, but in no case later than six months before final approval of the Federal activity. Each coastal state shall establish procedures for public notice in the case of all such certifications and, to the extent it deems appropriate, procedures for public hearings in connection therewith. At the earliest practicable time, but in no case later than 90 days before final approval of the Federal activity, the State or its designated agency shall notify the Office of the Secretary of Defense that the State concurs with or objects to the agency's certification. If the State or its designated agency fails to furnish the concurrence or objection 90 days prior to final approval of the Federal activity, the State's concurrence with the certification shall be conclusively presumed. The Secretary of Defense, within six months of the submission of the agency's certification, but not before affording the State the opportunity to concur or object to the certification, shall review the agency's consistency certification and the State concurrence or objection and either agree or disagree with the certification. In reviewing the agency certification and the State concurrence or objection, the Secretary shall weigh the best interests of the Nation, considering the defense interest to be served by the activity, any State interest to be protected, including the ecological, cultural, historic, esthetic and economic values in the coastal zone, and any other relevant factors. Agreement with the certification shall either be conclusive approval with respect to coastal zone concerns to proceed with the*

*activity, or may be qualified subject to agency modification of the planned activity. Disagreement shall be conclusive disapproval of agency activity***.**

(B) *Should the Secretary of Defense agree with the consistency determination despite State objection, appeal may be made to the President. The President may affirm or overrule the Secretary's decision to agree or disagree. In either case, such action will be final.*

(C) *Federally-permitted activities undertaken pursuant to activities approved under this paragraph shall be considered as a part of the parent activity and shall be exempt from the requirements of paragraph 3(A).*

(D) *No federal court shall have jurisdiction to review the decisions of either the Secretary of Defense or the President.*

APPENDIX B

The Consistency Provision of the Coastal Zone Management Act, 16 U.S.C.A. § 1456(c)

§ 1456 Coordination and cooperation

(c) Consistency of Federal activities with State management programs; Presidential exemption; certification

(1)(A) Each Federal agency activity within or outside the coastal zone that affects any land or water use or natural resource of the coastal zone shall be carried out in a manner which is consistent to the maximum extent practicable with the enforceable policies of approved State management programs. A Federal agency activity shall be subject to this paragraph unless it is subject to paragraph (2) or (3).

(B) After any final judgment, decree, or order of any Federal court that is appealable under section 1291 or 1292 of Title 28, or under any other applicable provision of Federal law, that a specific Federal agency activity is not in compliance with subparagraph (A), and certification by the Secretary that mediation under subsection (h) of this section is not likely to result in such compliance, the President may, upon written request from the Secretary, exempt from compliance those elements of the Federal agency activity that are found by the Federal court to be inconsistent with an approved State program, if the President determines that the activity is in the paramount interest of the United States. No such exemption shall be granted on the basis of a lack of appropriations unless the President has specifically requested such appropriations as part of the budgetary process, and the Congress has failed to make available the requested appropriations.

(C) Each Federal agency carrying out an activity subject to paragraph (1) shall provide a consistency determination to the relevant State agency designated under section 1455(d)(6) of this title at the earliest practicable time, but in no case later than 90 days before final approval of the Federal activity unless both the Federal agency and the State agency agree to a different schedule.

(2) Any Federal agency which shall undertake any development project in the coastal zone of a state shall insure that the project is, to the maximum extent practicable, consistent with the enforceable policies of approved state management programs.

(3)(A) After final approval by the Secretary of a State's management program, any applicant for a required Federal license or permit to conduct an activity, in or outside of the coastal zone, affecting any land or water use or natural resource of the coastal zone of that State shall provide in the application to the licensing or permitting agency a certification that the proposed activity complies with the enforceable policies of the State's approved program and that such activity will be conducted in a manner consistent with the program. At the same time, the applicant shall furnish to the State or its designated agency a copy of the certification, with all necessary information and data. Each coastal State shall establish procedures for public notice in the case of all such certifications and, to the extent it deems appropriate, procedures for public hearings in connection therewith. At the earliest practicable time, the State or its designated agency shall notify the Federal agency concerned that the State concurs with or objects to the applicant's certification. If the State or its designated agency fails to furnish the required notification within six months after receipt of its copy of the applicant's certification, the State's concurrence with the certification shall be conclusively presumed. No license or permit shall be granted by the Federal agency until the State or its designated agency has concurred with the applicant's certification or until, by the State's failure to act, the concurrence is conclusively presumed, unless the Secretary, on his own initiative or upon appeal by the applicant, finds after providing a reasonable opportunity for detailed comments from the Federal agency involved and from the State, that the activity is consistent with the objectives of this chapter or is otherwise necessary in the interest of national security.

(B) After the management program of any coastal state has been approved by the Secretary under section 1455 of this title, any person who submits to the Secretary of the Interior any plan for the exploration or development of, or production from, any area which has been leased under the Outer Continental Shelf Lands Act (43 U.S.C. 1331 et seq.) and regulations under such Act shall, with respect to any exploration, development, or production described in such plan and affecting any land or water use or natural resource of the coastal zone of such state, attach to such plan a certification that each activity which is described in detail in such plan complies with the enforceable policies of such state's approved management program and will be carried out in a manner consistent with such program. No Federal official or agency shall grant such person any license or permit for any activity described in detail in such plan until such state or its designated agency receives a copy of such certification and plan, together with any other necessary data and information, and until -

(i) such state or its designated agency, in accordance with the procedures required to be established by such state pursuant to subparagraph (A), concurs with such person's certification and notifies the Secretary and the Secretary of the Interior of such concurrence;

(ii) concurrence by such state with such certification is conclusively presumed as provided for in subparagraph (A), except if such state fails to concur with or object to such certification within three months after receipt of its copy of such certification and supporting information, such state shall provide the Secretary, the appropriate federal agency, and such person with a written statement describing the status of review and the basis for further delay in issuing a final decision, and if such statement is not so provided, concurrence by such state with such certification shall be conclusively presumed; or

(iii) the Secretary finds, pursuant to subparagraph (A), that each activity which is described in detail in such plan is consistent with the objectives of this chapter or is otherwise necessary in the interest of national security. If a state concurs or is conclusively presumed to concur, or if the Secretary makes such a finding, the provisions of subparagraph (A) are not applicable with respect to such person, such state, and any Federal license or permit which is required to conduct any activity affecting land uses or water uses in the coastal zone of such state which is described in detail in the plan to which such concurrence or finding applies. If such state objects to such certification and if the Secretary fails to make a finding under clause (iii) with respect to such certification, or if such person fails substantially to comply with such plan as submitted, such person shall submit an amendment to such plan, or a new plan, to the Secretary of the Interior. With respect to any amendment or new plan submitted to the Secretary of the Interior pursuant to the preceding sentence, the applicable time period for purposes of concurrence by conclusive presumption under subparagraph (A) is 3 months.

A CALL FOR A DEFINITION OF *METHOD 0F WARFARE* IN RELATION TO THE CHEMICAL WEAPONS CONVENTION

Major Ernest Harper, U.S. Marine Corps*

> Somalis continued to mass to the north. In the distance it looked like thousands. Smaller groups would probe south toward Chalk Two's position. One group moved down to just a block away. Maybe fifteen people. Nelson tried to direct his machine gun at only those with weapons, but there were so many people, and those with guns kept stepping from the crowd to take shots, so that he knew he either had to just let the gunmen shoot or lay into the crowd. After a few moments of debate, he chose the latter. That group dispersed, leaving bodies on the street, and another larger one appeared. They seemed to be coming now in swarms from the north, as though chased from somewhere else. They were close in, just forty or fifty feet up the road, some of them shooting. This time Nelson didn't have to weigh the alternatives. He cut loose with the 60 and his rounds tore through the crowd like a scythe. A Little Bird swooped in and threw a flaming wall of lead at it. Those who didn't fall, fled. One minute there was a crowd, the next minute it was just a bleeding heap of dead and injured.[1]

Riot control agents (RCA's) might have been very useful to United States military forces during the fighting in Mogadishu - but they were not

---

* *Major Harper currently serves as SJA, 22nd Marine Expeditionary Unit. Previous duty stations: Graduate Student, The Judge Advocate General's School of the Army; Headquarters, U.S. Marine Corps; Marine Corps Base, Quantico, Virginia; First Battalion, Eleventh Marines*. This article was edited by Major Jon W. Shelburne, USMC.

[1] MARK BOWDEN, BLACK HAWK DOWN 49 (1999).

used. Had they been used, hundreds of noncombatant lives, as well as the lives of United States soldiers might have been spared. Employment of RCA's have proved to be extremely useful in the numerous police actions engaged in by modern militaries, including those conducted by the United States military. However, employment of RCA's is a contentious issue and the status of the law regarding use of RCA's is anything but clear.

"Each State Party undertakes not to use riot control agents as a method of warfare."[2] Article I(5) of the Chemical Weapons Convention (CWC) is a seemingly simple, straightforward and sensible provision. It is in fact intentionally undefined and ambiguous text that represents a compromise designed to find middle ground between polarized parties. Consequently, it is open to varying interpretations. Current United States policy regarding military use of RCA's is based on an unclear and contentious interpretation of the term method of warfare. United States military commanders, acting in accordance with that policy, risk being accused of violating the CWC.

The term method of warfare is not defined anywhere in the CWC, nor is there a widely accepted, or even readily identifiable, definition in all of

---

[2] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and Their Destruction, Jan. 13, 1993, art. I, ¶ 5, S. Treaty Doc. No. 21, 103d Cong., 1st Sess. (1993), 32 I.L.M. 800 [hereinafter CWC]. CWC, art. 1, in its entirety, reads:

> 1. Each State Party to this Convention undertakes never under any circumstances:
> (a) To develop, produce, otherwise acquire, stockpile or retain chemical weapons, or transfer, directly or indirectly, chemical weapons to anyone;
> (b) To use chemical weapons;
> (c) To engage in any military preparations to use chemical weapons;
> (d) To assist, encourage or induce, in any way, anyone to engage in any activity prohibited to a State Party under this Convention.
> 2. Each State Party undertakes to destroy chemical weapons it owns or possesses, or that are located in any place under its jurisdiction or control, in accordance with the provisions of this Convention.
> 3. Each State Party undertakes to destroy all chemical weapons it abandoned on the territory of another State Party, in accordance with the provisions of this Convention.
> 4. Each State Party undertakes to destroy any chemical weapons production facilities it owns or possesses, or that are located in any place under its jurisdiction or control, in accordance with the provisions of this Convention.
> 5. Each State Party undertakes not to use riot control agents as a method of warfare.

international law. This ambiguity is precisely what led to the inclusion of the term method of warfare in the language of the Convention.

United States military policy, embodied in Chairman, Joint Chiefs of Staff Instruction 3110.07A[3] allows for use of RCA's in several situations that may constitute a violation of the CWC. Two situations where United States policy allows use of RCA's are of particular concern - civilians used to screen attacks and rescue of downed aircrew. The lack of a definition of method of warfare makes the legality of CJCSI 3110.07A uncertain under international law. Many senior policy makers, including several top military commanders, seem to want to keep this area of the law undefined and ambiguous. Ominously, the United States may be sitting on a powder keg, poised to light the fuse itself.

Clarification of the fundamental issue – what constitutes a method of warfare – will help ensure United States policy correctly identifies permissible uses of RCA's. Clarification will put field commanders contemplating use of RCA's on a firmer legal footing with regard to the law of war. This paper examines of the circumstances that gave rise to current United States policy and offers a definition in support of that policy. Part I examines the dispute over RCA's, the compromise nature of the solution and the military's implementation of United States policy. Part II illustrates that there is a rising threat to military commanders being accused of, if not prosecuted for, alleged violation of international law. Part III explores various uses of chemical weapons and RCA's as methods of warfare, as well as several possible defining aspects of the term. Part IV proposes and analyzes the following definition: RCA's are a method of warfare when used to systematically enable or multiply the use of lethal force against hostile enemies.

I. The Chemical Warfare Convention and the United States Response

A. The Chemical Warfare Convention and the RCA Issue

Upon entering the CWC negotiations in 1984, the United States official view was that RCA's did not constitute chemical weapons, due to their

[3] CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 3110.07A, NUCLEAR, BIOLOGICAL, AND CHEMICAL DEFENSE; RIOT CONTROL AGENTS; AND HERBICIDES (15 Dec. 1998) [hereinafter CJCSI 3110.07A].

nonlethal nature.[4] This view began with the Geneva Gas Protocol of 1925, which banned "the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids materials and devices."[5] This was not a complete ban, as many nations, including the United Kingdom, the Union of Soviet Socialist Republics and the United States, reserved the right to retaliate in kind to a poison gas strike.[6]

Since 1925 when the Geneva Gas Protocols were adopted, the United States held firm to its interpretation that use of RCA's in war were not prohibited. This view was not shared internationally, nor was it unanimous even within the government of the United States. In response to United States Senate concerns over RCA during the ratification process of the Geneva Gas Protocol in 1975,[7] President Gerald Ford developed a compromise policy on such use. He issued Executive Order 11850, which states in pertinent part:

> The United States renounces, as a matter of national policy . . . first use of riot control agents in war except in defensive military

---

[4] S*ee Chemical Weapons Convention (Treaty Doc. 103-21): Hearings Before the Comm. on Foreign Relations United States Senate (Senate Hearing 103-869)*, 103d Cong. 36 (1994) (statement of Hon. Stephen J. Ledogar, U.S. Rep. to the Conference on Disarmament, U.S. Dep't of State) [hereinafter *Senate Foreign Relations Comm. CWC Hearings*].

[5] Protocol for Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65, at 1[hereinafter Geneva Gas Protocol].

[6] *Id.* at Reservations.

The United States Reservation states:

> The Protocol shall cease to be binding on the government of the United States with respect to the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials, or devices, in regard to an enemy state if such state or any of its allies fails to respect the prohibitions laid down in the protocol.

The Reservation of the United Kingdom states, in pertinent part:

> The said Protocol shall cease to be binding on His Britannic Majesty toward any Power at enmity with him whose armed forces, or the armed forces of whose allies, fail to respect the prohibitions laid down in the Protocol.

[7] Indeed, the Geneva Gas Protocol remained unratified by the United States for fifty years.

> modes to save lives such as: (a) Use of riot control agents in areas under direct and distinct U.S. military control, to include controlling rioting prisoners of war, (b) Use of riot control agents in situations in which civilians are used to mask or screen attacks and civilian casualties can be reduced or avoided, (c) Use of riot control agents in rescue missions in remotely isolated areas of downed aircrews and passengers, and escaping prisoners, (d) Use of riot control agents in rear echelon areas outside the zone of immediate combat to protect convoys from civil disturbances, terrorists and paramilitary organizations.[8]

The United States was determined to maintain its military's ability to use RCA's, or at least the uses delineated in E.O. 11850. The United States believed the best way to maintain its ability to use RCA's was to define chemical weapons such that RCA's would not be included in the CWC, and thus, would not be prohibited.[9]

A significant contingent of nations, led by the United Kingdom, were opposed to the United States' position of excluding RCA's from the CWC, and sought to have all use of RCA's outlawed.[10] More specifically, the British sought to include RCA's in the definition of chemical weapons and thereby prohibit them. They believed that any use of a RCA could too easily escalate to the use of lethal chemical weapons, and viewed RCA's as a large loophole in the effort to eradicate chemical warfare; a loophole they were determined to close.[11]

---

[8] Exec. Order No. 11850, 40 Fed. Reg. 161, 187 (1975) [hereinafter Exec. Order No. 11850].
[9] *See Senate Foreign Relations Comm. CWC Hearings*, *supra* note 4, at 34.
[10] *See* Letter, Hugh S. Philpott, British Embassy, Washington D.C., to Lieutenant General Wesely Clark, Director for Strategic Plans and Policy (J-5), Office of the Joint Chiefs of Staff (6 July 1995) (citing Letter, HM Chief of Defense Staff, to General Colin Powell (24 May 1992); Letter, Ministry of Defense Undersecratary David Omand, to Under Secretary of Defense Walter Slocombe (6 June 1994)) *cited in* Major Michael Jordan, The Chemical Weapons Convention & Executive Order 11850, A Constitutional Collision During Treaty Ratification14, n.31 (1999) (unpublished LL.M. thesis, Georgetown University Law School) (on file with author). According to Mr. Philpott, Her Majesty's Government "had concerns that an interpretation of the CWC that would allow use of non-lethal agents in war might create a dangerous loophole in the Convention. These concerns were set out in detail [in the letters cited]."
[11] *Id.*

Ambassador Adolf von Wagner of Germany, chairman of the Conference on Disarmament working group, emerged as a leader to find middle ground between the two extreme positions. He proposed a draft treaty that allowed RCA's for domestic law enforcement purposes,[12] but prohibited their use "as a means of warfare."[13] Von Wagner felt his compromise left enough room for all parties to agree.[14]

Perhaps the reason there was enough room for all parties to agree is that the term method of warfare was not defined by the Convention, or in international law. That left a wide enough range of interpretation for each side to stake its own claim as to the proper definition. Chairman von Wagner did lend some shape to the term when he described the compromise language. "These [RCA's] will be banned as a method of warfare, but allowed for normal domestic law enforcement purposes or for non-warfare military purposes, such as rescuing a pilot shot down behind enemy lines, or dealing with a riot in an prisoner of war camp . . . ."[15] This language is taken directly from Executive Order (E.O.) 11850, and must have been a concession to the United States.

The compromise language and the statement of Chairman von Wagner left the United States in a quandary. The United States wanted to sign the treaty, but only if the treaty reflected the interests of the United States.[16] The United States felt strongly that RCA's should not be covered in any way by the CWC. The compromise language addressed RCA's, but only prohibited use of these agents under certain circumstances. Likewise, in a press release, Chairman von Wagner expressed his opinion that the uses enumerated in E.O. 11850 would be allowed for non-warfare military use.[17] However, Chairman von Wagner's opinion was neither official, nor controlling.

The United States offered to accept the proposed language, if statements would be made on the negotiating record that clarified the term "method of warfare" as allowing the uses enumerated in E.O. 11850.[18]

---

[12] CWC, *supra* note 2, art. II (9) (d).
[13] *Id.* art. I (5).
[14] U.N. Press Release, GENEVA DATELINE (June 23, 1992). Von Wagner stated that he was sure "countries would realize that acceptable middle ground had been found in all areas." This included, of course, RCA's. [hereinafter U.N. Press Release]
[15] *Id.*
[16] Telephone Interview with Mr. Bernard Seward, Legal Counsel, United States Delegation to the Conference on Disarmament (Jan. 7, 2000).
[17] U.N. Press Release, *supra* note 14.
[18] S*ee Military Implications of the Chemical Weapons Convention (CWC): Hearings Before the Committee on Armed Services United States Senate (Senate Hearing 103-835)*, 103d Cong. 56

Initially, the German delegation offered to make such statements, but the British threatened to make counter-statements to the effect that uses consistent with E.O. 11850 were prohibited by the CWC, under their interpretation of the term method of warfare.[19] The Germans withdrew their offer to state on the record their support for the United States position.[20] The shift in the German position created a dilemma for the United States.

If the United States made a statement on the record regarding their interpretation of the uses of RCA's as a method of warfare, then the British would do the same. The prevailing thought seemed to be that the two opposing views would cancel each other out and the United States would lose anything it gained by making the statement.[21] Moreover, since there were more parties in agreement with the British,[22] such an exchange invited heavy input opposing the United States position. Ultimately, all parties remained silent. The United States believed this was the best way to protect its position.[23]

Everyone agreed to accept the compromise language, but no one agreed on what the language meant. Everyone remained silent as to the meaning of the language, so as to avoid upsetting the delicate balance that had been created. All major parties, including the United States, signed the treaty banning all use, stockpiling or production of chemical weapons. Contrary to the initial United States goal, the CWC did address RCA's, but used language deliberately chosen to allow different interpretations. Though each side had

---

(1994) (statement of General Shalikashvili, Chairman, Joint Chiefs of Staff) [hereinafter *SASC CWC Hearings*].

> During the CWC negotiations, the U.S. delegation in Geneva believed that the phrase "method of warfare" could be interpreted as permitting all the uses of RCAs provided in Executive Order 11850. In Washington, some agencies were concerned that the delegation's interpretation was "easily contested," and that a clear statement in the negotiating record preserving all four uses was essential.

Id.

[19] Position Paper, Office of Secretary of Defense, General Counsel, subject: United States Policy on Use of Riot Control Agents in War and its Relation to the Chemical Weapons Convention (December 1992) [hereinafter DoD Position Paper of Dec. 1992] (on file with the Judge Advocate General, U.S. Navy).

[20] *Id.*

[21] *SASC CWC Hearings*, *supra* note 18, at 56 (statement of General Shalikashvili).

[22] DoD Position Paper of Dec. 1992, *supra* note 19.

[23] *SASC CWC Hearings*, *supra* note 18, at 56 (statement of General Shalikashvili). "At that point, 'to best protect our position' against a more damaging negotiating record, the U.S. delegation was directed to accept the provision without a negotiating record statement." *Id.*

the opportunity, all parties chose not to clarify the meaning of method of warfare, as it related to RCA's. The situation was at least as muddled as before the CWC, perhaps more so.

B. United States Government Response to the Chemical Warfare Convention

As the Executive Department tried to figure out the exact scope and impact of the CWC, considerable debate arose regarding the use of RCA's prescribed in E.O. 11850. While the negotiators felt they agreed to a treaty that allowed all uses in E.O. 11850,[24] President William Clinton and his Administration ultimately made a contrary determination. Following considerable interagency review, the Clinton Administration concluded that the CWC precluded use of RCA's in two situations mentioned in E.O. 11850. These were "case 2: civilians used to screen attacks; and case 3: rescue of downed aircrew."[25] President Clinton proposed to modify E.O. 11850 accordingly.[26] When the Senate Armed Services Committee (SASC) took up

---

[24] *SASC CWC Hearings*, *supra* note 18, at 76 (statement of Senator Sam Nunn, Committee Chairman).

> The Committee understands that the U.S. signed the CWC in Paris with the understanding that the treaty allowed for the use of RCAs as defined in Executive Order 11850. General Shalikoshvili testified that: "During the CWC negotiations, the U.S. delegation in Geneva believed that the phrase 'method of warfare' could be interpreted as permitting all the uses of RCAs provided in Executive Order 11850."

Id.

[25] *Id.* at 56 (statement of General Shalikashvili).

> After the CWC was signed, the Clinton Administration conducted a thorough interagency review of the RCA issue. The administration determined, based on the position during and since the negotiations of other states, including key U.S. allies, that the current international understanding of the phrase "method of warfare" precludes two of the RCA uses (case 2: civilians used to screen attacks; and case 3: rescue of downed aircrew) outlined in EXEC. ORDER NO.11850.

Id.

[26] In a letter of transmittal to the U.S. Senate, dated June 23, 1994, regarding advice and consent of the CWC, President Clinton wrote:

> Article I(5) of the CWC prohibits Parties from using RCAs as a "method of warfare." That phrase is not defined in the CWC. The United States interprets this

the issue of the use of RCA's during its advice and consent process, a sizable contingent, led by Chairman Sam Nunn of Georgia, was ardently determined that commanders retain RCA's in the full range of uses prescribed in E.O. 11850.[27]

Senator Nunn demanded that commanders retain all options, even after the service chiefs agreed with the Clinton Administration position.[28] He

---

> provision to mean that: The CWC applies only to the use of RCAs in international or internal armed conflict. Other peacetime uses of RCAs . . . are unaffected by the Convention. The CWC does not apply to all uses of RCAs in time of armed conflict. Use of RCAs solely against noncombatants for law enforcement, riot control or other noncombat purposes would not be considered as a "method of warfare" and therefore would not be prohibited . . . . The CWC does prohibit the use of RCAs solely against combatants. In addition, according to the current international understanding, the CWC's prohibition on the use of RCAs as a method of warfare also precludes the use of RCAs even for humanitarian purposes in a situation where combatants and noncombatants are intermingled, such as the rescue of downed air crews, passengers and escaping prisoners and situations where civilians are being used to mask or screen an attack.

Letter of transmittal, President of the United States, to Senate of the United States, subject: Ratification of the CWC (June 23, 1999).

[27] *See SASC CWC Hearings*, *supra* note 18, at 76. Senator Nunn felt the United States legitimately understood the uses of Exec. Order No. 11850 were outside the meaning of the term method of warfare as used in CWC Article I(5), at the time of agreement. However, the United States position to forego placing a statement on the record as to the definition of method of warfare waylays that position. Since it chose to remain silent on the issue of the exact definition of method of warfare, the United States cannot then claim that the interpretation it professed, but did not proclaim, is binding or authoritative. Had it made the statement on the record, and dealt with the consequences, the United States could validly claim that its position must be recognized. Neither side wanted to jeopardize the entire treaty over this small point, no matter how fervently they felt about it. United States silence is thus understandable in light of its desire to avoid antagonizing the British. However, the United States could not have it both ways.

[28] *Id.* at 56 (statement of General Shalikashvili).

> The Joint Chiefs and I believe that several arguments can be made for RCA use in these two cases. However, we also recognize that a unilateral decision to adopt this position could cause serious divisions with key allies whose cooperation is essential to the CWC. Accordingly, on balance, the Joint Chiefs decided that the benefits of the CWC outweighed the importance of preserving the ability to use RCAs in these cases and that they would support the consensus

won. The Senate agree give its advice and consent to the ratification of the CWC, but only upon the President's agreement to 28 conditions.[29] Senate Ratification Condition 26B addressed the use of RCA's and stated, in pertinent part: "The President shall take no measure, and prescribe no rule or regulation, which would alter or eliminate Executive Order 11850 of April 8, 1975."[30] One week later, the President agreed to abide by all conditions.[31] The instrument of ratification was deposited with the United Nations Secretary General that same day, and the CWC went into force, with the United States as a Party, on April 27, 1997.

C. Implementation of United States Policy by the Armed Forces

When CJCSI 3110.07A came up for annual review in 1997, the question was raised whether the use of RCA's described in E.O. 11850 were still legal, given the recent entry into force of the CWC. Once again, no consensus opinion could be obtained. The Joint Staff, the CINCs, and the service chiefs[32] all wanted to maintain every option. Yet, the CJCSI had to take into account E.O. 11850 and the language of Senate Ratification Condition 26B.

The DoD attorneys charged with providing legal analysis of CJCSI 3110.07A decided that no determination was necessary on the RCA's issue because CJCSI 3110.07A is a policy instrument.[33] The President reserved the authority in E.O. 11850 to approve use of RCA's[34] making any legal analysis

---

reached within the administration on the RCA issue. The CINCs were informed of this decision.

Id.

[29] The conditions to Senate advice and consent are separate and distinct from reservations to the treaty itself. The CWC is a no reservations treaty.

[30] Relative to the Chemical Weapons Convention, Senate Advice and Consent Subject to Conditions, S. Exec. Res. 75, 105th Cong., 1st Sess., § 2, Condition 26B, 155 CONG. REC. S,3378, (1997) (enacted).

[31] Letter, President Clinton, to Senate of the United States (Apr. 25, 1997). In this letter, President Clinton refers to the conditions of ratification, and states; "I will implement these provisions." *See also* Letter, President Clinton, to Congress of the United States (Apr. 25, 1997). The period for ratification of the CWC was rapidly coming to a close. If the United States was to be in the initial set of parties to the Convention, it had to ratify by Apr. 27, 1997. Thus, the President had little choice but to accept the conditions of the Senate.

[32] Electronic Interview with General Carl Mundy, U.S. Marine Corps (retired) [hereinafter Mundy interview]. General Mundy was the Commandant of the Marine Corps at the time. He indicated that the Marine Corps and the Army, principally, wanted to retain all uses, especially for the purposes of riot control and force protection.

[33] Interview with Lieutenant Colonel William Lietzau, U.S. Marine Corps, then a major in the Office of Legal Counsel to the Chairman of the Joint Chiefs of Staff, in Quantico, Va. (7 Jan. 2000) [hereinafter Lietzau Interview].

[34] Exec. Order No.11850, *supra* note 8.

of CJCSI 3110.07A premature and unnecessary.[35] This was done as a matter of convenience, since neither consensus agreement nor a convincing analysis existed. The language of E.O 11850 remained in CJCSI 3110.07A because to remove language regarding use of RCA's following the CWC would imply that the U.S. considered some or all of the uses therein prohibited. The DoD was not prepared to take that position.[36] Thus, exactly when use of a RCA would constitute a method of warfare remains a mystery.

CJCSI 3110.07A is not a particularly clear document. It addresses the prohibitions of the CWC in paragraph 4.c.3,[37] and addresses RCA's in paragraph 4.d.,[38] referring the reader to Enclosure B for substantive information. Enclosure B gives two general categories for the use of RCA's: (1) in war; and (2) in peacetime military operations and operations other than war (OOTW). The uses permitted in war are listed in paragraph 2, and are verbatim from E.O. 11850, plus the addition of a fifth use: "Security operations regarding the protection or recovery of nuclear weapons."[39] Paragraph 3.e. addresses uses in OOTW.[40]

---

[35] Lietzau Interview, *supra* note 33.
[36] *Id.*
[37] CJCSI 3110.07A, *supra* note 3, at 3. ¶ 4.c.3. states: "The United States signed the Chemical Weapons Convention (CWC) in 1993, reference c and ratified the Treaty in April 1997. The United States agreed not to use, develop, produce, acquire, stockpile or retain chemical weapons for any reason."
[38] *Id*. at 3, ¶ 4.d. states:

> The CWC prohibits the use of RCAs as a "method of warfare." US policy distinguishes between the use of RCAs in war and in situations other than war. Approval to use RCAs is dependent of the situation in which their use is contemplated (See Enclosure B for policy on RCA use).

[39] CJCSI 3110.07A, *supra* note 3, at B-1.
[40] *Id*. at B-2.

> [T]he United States is not restricted by the CWC in its use of RCAs, including against combatants who are a party to a conflict, in any of the following cases . . . : (1) The conduct of peacetime military operation within an area of ongoing armed conflict when the United States is not a party to the conflict. (2) Consensual peacekeeping operations when the use of force is authorized by the receiving state including operations pursuant to Chapter VI of the United Nations Charter. (3) Peacekeeping operations when force is authorized by the Security Council under Chapter VII of the United Nations Charter.

Senate Ratification Condition 26 requires that RCA's be allowed during peacekeeping operations. CJCSI 3110.07A reflects this. The theory is that the United States would not be waging war in those situations, so any use of RCA's would not amount to a method of warfare. RCA's would only be prohibited as a method of warfare in international armed conflict or an internal conflict to which the United States was a party. However, the issue of whether a conflict has risen to the level of an armed conflict is open to as much interpretation as the definition of method of warfare.[41] Therefore, to discount the need for a method of warfare analysis based on the lack of an armed conflict does nothing to shore up the legal foundation on which United States policy stands.[42] The prudent course of action is to conduct the method of warfare analysis in any situation where military forces foresee using RCA's.[43]

II. The Rising Threat to Military Commanders

The ambiguity of the term method of warfare in the CWC raises the specter of United States policy opening military commanders to charges of violation of international law. Despite well-intentioned legal analysis by United States government attorneys, CJCSI 3110.07A permits uses that may be, in the majority view of nations, violations of the CWC.

A recent Associated Press report, regarding the death of an Albanian boy as a result of the North Atlantic Treaty Organization (NATO) bombing

---

Id.

[41] CJCSI 3110.07A, *supra* note 3, at B-1, defines armed conflict as "a use of force of a scope, duration, and intensity that would trigger the laws of war with respect to United States Forces." However, Pictet's Commentary on the Geneva Conventions differs dramatically: Any difference arising between two states and leading to the intervention of members of the armed forces is an armed conflict . . . . It makes no difference how long the conflict lasts, or how much slaughter takes place." *See* JEAN PICTET, GENEVA CONVENTIONS OF 12 AUGUST 1949 COMMENTARY 20-21 (1952).

[42] The United States argued that its military action in Panama in 1989 was not an international armed conflict, and that former Panamanian President Manuel Noriega was thus not a prisoner of war. A U.S. Federal District Court Judge disagreed and ruled that the action was indeed an international armed conflict. *See* United States v. Noriega, 800 F.Supp. 791 (S.D. Fla. 1192). It is exactly because of such differences of opinion that a determination that an action is OOTW rather than use in war is not sufficient to enable use of RCA's without regard for the CWC.

[43] Memorandum, Secretary of Defense, to Assistant to the President for National Security Affairs, subject: Riot Control Agents and the Chemical Weapons Convention (Apr. 4, 1994) [hereinafter DoD Memo]. "We cannot afford to abandon the executive order-protected use of RCAs on the ground that peacekeeping is not covered by the prohibition. Where peacekeeping forces face armed or semi-armed forces, (*e.g.* in Somalia) we will need to follow the law of war in our conduct." *Id.*

campaign designed to halt aggression by Serbian forces, contains the following passage:

> The two attacks are among cases cited by a group of Western legal experts and Russian lawmakers who want the international war crimes tribunal in the Hague to investigate alleged violations of international law by NATO and the United States during the 78-day bombing campaign aimed at halting a Yugoslav offensive against ethnic Albanians in Kosovo.[44]

It is not hard to imagine a similar outcry should chlorobenzylidene malononitrile (CS)[45] be used to disperse crowds of soldiers mixed with women and children around a downed NATO aircraft in Kosovo. Nor is it impossible to imagine an international tribunal convicting the commander who used that CS.

There is also a growing movement towards personal accountability for such offenses. Mr. Gary Sharp believes there is a need to prosecute the individual who commits the act, below the level of national leadership. He writes "[e]ffective system wide deterrence demands that a negative incentive be applied to all who have the ability to influence the commission of an unlawful act."[46] Mr. Sharp refers specifically to the failure of international law to hold the military leadership of totalitarian regimes responsible for their actions, focusing instead on the political leadership, and thus allowing the actual perpetrator to escape liability. However, this reasoning can easily be applied to the military leadership of democratic and republican nations, as

---

[44] Associated Press, *Albanian family seeks apology from NATO*, DAILY PROGRESS (Charlottesville, Va.), Jan. 7, 2000, at A5.

[45] *See generally* U.S. DEP'T OF ARMY, CENTER FOR HEALTH PROMOTION & PREVENTIVE MEDICINE, *Detailed Chemical Fact Sheets*, *at* http://www.apgea.army.mil/dts/dtchemfs.htm (last updated 23 July 1998) (referencing U.S. DEP'T OF ARMY, FIELD MANUAL 3-9, POTENTIAL MILITARY CHEMICAL / BIOLOGICAL AGENTS AND COMPOUNDS (1990)) ("CS was developed in the late 1950s as a riot-control substance. It is a more potent irritant than chloroacetophenone [CN] but less incapacitating. In the late 1960s, stocks of CS replaced CN. Presently, the U.S. Army uses CS for combat training and riot control purposes.") [hereinafter Army Chemical Fact Sheet]. *See* MP Laboratories, Inc., *Tear Gas Online – CS Info*, *at* http://www.homepage.third-wave.com/donpeace/cs.html (last revised 4 February 1999) ("It [CS] is used primarily as an incapacitating agent, both by military and law enforcement personnel.") [hereinafter MP Laboratories].

[46] WALTER GARY SHARP, *JUS PACIARII*, EMERGENT LEGAL PARADIGMS FOR U.N. PEACE OPERATIONS IN THE 21ST CENTURY 167 (1999).

well. Mr. Sharp cites *United States v. List*,[47] a famous Nuremberg case, to illustrate the failure of the defense of superior orders to insulate a commander from war crimes guilt. General List was not permitted to pass the blame for his actions to the dead Nazi leadership.[48] Similarly, a United States military commander could be held accountable for his actions in the field even though he was acting in complete compliance with higher military command guidance, as well as Presidential authority.

Lieutenant Colonel William Lietzau, U.S. Marine Corps, represented the United States in the Preparatory Commission for the International Criminal Court (ICC), Working Group on Elements of Crimes, the group responsible for drafting the elements of the substantive law over which the International Criminal Court will have jurisdiction. He also worked on the legal review of CJCSI 3110.07A immediately following the effective date of the CWC making him intimately familiar with the permitted uses of RCA's within the context of E.O. 11850.[49]

Given the lack of a clear definition of method of warfare, Lieutenant Colonel Lietzau recognized that some uses of RCA's contemplated by E.O. 11850 could be deemed methods of warfare, and could be viewed as violations of the CWC. He was particularly concerned with the use of civilians to screen attacks and the rescue of downed aircrew, as well as the fifth use described in CJCSI 3110.07A, recovery of nuclear weapons, a use which is not detailed in E.O. 11850.[50] Lieutenant Colonel Lietzau incorporated his concerns into his negotiating efforts. Most states taking part in the negotiations have attempted to define the use of a RCA as a method of warfare, and to include such use as an element to the crime of illegally using chemical weapons. Recognizing that current United States policy puts commanders in jeopardy of being judged to have used a RCA in such a manner, Lieutenant Colonel Lietzau steadfastly refused to allow that element to be included.[51]

---

[47] UNITED STATES V. LIST, 11 TRIALS OF WAR CRIMINALS BEFORE THE NUREMBERG MILITARY TRIBUNALS 759, 1218-19 (1950).
[48] SHARP, *supra* note 46, at 171.
[49] Lietzau Interview, *supra* note 33.
[50] Lietzau Interview, *supra* note 33.
[51] The current working copy of the Working Group's efforts reads:

> Article 8(2)(b)(xviii): War Crime of employing prohibited gases, liquids, materials or devices:
>
> 1. The conduct took place in the context of and was associated with an international armed conflict.
> 2. The accused employed a gas, other substance or device that causes death or serious damage to health in

Lieutenant Colonel Lietzau's experience in the ICC elements negotiations leads him to unhesitatingly declare that the United States interpretation is not shared by the majority of the states of the world.[52] Mr. Sharp, a participant in the initial legal analysis of the RCA's debate as a result of CWC Article I (5), personally believes that at least three of the uses permitted under CJCSI 3110.07A – civilians used to screen attacks, rescue of downed aircrew and action by United States forces in an area of armed conflict to which the United States is not a party – could be methods of warfare, depending on the circumstances.[53]

Most European commentators take an even sharper view. In their Commentary on the CWC, Walter Krutzsch and Ralf Trapp take the stance that a RCA used in circumstances directly correlating to CJCSI 3110.07A, Enclosure B, paragraph 3.e.1[54] is prohibited by the CWC as a method of warfare, and they take issue with the United States policy embodied in CJCSI 3110.07A.

> The expression "method of warfare" used in this paragraph [CWC, Article I(5)] was coined by the Geneva Conventions. The relevant restrictions on the use of certain weapons as a method of warfare apply not only to international conflicts, but also to

---

> the ordinary course of events, through asphyxiating or toxic properties.*
> 3. The accused was aware of the nature of such gas, substance or device.
>
> * Nothing in this element shall be interpreted as limiting or prejudicing in any way existing or developing rules of international law with respect to development, production, stockpiling and use of chemical weapons.

Discussion Paper Proposed by the Coordinator, Prepatory Commission for the International Criminal Court, Working Group on Elements of Crimes, subject: Article 8, prohibited gases, (2 Dec. 1999).

[52] Lietzau Interview, *supra* note 33.

[53] Telephone Interview with Mr. Walter Gary Sharp (21 December 1999). Mr. Sharp is a Lieutenant Colonel, U.S. Marine Corps (retired), and a former senior judge advocate. He is presently an adjunct professor of law at Georgetown University School of Law and has written several books on international law.

[54] CJCSI 3110.07A, *supra* note 3, at B-3. "The conduct of peacetime operations within an area of ongoing armed conflict when the United States is not a party to the conflict." *Id.*

> non-international conflicts. This is a generally accepted principle, resulting from the humanitarian character of rules related to the application of such weapons. From this it can be concluded that any use of riot control agents in a non-international armed conflict or in civil strife will, also when falsely interpreted as 'policy action,' be a prohibited use of such method of warfare.[55]

III. Towards a Method of Warfare Definition and Analysis

A. Chemical Weapons

Perhaps a useful place to begin an analysis of the term method of warfare, as it relates to chemical weapons and the CWC, is with the issue of whether chemical weapons are truly more dangerous than conventional weapons, and if so, why? According to Mr. Anthony Chordesman,

> [I]t is important to understand that regardless of how horrifying chemical weapons may seem to those who have never engaged in war, the more effective chemical weapons are far more merciful than untreated or badly treated fragmentation or body cavity wounds from small arms. . . . Regardless of the media impact on an event like Halabja, its actual impact on killing and human suffering is almost meaningless in the context of the horrors of the killing, disease and starvation produced by conventional bombing and forced relocation of the Kurds.[56]

---

[55] WALTER KRUTZSCH AND RALF TRAPP, A COMMENTARY ON THE CHEMICAL WEAPONS CONVENTION 18-19 (1994). Mr. Krutzsch is the former working group chairman, ad-hoc committee on chemical weapons, CD, Geneva Switzerland; Mr. Trapp was a guest researcher, Stiftung Wissenschaft und Politik, Ebenhauser, Germany.

[56] ANTHONY C. CHORDESMAN, ONE HALF CHEER FOR THE CWC: MILITARY PERSPECTIVE, IN RATIFYING THE CHEMICAL WEAPONS CONVENTION, 36 (1994).

Brigadier General John DeBarr, U.S. Marine Corps (retired), a veteran of the vicious fighting for the island fortress Iwo Jima during World War II, is one who has engaged in war. His views contradict those of Mr. Chordesman. Despite the horrendous American and Japanese losses he witnessed, General DeBarr stated that he would not favor a plan to use lethal chemical compounds on Iwo Jima.[57] General Debarr stated that he would have to think long and hard before using a weapon he so abhorred, even though the success of the plan would have obviated the need for him and thousands of other Marines to fight that grueling battle.[58] Use of chemical weapons might have saved over 7,000 American lives and 15,000 more American casualties on Iwo Jima. Interestingly, General DeBarr did not hesitate in the least in supporting the use of two atomic bombs on Japan.[59]

Mr. Chordesman offers statistics to show how chemical weapons might be employed and their lethal effect.[60] Perhaps it is the ease and stealth

---

[57] *SASC CWC Hearings*, *supra* note 18 (statement of Mr. Porter). Fleet Admiral Chester Nimitz, U.S. Navy, proposed to saturate the island of Iwo Jima with lethal chemical compounds that would penetrate the caves of the Japanese defenders and kill them, thus avoiding the costly assault. President Franklin Roosevelt overruled the plan.

[58] Telephone Interview with Brigadier General John DeBarr, U.S. Marine Corps (retired) (Feb. 2, 2000). General Debarr is the former Staff Judge Advocate to the Commandant of the Marine Corps, and commanded an infantry platoon on Iwo Jima in 1944.

[59] *Id.*

[60] CHORDESMAN , *supra* note 56, at 49.

> Using one aircraft delivering 1,000 kilograms of Sarin nerve gas or 100 kilograms of anthrax spores: Assumes the aircraft flies in a straight line over the target at optimal altitude and dispenses the agent as an aerosol. The study assumes that the biological agent would not make maximum use of this payload capability because this is inefficient. It is unclear whether this is realistic.
>
> | **Area Covered in Square Kilometers** | | **Deaths Assuming 3,000-10,000 People Per Square Kilometer** |
> |---|---|---|
> | Clear sunny day, light breeze: | | |
> | Sarin nerve gas | 0.74 | 300-700 |
> | Overcast day or night, moderate wind: | | |
> | Sarin nerve gas | 0.8 | 400-800 |
> | Clear calm night: | | |
> | Sarin nerve gas | 7.8 | 3,000-8000 |
>
> *Id.*

with which chemical agents can be used, and the frightening manner of death they can cause, that makes them so abhorrent and dangerous.

The poet and World War I veteran Wilfred Owen states this case most eloquently:

> Gas! Gas! Quick Boys!—An ecstasy of fumbling
> Fitting the clumsy helmets just in time,
> But someone still was yelling out and stumbling
> And flound'ring like a man in fire or lime.
> Dim, through the misty panes and thick green light,
> As under a green sea, I saw him drowning.
> In all my dreams before my helpless sight,
> He plunges at me, guttering, choking, drowning.
>
> If in some smothering dreams, you too could pace
> Behind the wagon that we flung him in,
> And watch the white eyes writhing in his face,
> His hanging face, like a devil's sick of sin;
> If you could hear, at every jolt, the blood
> Come gargling from the froth-corrupted lungs.
>
> Wilfred Owen[61]

B. Black and White – RCA's as a Method of Warfare

A complete picture of what chemical weapons can do makes it apparent why the CWC strives so momentously to eliminate them. Some argue RCA temporarily incapacitate; they do not kill - thus they do not pose the dangers detailed above.[62] However, others are concerned that perhaps they do pose those dangers, after all. The concern is twofold. First, is the use of RCA in conjunction with lethal weapons both chemical and conventional; second is the possibility of RCA use escalating to an exchange of lethal chemical agents.

1. RCA in Conjunction with Lethal Weapons

In her testimony before Congress in the ratification process of the CWC, Dr. Amy Smithson offered examples of RCA use that certainly constitute a method of warfare:

---

[61] Wilfred Owen, *Dulce Et Decorum Est*, *in* AN ANTHOLOGY OF WAR POEMS 114 (Frederick Brereton ed., 1930).
[62] *See generally* Army Chemical Fact Sheet, *supra* note 45; MP Laboratories, *supra* note 45.

> Distinguishing method of warfare use from a limited, defensive, life saving use of RCAs should be a fairly straightforward matter. The law of war describes a method of warfare as a way to attain military objectives . . . . According to this definition, flushing enemy soldiers from foxholes into the line of fire, or launching an RCA attack on an enemy command post easily qualify as method of warfare uses."[63]

The editors of the Chemical Weapons Convention Bulletin report that RCA have been used in warfare throughout the twentieth century.

> Police gases extensively used in war include ethyl bromoacetate and congeners in the first World War; agent CN in Ethiopia (from December 1935), China (from late 1937) and the Yemen (1963); and agent CS in the Vietnam War and the Iraq-Iran war. In each case, these agents were used mainly or entirely not to avoid the use of conventional firepower but in conjunction with it, as a force multiplier. Moreover, starting in World War I, combat use of such gases preceded every significant outbreak of lethal chemical warfare.[64]

Employment of RCA in advance of lethal weapons, whether chemical or conventional, against enemy troops, positions and equipment is the archetypal use as a method of warfare.[65] However, RCA's need not be used

---

[63] *SASC CWC Hearings*, *supra* note 18, at 149 (statement of Dr. Amy Smithson).
[64] Editors, 15 CHEMICAL WEAPONS CONVENTION BULL. 4 (March 1992) [hereinafter BULL.].
[65] CHORDESMAN, *supra* note 56, at 44. Possible chemical weapons uses and effects against military positions are illustrated by this chart:

Typical War-Fighting Uses of Chemical Weapons

Mission	**Quantity**
Attack an infantry position:	
Cover 1.3 square kilometers of territory with a "surprise dosage" attack of Sarin to kill 50% of exposed troops.	216 240-mm rockets (e.g., delivered by 18 12-tube Soviet BM-24 rocket launchers, each

only against strictly military targets in order to qualify as a method of warfare. When used in conjunction with lethal weapons, RCA is a method of warfare even if the targets are civilians.

The North Vietnamese used a combination of RCA and lethal chemical weapons in attacks on Hmong villagers in the 1970s. The incapacitating agents were used to quickly stun the targets and fix them in place until the deadly toxins, which worked more slowly, could be delivered. One journalist's account of a villager's experience is particularly telling.

> While we were all on the hill across from the village the MIGs came. We saw the colored gas, and the people in the village began to lie down and go to sleep. Then the MIGs came back and dropped the bags. When the bags burst, the powder inside turned into yellow gas like a cloud. When it came down it was like yellow rain . . .

---

	carrying 8 kilograms of agent and totaling 1,728 kilograms of agent.
Prevent launch of enemy mobile missiles:	
Contaminate a 25-square-kilometer missile unit operating area with a persistent nerve gas like VX.	8 MiG-23 or 4 Su-24 fighters, each delivering 0.9 tons of VX (totaling 7.2 tons of VX per square kilometer.)
Immobilize an air base:	
Contaminate a 2-square-kilometer air base with 0.3 tons of VX twice a day for 3 days.	I MiG-23 with six sorties or any similar attack aircraft.
Defend a broad front against large-scale attack:	
Maintain a 300-meter-deep strip of VX contamination in front of a position defending a 60 kilometer wide area for 3 days.	65 metric tons of agent delivered by approximately 13,000 155-mm artillery rounds.
Terrorize population:	
Kill approximately 125,000 unprotected civilians in a densely populated (10,000 per square kilometer) city.	8 MiG-23 or 4 Su-24 fighters, each delivering 0.9 tons of VX (totaling 7.2 tons) under optimum conditions.

Id.

> [W]e went back. Most of the people were already dead. There was blood coming from their noses and ears and blisters appeared on their skin. Their skin was turning yellow. The people who were not dead were jerking like fish when you take them out of the water. Soon some of them turned black and they got blisters like the others. Blood came from their noses and they died.[66]

The investigation of that incident led to the conclusion that "at least two, maybe three, different chemical agents may have been used, including a nerve agent, an irritant or riot control agent plus one or more other chemicals."[67]

RCA that are employed to enhance the effect of lethal weapons are thus certainly used as a method of warfare and are prohibited. "The Secretary of Defense agrees that the CWC would prevent some militarily useful applications of RCA's, when they would be used to achieve a military objective, e.g. against troops in caves."[68] But why prohibit a resource that can be very effective on the battlefield?

2. The Danger of Escalation

The fear is that use of RCA's on the battlefield will result in escalation to an exchange of lethal chemical weapons. General Carl Mundy, U.S. Marine Corps (retired), Commandant of the Marine Corps from 1992-1996, recalls that the RCA issue centered on the premise that use of RCA's could send a dangerous signal that chemical agents had been employed.[69] RCA's may be mistaken for lethal chemical weapons, and a retaliatory strike in kind launched. Even if the RCA is recognized for its true nature, its employment invites the use of lethal chemical weapons, by its mere presence on the battlefield. An editorial from the CWC Bulletin sums up the point:

> While some applications in this category may not be "use in war," [sic] others clearly are. The question here is whether

---

[66] STERLING SEAGRAVE, YELLOW RAIN 25 (1981).
[67] *Id*. at 32.
[68] DoD Memo, s*upra* note 43.
[69] Mundy Interview, *supra* note 32.

> the risk of further escalation does not outweigh such limited military benefit as these uses might bring. Use of disabling chemicals on intermingled combatants and civilians in a war zone, for example, could lead to or become the excuse for unrestricted employment in urban warfare."[70]

C. The Gray Area – When RCA May be a Method of Warfare and the Search for a Definition

At one end of the spectrum, there are uses of RCA's that are clearly allowed. For instance, the CWC itself allows for use of RCA's for law enforcement and domestic riot control.[71] At the other end of the spectrum are uses of RCA that are clearly designed to enhance the effect of lethal weapons in attaining a military objective, or that act as force multipliers. These uses are methods of warfare. The difficulty lies in finding where along that spectrum the employment of RCA's change from a permissible use to a prohibited method of warfare.

The analysis provided by the editors of the CWC Bulletin is instructive: "[s]omewhere in the spectrum of possible permitted purposes there must be a formulation, short of permitting use as a means of warfare, that the great majority of states can accept as a uniform standard in a treaty designed to benefit all its parties."[72] They were referring to finding acceptable language for the CWC's text, but the editors could just as easily have been referring to a definition of method of warfare. Exploration of various aspects of RCA's as a method of warfare is useful in attempting to find that formulation, and to propose a definition for method of warfare.

1. Avoiding Unnecessary Noncombatant Casualties

The most important measure in determining if a particular employment of a RCA constitutes a method of warfare is whether the goal of that employment is to avoid unnecessary noncombatant casualties. When the intent is to save innocent lives, rather than to enhance the effects of lethal weapons, then such use should not be identified as a method of warfare. Unnecessary noncombatant casualty avoidance is also the most useful purpose

[70] BULL, *supra* note 64, at 5.
[71] CWC, *supra* note 2, art. II(9).
[72] BULL, *supra* note 64.

of RCA's and the real reason the CINCs and service chiefs wanted to retain the option of using RCA's.[73]

The term defensive is often mistakenly used to convey the goal of avoiding combatant and noncombatant casualties. Moreover, a distinction is often drawn between offensive and defensive uses of RCA's in determining whether use of a RCA is a method of warfare. This differentiation is unimportant. The important distinction is whether the RCA is used to avoid casualties or as a multiplier of lethal force.

For many, the term defensive mistakenly connotes a sense of defenselessness and non-aggression. In fact, the defense is usually considered the strongest military form.[74] A force can inflict more casualties on an enemy from a strong defensive position than from any other. RCA's can be used to canalize attacking enemy troops into minefields or kill zones, to disorient them in their attack or to prepare them for a counteroffensive. It is no more legal or moral to use an RCA as a method of warfare in the defense than in the offense.

The defensive use of an RCA cannot be the yardstick by which to determine whether a particular employment of an RCA is a method of warfare. Taken to the extreme, focusing on the defensive as the critical evaluation of a method of warfare could lead to the conclusion that atomic warfare on Japan in 1945 was not a method of warfare. Following the attack on Pearl Harbor, all United States action in the Pacific could be termed defensive against Imperial Japan. Whether the force employing the RCA is on the defensive or the offensive is irrelevant. Rather, the purpose of the RCA employment is the critical determination.

Recent United States' military involvement in Somalia is an excellent example. RCA's could have been used to control Somali civilians who were rioting and threatening food convoys traveling to Somali refugee camps. Employment of RCA's in such a way would almost certainly be considered a permitted use, not because it defended the food, but because it sought to protect the food without inflicting casualties on the refugees.

---

[73] Mundy Interview, *supra* note 32. According to General Mundy, the key reason for retaining the option to use RCA's was to avoid casualties, where possible.

[74] CARL VON CLAUSEWITZ, ON WAR, 358 (Michael Howard et. al. trans., Indexed ed., Princeton Univ. Press) (1984) [hereinafter CLAUSEWITZ] ("[T]he defensive form of warfare is intrinsically stronger than the offensive."); *See generally* MARINE CORPS INSTITUTE, U.S. MARINE CORPS COMMAND AND STAFF NONRESIDENT COURSE: COURSE 9901 (1998) [hereinafter USMC C & S]. These references will give the reader a thorough grounding in the various forms of warfare and their relative strengths.

2. Method of Warfare vs. Means of Warfare

During the internal debate conducted by the various agencies of the Executive Branch concerning ratification of the CWC, Mr. Hays Parks[75] declared, on behalf of the Department of Defense, that all of the uses of RCA's contained in E.O. 11850 were clearly permitted under the language of the CWC, and specifically Article I(5). His opinions formed the basis of the initial DoD stance, which was rejected by President Clinton in favor of the Department of State viewpoint, but was ultimately rescued by Senator Nunn and his colleagues on the Senate Armed Services Committee (SASC).[76] Mr. Parks did not offer a definition of method of warfare, which would have defeated the United States strategy of maintaining ambiguity so as to be able to interpret method of warfare as it pleased. He did, however, offer some important distinctions and insights.

Mr. Parks draws a distinction between the term "method of warfare" and the term "means of warfare." He argues that method of warfare is aimed at the strategic and operational levels of war, while means of warfare is aimed at the tactical level of war.[77]

> *Means of warfare* generally refers to the effect of weapons in their use against combatants, while *methods of warfare* refers to the way in which weapons are used in a broader sense. Starvation of an enemy nation is a *method of warfare*; destruction of crops is a *means* by which the *method* would be accomplished.[78]

Mr. Parks points out that the use of RCA's contemplated under E.O. 11850 are all on the tactical level, and are, in fact, means of warfare, not methods of warfare. Therefore, the language of CWC, Article I(5) does not prohibit their use in those situations. He argues:

---

[75] Mr. Parks is a retired U.S. Marine Corps lieutenant colonel and judge advocate. He is the Special Assistant for Law of War Matters to the Judge Advocate General of the Army and an adjunct professor of law at George Washington University Law School. He has written and lectured, and is an acknowledged authority, on the law of war.

[76] *See supra* Part I.B.

[77] S*ee generally*, CLAUSEWITZ, *supra* note 74; USMC C & S, *supra* note 74. These references provide a complete discussion of the various levels of warfare.

[78] Memorandum, Hays Parks, Special Assistant for Law of War Matters to The Judge Advocate General of the Army, to DAMO-FDB (Ms. Kotras), subject: Meaning of Method of Warfare (22 June 1995) [hereinafter Parks Memo.].

> Had the CWC negotiators intended to prevent limited, tactical use of RCA . . . the language of the CWC would prohibit RCA use 'as a means or method of warfare.' Such language is used in the 1977 Additional Protocol I to the Geneva Conventions of August 12, 1949, a treaty with which negotiators were undoubtedly familiar.[79]

Mr. Parks' argument regarding the clarity of the intent of the CWC is convincing, though not without faults.[80] More importantly, the differentiation between means of warfare and method of warfare is critical. The further down the lethality scale of warfare an RCA is employed, the less likely that employment will constitute a method of warfare.

3. Incidental Operations

Another DoD document drafted during the CWC ratification debate offers helpful insights into the meaning of method of warfare.

> [I]t is entirely consistent with the CWC that DoD retain the flexibility to employ riot control agents in armed conflict as an effective and morally acceptable alternative to deadly force in situations where civilians and combatants are intermixed, in downed aircrew/passenger rescue missions, and in situations involving escaped prisoners.

---

[79] Parks Memo., *supra* note 78.

[80] Mr. Parks himself wrote that the terms method of warfare and means of warfare have been used indiscriminately in the recent past. He cites Article 35 of the 1977 Additional Protocol I to the Geneva Conventions. According to Mr. Parks: "The first paragraph merged the two phrases; the second used *methods of warfare* where (by the traditional understanding . . .) means of warfare would have been more accurate. This merger and misuse created confusion that has been impossible to resolve." *See* Memorandum, Hays Parks, Special Assistant for Law of War Matters to The Judge Advocate General of the Army, to Senior Deputy General Counsel, subject: CWC Convention (28 August 1995).

If the merger of the two terms is impossible to resolve, then interpretation of the exact meaning of the language used in the CWC cannot be based on the inclusion of the term method of warfare and the omission of the term means of warfare. This is especially so given all parties' silence on the negotiating record concerning the meaning of those terms.

> These are not "methods of warfare" but means of avoiding unnecessary casualties *in incidental operations*.[81]

The key concept is that of incidental operations. If the use of RCA's are not integral to attaining the military objective, but rather incidental to it, then it weighs less heavily against being classified a method of warfare. For example, using a RCA to clear civilians from the vicinity of a downed aircraft is an employment of a RCA which is incidental to the true objective, recovery of the aircrew. The goal is not clearing the civilians, but rather recovering the aircrew. Conversely, if the use of a RCA is part of achieving the military objective, then it weighs heavily in favor of constituting a method of warfare. For example, flushing soldiers from caves in order to engage them is part of the objective of overwhelming the enemy's defensive position; consequently, such use of an RCA is a method of warfare. The concept of incidental operations dovetails with Mr. Parks' distinction between method of warfare and means of warfare, and points to a definition of method of warfare that is aimed at a larger military design.

4. Dual Purpose

Dr. Matthew Meselson, a professor in the Department of Biochemistry and Molecular Biology at Harvard University, testified before the SASC concerning the CWC. Dr. Meselson's testimony illustrates the necessity to consider the dual use nature of RCA's in attempting to find a definition for method of warfare as used in the CWC. He specifically addressed whether RCA's should be subject to the prohibitions against development and stockpiling, beyond use as a method of warfare.[82] He points out that the Convention's definition of chemical weapons based on purpose allows for dual use chemicals, which have purposes in both peace and warfare. In his testimony, Dr. Meselson states that:

> In war, riot control agents are used to drive personnel from protective cover into the line of ground fire or bombing, to disrupt their operations and otherwise as multipliers of lethal force. History and common sense make it absolutely clear that

[81] DoD Memo, *supra* note 43 (emphasis added).
[82] *SASC CWC Hearings*, *supra* note 18, at 97-99 (statement of Dr. Matthew Meselson, professor, Harvard University Department of Biochemistry and Molecular Biology).

> riot control agents can be, depending on how they are used and in what quantities, chemical weapons of war.[83]

Dr. Meselson's concern is that if the only prohibition against riot control agents is one of use as a method of warfare, large-scale stockpiling of bombs and artillery shells filled with disabling chemicals would take place. The United Nations Special Commission inspectors found that approximately half of the Iraqi chemical arsenal consisted of large-scale mortar rounds filled with CS.[84] The only conceivable reason to possess such munitions is use as a method of warfare.

The Convention's primary aim is to prohibit not only the use of chemical weapons – something already accomplished by the 1925 Gas Protocols – but to end the existence of them. Since the use of RCA's are prohibited as a method of warfare, as are lethal chemical weapons, RCA's should also be subject to the entire regime of the CWC. Consequently, a method of warfare definition must allow for dual purposes. That is, it must allow for the existence of the chemicals that comprise RCA's when used for permitted purposes, such as domestic law enforcement. At the same time, it must prohibit not only RCA's used as a method of warfare, but stockpiling in a form that can only amount to use as a method of warfare.

5. Escalation

In determining a definition of method of warfare, a balance must be struck between avoiding unnecessary noncombatant casualties and the risk of escalating a conventional engagement into a lethal chemical weapons exchange. Use of RCA's against soldiers presents the danger of the enemy force mistaking the use of an RCA for lethal chemical warfare and retaliating in kind. Thus, the risk of escalation is high, while the need to avoid unnecessary non-combatant casualties is nonexistent. In the balance, use of RCA's in this manner would more likely be viewed as a method of warfare.

When only noncombatant civilians are present, the risk of escalation is minimal. Of course, every effort must be made to avoid injury to non-combatants. Therefore, use of RCA's on civilians without accompanying lethal force alone weighs heavily against being considered a method of

---

[83] *Id.*

[84] *SASC CWC Hearings*, *supra* note 18, at 97-99; MP Laboratories, *supra* note 45 ("CS can be disseminated in grenades, projectiles, aerosols, or as a powder.").

warfare. Mission accomplishment without casualties is ultimately the goal of employing RCA's.

The most difficult situation is that of commingled soldiers and noncombatants. The threat of escalation exists from the soldiers, but the responsibility to avoid unnecessary noncombatant casualties also looms large. Add force protection to this dilemma, and the military commander is faced with a difficult set of considerations, in the very scenario where RCA's are most important. The judgement must be made as to whether casualty avoidance is more important than the risk of escalation on a case-by-case determination. The option to use RCA's in a commingled situation should be available, in order to avoid noncombatant casualties, when that consideration outweighs the risk of escalation. Thus, use of RCA's when noncombatants are commingled with combatants should not be considered to be a method of warfare.[85]

IV. A Proposed Definition and Analysis

A definition of method of warfare, in relation to RCA's, might read: Riot Control Agents are a method of warfare when used to systematically enable or multiply the use of lethal force against hostile enemies. This simple definition needs an accompanying analysis to make it useful, and complete.

The following conclusions drawn from Part III of this paper are essential to full understanding of the proposed definition: First, when used as other than a method of warfare, the primary goal of employing a RCA is avoiding unnecessary noncombatant casualties, rather than enabling or enhancing lethal force. Emphasis on a defensive nature of employment is misplaced and irrelevant. Second, the further down the lethality scale of warfare RCA's are applied, the less RCA's are used in the manner the CWC sought to prohibit. When used in small scale, isolated and unique situations, rather than systematically, RCA's are not prohibited. Third, when employment of RCA's are incidental to accomplishment of the larger military goal, then such incidental use is not prohibited. Fourth, the determination must be made on the basis of purpose or intent for which RCA's are employed, rather than the substance of the RCA employed. This determination is necessary if the RCA issue is to be consistent with the CWC as a whole. Finally, the high risk of escalation prohibits use of RCA's against troops alone, but the low risk of escalation permits use against civilians alone, if used to avoid casualties. The benefits of RCA's used against commingled troops and civilians may outweigh

[85] Mundy Interview, *supra* notes 32 and 73.

the risk of escalation – thus use against commingled targets is not a method of warfare, and not a prohibited use.

The final conclusion regarding escalation bears further explanation. The proposed definition and analysis yield some of the protection against the fear of escalation in order to gain the benefit of avoiding unnecessary noncombatant casualties. Thus, use of RCA's in an environment of commingled enemy military and civilians would be permitted. The threat of escalation is greatest when enemy military forces are the targets of the RCA, the least when the targets are solely civilians. Consequently, use on troops alone must be prohibited and on civilians alone permitted. While the threat of escalation still exists in a commingled situation, this analysis rests on the premise that immediate avoidance of unnecessary casualties often outweighs the threat of a future retaliation. Moreover, it is exactly in the commingled situation that the commander has the toughest decision to make and the best opportunity to use RCA's to save lives.[86]

Summary

Under the status quo, several uses of RCA's allowed by CJCSI 3110.07A could be declared methods of warfare. There is no widely accepted definition for that critical term "method of warfare" and thus differing interpretations. The lack of a widely accepted definition results in United States policy standing on a flawed foundation. The definition proposed by this article would maintain all uses of RCA's during armed conflict that are presently deemed permissible. Some of the protections against escalation have been traded for the more immediate benefit of avoiding unnecessary noncombatant casualties.

The proposed definition allows RCA's to be used where civilians are commingled with enemy forces. Thus, RCA's would be permitted where civilians are used to screen attacks, as in the Mogadishu scenario presented at the beginning of this paper.[87] RCA's would also be permitted in the rescue of downed aircrew if the approaching danger to the aircrew consisted of civilians or commingled forces, but not if it consisted solely of enemy military forces. RCA's would be similarly permitted in the recovery of nuclear weapons. The use of RCA's under such circumstances strikes the best balance between avoiding the possibility of escalation and the unnecessary use of lethal force. Perhaps most importantly, it allows military commanders to retain the option

[86] Mundy Interview, *supra* notes 32 and 73.
[87] BOWDEN, *supra* note 1, at 49.

to use RCA's for riot control and force protection, their most valued employment.[88]

Regardless of whether the definition proposed in this paper or some other is used, the term method of warfare must be clarified. As military forces of all nations take on increasingly diversified missions, the utility of RCA's become more apparent. NATO forces have already used RCA in this new millenium.[89] As it stands, the foundation upon which United States policy rests is composed of shifting sand, which may be convenient for some, but exposes military commanders to accusations of violation of international law. In a world of increasing consciousness on such issues, commanders require firmer footing in order to act. Defining method of warfare provides commanders a firm foundation from which action that involves the use of RCA's may be taken.

[88] Mundy Interview, *supra* note 31.

[89] Associated Press, *NATO troops use tear gas in Kosovo*, DAILY PROGRESS (Charlottesville, Va.), Mar. 2, 2000, at A3. "French and British Troops fired tear gas to push back thousands of ethnic Albanians trying to force their way across a bridge into the Serb controlled side of this ethnically divided city." *Id.*

WHO'S DEFENDING THE DEFENDERS? : REBUILDING THE FINANCIAL PROTECTIONS OF THE SOLDIERS' AND SAILORS' CIVIL RELIEF ACT.

LIEUTENANT COLIN A. KISOR, JAGC, USNR*

I. Introduction: The history of special protections for military servicemen dates back to the Civil War.

The Soldiers' and Sailors' Civil Relief Act[1] (SSCRA) provides substantive and procedural legal protections to those "who have been obliged to drop their own affairs to take up the burdens of the nation."[2] The statute states Congress's purposes unambiguously:

> In order to provide for, strengthen, and expedite the national defense under the emergent conditions which are threatening the peace and security of the United States . . . provision is hereby made to suspend enforcement of civil liabilities, in certain cases, of persons in the military service of the United States in order to enable such persons to devote their entire energy to the defense needs of the Nation . . .[3]

When Congress enacted the modern statute in 1940, no new legal ground was broken. In 1864, Congress enacted a law limiting both civil and

---

* *Lieutenant Kisor holds a Bachelor of Arts in History from Trinity College in Hartford, Connecticut, and a Juris Doctor, cum laude, from Boston University School of Law.* *The Author thanks his wife, Melody, for her unfaltering support during the many weekends of research on the project, Lieutenant John Fojut for his counsel and guidance in researching this article, and Lieutenant Josh Nauman for his exceptional knowledge on the subtleties of income tax litigation. The opinions contained in this article are those of the author and do not necessarily reflect any opinion or policy of the Department of the Navy or the Department of Defense.* This article was edited by LCDR Rebecca A. Conrad, JAGC, USN and LT De Andrea G. Fuller, JAGC, USNR.

[1] Soldiers' and Sailors' Civil Relief Act, 50 U.S.C. Appx. §§ 501-91 (2001).

[2] Boone v. Lightner, 319 U.S. 561 (1943), *reh'g denied*, 320 U.S. 809 (1943).

[3] 50 U.S.C. Appx. § 510 (2001).

criminal actions against Union soldiers and sailors.[4] The Act of June 11, 1864 stated:

> That whenever, during the existence of the present rebellion, any action, civil or criminal, shall accrue against any person who by reason of resistance to the execution of the laws of the United States, or the interruption of the ordinary course of judicial proceedings, cannot be served with process for the commencement of such action or arrest of such person –
>
> Or whenever, after such action, civil or criminal, shall have accrued, such person cannot by reason of such resistance of the laws, or such interruption of judicial proceedings, be served with process for the commencement of the action –
>
> The time during which such person shall be beyond the reach of judicial process shall not be deemed or taken as any part of the time limited by law for the commencement of such action.[5]

Several Confederate States followed with similar Acts.[6] Notably, there were scant financial protections enacted in the laws of either the Union or Confederate relief acts; however, it is important to note that the Sixteenth Amendment to the United States Constitution (providing for income taxation) had not yet been written or ratified.[7] Additionally, the economy in the 1860s was not nearly as complex as it is today, and consumer credit was not as widespread prior to the advent of credit cards and the deregulation of interest rates.[8]

---

[4] Act of June 11, 1864 ch. 118, 13 Stat. 123 (1864) (session law title: Limitation of Action. Certain Time not to be Reckoned) [hereinafter Act of June 11, 1864].
[5] *Id.*
[6] WILLIAM MORRISON ROBINSON, JUSTICE IN GREY: A HISTORY OF THE JUDICIAL SYSTEM OF THE CONFEDERATE STATES OF AMERICA, 83-88 (1941).
[7] U.S. CONST. amend. XVI (ratified in 1913).
[8] *See* David A. Moss and Gibbs A. Johnson, *The Rise of Consumer Bankruptcy: Evolution, Revolution, or Both?,* 73 AM. BANKR. L.J. 311 (Spring 1999).

Congress enacted the Soldiers' and Sailors' Civil Relief Act in 1918, as America prepared to enter World War I.[9] Reflecting a policy change on the part of Congress, the SSCRA of 1918, did not include a provision for the automatic stay of criminal proceedings.[10] The SSCRA of 1918 provided for a stay of proceedings which would prejudice a servicemember's "civil rights," where the servicemember's ability to perform contractual obligations or present a defense in a civil lawsuit were "materially affected" by military service.[11]

Congress enacted the SSCRA of 1940 as America's involvement in World War II loomed on the horizon.[12] The Act essentially resurrected the SSCRA of 1918 (which had expired by its own provision six months after the end of World War I). The SSCRA of 1940 largely mirrored the SSCRA of 1918, including limited application to civil proceedings where the servicemember's ability to participate in civil actions was "materially affected" by his military service.[13] Congress amended the SSCRA in 1942,[14] 1944,[15] 1948,[16] 1952,[17] 1958,[18] 1960,[19] 1962,[20] 1966[21] and 1972[22] -- each time focusing on the SSCRA during a time when national interest turned to military conflicts.

One commentator credits Saddam Hussein with directing Congress' attention back to the SSCRA for the first time in eighteen years.[23] The Persian Gulf War involved activation of some 50,000 military reserve and National Guard personnel and served as the impetus for the 1991 amendments to the

---

[9] Soldiers' and Sailors' Civil Relief Act of March 18, 1918, ch. 20, 40 Stat. 440 (1918).
[10] *Id.*
[11] *Id.*
[12] Soldiers' and Sailors' Civil Relief Act of 1940, ch. 888, 54 Stat. 1178 (1940).
[13] *Id.*
[14] Soldiers' and Sailors' Relief Act, Amendment, ch. 581, 56 Stat. 769 (1942).
[15] Soldiers' and Sailors' Relief Act, Amendment, ch. 397, § 1, 58 Stat. 722 (1944).
[16] Veterans' Administration, Expenditures, ch. 170, § 6, Pub. L. 473, 62 Stat. 160 (1948) (amending the SSCRA); Selective Service Act of 1948, ch. 625, tit. I, § 14, 62 Stat. 623 (1948) (amending the SSCRA).
[17] Soldiers' and Sailors' Relief Act, Amendment, ch. 450, 66 Stat. 151, (1952).
[18] Soldiers' and Sailors' Relief Act, Amendment, ch. 857, § 14(76), 72 Stat. 1272 (1958).
[19] Soldiers' and Sailors' Relief Act, Amendment, 74 Stat. 820 (1960).
[20] Soldiers' and Sailors' Relief Act, Amendment, ch. 771, 76 Stat. 768, (1962).
[21] Internal Revenue Code of 1939, Amendment, ch. 358, § 10, 80 Stat. 28, (1966) (amending IRS application of sections of the SSCRA).
[22] Veterans' Employment and Readjustment Act of 1972, ch. 540, tit. V, § 504, 86 Stat. 1098, (1972).
[23] Lieutenant Colonel Gregory M. Huckabee, *Operation Desert Shield and Desert Storm: Resurrection of the Soldiers' and Sailors' Civil Relief Act*, 132 MIL. L. REV. 141, 158 (1991).

SSCRA of 1940.[24] Though amendments were needed, the Act did not require many new substantive legal protections for servicemembers.[25]

This article examines two of the most often violated provisions of the Soldiers' and Sailors' Civil Relief Act. These two provisions bear most directly on individual military readiness with respect to servicemembers' finances: (1) the residence and taxation provision, and (2) the interest rate cap. Part II explores the erosion of the SSCRA's residency and taxation provisions, arguing that amendments are needed to prevent the further collapse of these protections. Part III addresses the interest rate cap, exploring the various policy reasons for the protection and arguing that the protection should be expanded to promote retention of trained personnel in the armed forces. Ultimately, this article concludes that the once powerful financial protections of the SSCRA are being chipped away by erroneous decisions of various state and federal courts. Congress should take immediate action to strengthen the SSCRA's language to effectuate its ultimate purposes in enacting the Act--"to enable members of the armed forces to devote their entire energy to the defense of the nation."[26]

II. Court decisions have eroded the valuable protections involving residency and taxation.

In order to keep states from taxing the military income of nonresident servicemembers, Congress should revisit, strengthen and expand the SSCRA provisions involving residency and taxation. Section 574 was intended to protect servicemen who are stationed in a state pursuant to military orders from paying income or personal property taxes in that state. The plain language of the Act is just vague enough, however, to have its once powerful protections eroded by recent court decisions regarding domicile and income tax. The Act states:

> For the purpose of taxation of any person, or of his personal property, income, or gross income, by any state, territory, possession, or political subdivision of any of the foregoing, or by the District of Columbia, such person shall not be deemed to have lost a residence or domicile in any

[24] *Id.* at 157-58.
[25] *Id.* at 142; 157-58.
[26] 50 U.S.C. Appx. § 510 (2001).

> state, territory, possession, or political subdivision of any of the foregoing, or in the District of Columbia solely by reason of being absent therefrom in compliance with military or naval orders, or to have acquired a residence or domicile in, or to have become a resident in or a resident of, any other state, territory, possession, or political subdivision of any of the foregoing, or in the District of Columbia while, and solely by reason of being, so absent.[27]

Congress's primary intention here was to exempt military members who are residents of one state, but are stationed in another, from having the second state assess income tax on their military salaries.[28] Recently, some states have tried to tax military income by circumventing the statute. Minnesota and New Jersey have found ways to involuntarily convert nonresident military members stationed there into state residents for the purpose of subjecting their military income to the states' income tax. Additionally, employed spouses of servicemembers are left unguarded by the statute in its current form; consequently, in some states spouses must pay more tax on their incomes than persons not married to military members. For example, some states compute the tax rate applied to the non-military spouse's income based on the total joint income, effectively taxing some of the non-resident, military member's pay.

A. *Aggressive state income tax collection on the military: An assault on the SSCRA's protection.*

The Federal District Court in Minnesota recently decided a case brought by the United States which, absent a swift Congressional response, could spell the end of SSCRA income tax protections for servicemembers entirely.[29] In that case, the State of Minnesota sought "to tax the income of twelve Public Health Service (PHS) Officers who are posted within the State of Minnesota, yet legitimately claim domicile elsewhere."[30] Recognizing clear

---

[27] 50 U.S.C. Appx. § 574 (2001).

[28] *See* Captain Robert L. Minor, *Inclusion of Nonresident Military Income in State Apportionment of Income Formulas: Violation of the Soldier's and Sailor's Civil Relief Act*, 102 MIL. L. REV. 97 (1983).

[29] *See* United States v. Minnesota, 97 F. Supp. 2d 973 (D. Minn. 2000).

[30] *Id.* at 975. The United States Public Health Service is one of the Federal Uniformed Services and Public Health Service Officers are entitled to SSCRA protections. *See* 42 U.S.C. § 213(e).

violations of the SSCRA, the United States brought suit in Federal District Court, seeking a ruling that the PHS Officers were not "residents" within the meaning of the Minnesota statute at issue.[31]

The District Court noted that under the Minnesota statute "resident" meant "any individual domiciled in Minnesota"[32] and accurately framed the question: "the case turns on the proper 'domicile' of the PHS Officers."[33] Citing the United States Supreme Court's language from *Mitchell v. United States*[34] the court noted that, "[D]omicile is a term often invoked in the law, yet often without exact clarity. The Supreme Court has defined domicile as 'a residence at a particular place accompanied with positive or presumptive proof of an intention to remain there for an unlimited time.'"[35]

The first issue confronting the District Court was whether the SSCRA preempted the entire body of Minnesota tax law at issue. The court correctly noted that, "[t]o the extent that a state law is in 'irreconcilable conflict' with federal law, the state law is preempted. When a state law 'stands as an obstacle to the accomplishment and execution of the full purpose and objectives of Congress,' such an irreconcilable conflict is present."[36]

The District Court considered the plain language of the SSCRA, and determined that although the SSCRA prohibits any state from presuming a servicemember to be a resident of that state "solely" based on military orders, Minnesota could consider other factors to determine if the servicemember was in fact a resident of that state.[37] Paradoxically, then, the SSCRA did not preempt application of Minnesota state law to determine whether or not an out-of-state servicemember was a resident of Minnesota.

The factors the District Court went on to consider under the Minnesota statute included: (1) the domicile of the PHS officer's spouse, (2) the location of his home (regardless of whether it was owned or rented), (3) the state that issued his driver's license, (4) the state that registered his

---

[31] *United States v. Minnesota*, 97 F. Supp. 2d at 981.
[32] *See* MINN. STAT. § 290.01(7) (2000).
[33] *United States v. Minnesota*, 97 F. Supp. 2d at 981.
[34] 88 U.S. 350 (1874). S*ee generally* Lea Brilmayer, et. al. *A General Look at General Jurisdiction*, 66 TEX. L. REV. 723 (1988) (providing a useful discussion of the evolution of the concept of "domicile").
[35] *United States v. Minnesota*, 97 F. Supp. 2d at 981.
[36] *Id*. (citing Barnett Bank of Marion County v. Nelson, 517 U.S. 25 (1996)).
[37] *United States v. Minnesota*, 97 F. Supp. 2d at 984.

automobile, and (5) whether or not the PHS officer had coached little league baseball in the local community.[38]

The District Court found the inquiry concerning a domicile of a PHS officer to be "fact intensive" and noted that SSCRA protections for servicemembers are "not total."[39] Exhibiting a certain clarity of thought, if not syntax, the court realized that the domicile of a PHS officer's spouse was "a decision reflecting not whatsoever on any intention by the officer to remain in Minnesota,"[40] and thus held that the SSCRA preempted this factor from consideration. However, in a ruling with potentially catastrophic effects on military families, the court held that "[t]he Soldier's and Sailor's Civil Relief Act of 1940 does not pre-empt the use of the [other] factors listed in Minnesota Rule 8001.0300 [location of owned or rented home, drivers license, auto registration, civic clubs] to determine the domicile of Public Health Officers."[41] Thus, the federal court decided a federal question by conducting a state law analysis.

Interestingly, the Kansas Court of Appeals conducted an identical preemption analysis and reached the opposite result.[42] *In the matter of the Application of Karsten for Exemption from Ad Valorem Taxation in Riley County, Kansas*, ("*Karsten*") a consolidation of five tax appeals, the Tax Assessor of Riley County, Kansas, sought a determination that the appellees, Army personnel stationed at Fort Riley, Kansas, were Kansas residents.[43] Riley County relied upon Kansas' statutes regarding taxation and argued that under Kansas law, the servicemembers were Kansas residents.[44]

The Kansas Court of Appeals properly noted that "[s]tate law impermissibly conflicts with a federal right if 'the state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.'"[45] The Kansas court cited the United States Supreme Court's often quoted statement on the presumption inherent in any analysis of the SSCRA: "[T]he Act must be interpreted 'with an eye friendly' to those

[38] *United States v. Minnesota*, 97 F. Supp. 2d at 983.
[39] *Id.* at 985.
[40] *Id.*
[41] *Id.*
[42] *See In the matter of the Application of Karsten for Exemption from Ad Valorem Taxation in Riley County, Kansas*, 924 P.2d 1272 (Kan. Ct. App. 1996).
[43] *Id.* at 1275.
[44] *See Id.* at 1275. The statute at issue defines a "resident" as "any person registered to vote in any county" the statute also created a rebuttable presumption that a person was a resident if he or she "owns, leases, or rents a domicile" in Kansas. *See* KAN. STAT. ANN. § 8-1, 138 (1996).
[45] *Karsten*, 924 P.2d, at 1276 (citing Jones v. Rath Packing Company, 430 U.S. 519 (1977)).

who dropped their affairs to answer the country's call.'"[46] Thus approaching the preemption question with an understanding of the proper analysis to be undertaken, the court stated,

> The Soldiers' and Sailors' Civil Relief Act does not define "residence" or "domicile" and does not set forth any standards for determining where a serviceman's or servicewoman's residence or domicile exists under the Act. However, the exemption created by the Act is a creature of federal law, and it is inconsistent to look to state law to determine where such residence or domicile exists. This would subject military personnel to potentially inconsistent state laws for determining their eligibility for [tax exemptions].[47]

Applying this principle, the court reached exactly the opposite result as the United States District Court for the District of Minnesota. The Kansas Court of Appeals held "that the applicant's residency, for purposes of the Soldiers' and Sailors' Civil Relief Act, must be determined under federal principles and not state law."[48]

This analysis is consistent with Congress' intent in enacting the SSCRA as determined by the United States Supreme Court. Congress should remedy the determination of "residency or domicile" legislatively, by amending the SSCRA so that states cannot involuntarily convert nonresident servicemen into resident taxpayers.

The problems of preemption and residency determination are not unique to Minnesota and Kansas. New Jersey has also sought to convert nonresident servicemembers into state residents in order to tax their income.[49] In one New Jersey Tax Court case, the plaintiff, a Navy sailor, testified that he did not consider himself to be a New Jersey resident.[50] The sailor, Norman D. Wolff, testified that he entered the Navy while living in Pennsylvania, and still

---

[46] *Karsten,* 924 P.2d, at 1276 (citing California v. Buzard, 382 U.S. 386 (1966)).
[47] *Karsten,* 924 P.2d, at 1276.
[48] *Id.*
[49] *See* Wolff v. Baldwin, 9 N.J. Tax 11 (N.J Tax Ct. 1986).
[50] *Id.*

used his parents' address in Philadelphia as his military "home of record."[51] Mr. Wolff also maintained a valid Pennsylvania drivers' license, voted by absentee ballot in Pennsylvania, and paid local Philadelphia school taxes.[52] In fact, the only connection Mr. Wolff had with New Jersey (other than being stationed there) was that he and his wife had jointly purchased a house as "tenants by the entirety" and had filled out a "homestead rebate claim form" which vested the property with certain tax advantages.[53] Mr. Wolff and his wife, as tenants by the entirety, were both required to sign the form in order for her to gain the protections of the statute.[54]

The New Jersey Tax Court considered, and rejected, Mr. Wolff's assertion that the SSCRA prohibited New Jersey from taxing his military pay. The New Jersey Tax Court held, "[B]y executing and filing a homestead rebate form, plaintiff and his wife assert that they are citizens and residents of this state. 'Citizen' and 'resident' has been defined as domicile under [New Jersey law]."[55] In finding that Mr. Wolff was in fact a New Jersey resident, the court stated, "[w]hile the Soldiers' and Sailors' Civil Relief Act is a shield to protect servicemen from double taxation, it is not a sword to avoid the payment of taxes justly imposed."[56] It is important to scrutinize the New Jersey Tax Court's rationale that produced this decision--a decision flawed in two major respects. First, the court did not adequately address the issue of whether the SSCRA preempted application of the state tax at issue, thereby deciding residency according to the New Jersey statutes. Second, the court's analysis evidences a misunderstanding of the Supreme Court's holding in *Mitchell v. United States*[57] where the Supreme Court defined domicile as "a residence at a particular place accompanied with positive or presumptive proof of an intention to remain there for an unlimited time."[58]

The New Jersey Tax Court dismissed the sailor's ties to Pennsylvania, ignoring the plain language that "such person shall not be deemed to have lost a residence or domicile in any state . . . solely by reason of being absent

---

[51] *See Id.* at 12. ("[U]pon entering active duty in the Navy in 1958, the year of his entry, a person must have completed a form NAVPERS 262, which established a 'home of record' for tax and statistical purposes.").
[52] *See Id.* at 13.
[53] See *Id.* at 6.
[54] Homestead Rebate Act, N.J. STAT. ANN. § 54:4-3.80.a (West 1982).
[55] *Wolf*, 9 N.J. Tax at 22 (citing N.J. STAT. ANN. § 54:4-3.30; Roxbury Tp. V. Heydt, 6 N.J. Tax 73 (N.J. Tax Ct. 1983)).
[56] *Wolff*, 9 N.J. Tax at 12.
[57] 88 U.S. 350 (1874).
[58] *United States v. Minnesota*, 97 F. Supp. 2d at 981.

therefrom in compliance with military or naval orders"[59] and attacking each factor in Mr. Wolff's absence from Pennsylvania in a way which, if duplicated, would strip servicemembers everywhere of SSCRA tax protections.

The Court dismissed the use of his parents' address in Philadelphia as his "home of record," stating "the property on Burlhome Avenue is a single family residence owned by his parents for which they pay the local property taxes. It is not the place of residence of plaintiff and his wife...."[60] This statement bespeaks a misunderstanding of the realities of military service. Clearly, the plaintiff and his wife lived in New Jersey because he was stationed there. The court apparently expected the plaintiff and his wife to maintain an apartment in Pennsylvania to use as a "home of record." The court stated, "there is absolutely no evidence before the court that plaintiff and his wife ever resided in the Philadelphia property or that plaintiff has had any physical presence there since he went into the Navy except to visit his parents."[61] Implicit in the court's reasoning here is that marriage, subsequent to induction into the military service, is enough to divest the servicemember of residency from his "home of record" unless his wife had lived in that home as well. The court failed to state what action or circumstance which, coupled with parental visitation, would be sufficient to show a physical presence sufficient to maintain residence at the Philadelphia address.

The court next focused on his Pennsylvania driver's license, listing his parents' Philadelphia address, and dismissed it as "a convenience to avoid the necessity of obtaining a license in each state in which he was stationed."[62] While this may indeed have been convenient, the court placed no evidentiary value on this factor in its determination of New Jersey residency. Similarly, the court dismissed his voting in the presidential election with a Pennsylvania absentee ballot. "The court concludes that plaintiff's voter registration was again a convenience to him."[63] Most shockingly, the court considered his payment of Philadelphia School Tax with a heavily jaundiced eye,[64] stating:

> [h]is payment of the school income tax does not support physical contact. While the

[59] 50 U.S.C. Appx. § (2001). This section was in effect in its present form when *Wolff* was decided in 1986.
[60] *See Wolff*, 9 N.J. Tax at 16.
[61] *Id.*
[62] *Id.*
[63] *See Wolff*, 9 N.J. Tax at 16. Voting by absentee ballot is arguably more *inconvenient* than voting locally.
[64] *Id.; But see* California v. Buzard, 382 U.S. 386 (1966) (mandating that the SSCRA be interpreted "with an eye friendly to those who dropped their affairs to answer the country's call").

> establishment of a domicile to obtain beneficial tax treatment is not improper, the payment of a tax in a given state does not establish domicile or even residence. In other words one can establish a domicile for tax purposes but one cannot pay taxes to establish domicile. *This is especially so in the case where the State of Pennsylvania does not tax income derived from the United States Government for active duty outside the Commonwealth of Pennsylvania as a member of its armed forces*.[65]

Again, the court placed an impossible burden on the servicemember to establish physical presence in one state while stationed in another. More importantly, the court totally misconstrued the plain language of Section 574. The New Jersey Tax Court is apparently of the view that the SSCRA applies differently with respect to residency if the "home of record" state does not have an income tax, or has special tax benefits for servicemembers. This would subject servicemembers to inconsistent application of the federal statute. Congress clearly intended to avoid the entire "residency" versus "domicile" argument by stating the terms "residency" and "domicile" in the disjunctive.[66] "Such person shall not be deemed to have lost a *residence or domicile* in any state . . . solely by reason of being absent therefrom in compliance with military or naval orders, or to have acquired a *residence or domicile* in [the state stationed in]."[67]

In addition to a failure to correctly weigh the residency factors, the court placed undue emphasis on the "homestead rebate form" completed by Mr. Wolff and his wife.[68] Despite the court's realization that " . . . [t]here were no government quarters available or assigned to his family, and he was therefore required by the Navy to seek the rental or purchase of a residence in a local community,"[69] completion of this form was enough to outweigh all other factors and establish New Jersey residency for Mr. Wolff.[70] Under the New Jersey law, there was no way for Mrs. Wolf, presumably a New Jersey resident (as she was not a plaintiff in the action), to file for a "homestead

---

[65] *Wolff*, 9 N.J. Tax, at 17 [emphasis added].
[66] 50 U.S.C. Appx. § 574 (2001)
[67] *Id.* [emphasis added].
[68] *See Wolff*, 9 N.J. Tax, at 7.
[69] *Id*. at 14.
[70] *Id*. at *7.*

rebate" when the property was deeded as a tenancy by the entirety with a nonresident servicemember.

Wolf v. Baldwin highlights two areas where Congress should act to prevent states from involuntarily conferring residence upon servicemembers, subjecting them to state income tax. First, Congress should eliminate the word "solely" each place it appears in Section 574(1) of the SSCRA. Second, Congress should expand the scope of Section 574 to protect military dependents as well.

Congress intended to protect servicemembers from the precise type of state taxing determinations imposed in *United States v. Minnesota* and *Wolff v. Baldwin*. These cases establish precedents encouraging States to tax military members as long as there is some additional connection to the state, however tenuous, besides the military orders.

The fundamental problem with the courts' analyses in Minnesota and New Jersey lies in the fact that those courts ignored Congressional intent, and shifted to the *states* the ability to determine who among the military population is, or is not, a domiciliary for tax purposes. Additionally, the United States Supreme Court has stated that the servicemember, not the state, chooses the residence of the servicemember.[71] Nothing in the SSCRA prevents a servicemember from voluntarily changing residences when stationed in a state in order to take advantage of more favorable tax laws. But, given the nature of military service, the decision on "residency" is fundamentally personal. Though this is clear under the intended interpretation of the SSCRA, it has been ignored by some courts, and therefore should be made explicit by Congress.[72]

A properly amended Section 574(1) would read:

> For the purpose of taxation of any person, or of any person's personal property, income, or gross income, by any state,

[71] *See* Carrington v. Rash, 380 U.S. 89 (1965).

[72] 50 U.S.C. Appx. § 574 (2001). Practically speaking, many people in the military who have been stationed at one time or another in Florida or Texas voluntarily acquired residency in those states because they have no state income tax. Thus, though people in the United States military come originally from all 50 states and many foreign countries, the number who carry Florida or Texas driver's licenses, and claim Florida or Texas residency is disproportionately high. However, the freedom to reside in any of the 50 United States is inherent in the Constitution, as is a State's freedom to levy tax on the income of its domiciliaries, or choose not to do so.

> territory, possession, or political subdivision of any of the foregoing, or by the District of Columbia, such person shall not be deemed to have lost a residence or domicile in any state, territory, possession, or political subdivision of any of the foregoing, or in the District of Columbia by reason of being absent therefrom in compliance with military or naval orders, *or being a dependent of a person in such compliance*, or to have acquired a residence or domicile in, or to have become a resident in or a resident of, any other state, territory, possession, or political subdivision of any of the foregoing, or in the District of Columbia while, and by reason of being, so absent.

The word "solely" appears twice in the Section 574(1) and should be deleted to avoid confusion.

To preserve the right of a servicemember to choose his state of residence, and to preempt states from applying widely varying tax laws which determine residency for tax purposes, Congress should draft an additional Subsection to 574 which would read:

> Nothing in this Section or this Act shall be construed to prevent any person from voluntarily changing residence or domicile. The state, territory, possession, or political subdivision of any of the foregoing, or the District of Columbia in which such person maintains an active driver's license and in which his or her ballot is counted in national elections, if identical, shall constitute an irrebuttable presumption that such person is a resident and domiciliary of that state, territory, possession, or political subdivision of any of the foregoing, or the District of Columbia.

Thus, states would be unable to consider military members and their spouses, stationed therein solely as a result of military orders, as residents. Nor would the state be able to tax their military income if two factors exist concurrently:

(1) a drivers license maintained in the home state, and (2) voting by absentee ballot in the home state. The proposed language would explicitly preempt application of state law to determine the residence of a servicemember, or his or her family, and would better accomplish Congress' intent to protect servicemembers from state taxation outside the "home state" as determined by the member.

The suggested modification to Section 574 would benefit individual sevicemembers, the Armed Forces, and the states in three respects. First, there would be a bright line rule: if the military member maintains a driver's license and votes by absentee in his or her home state, he or she cannot be found to have lost his or her residence there, nor to have gained a new residence by having been stationed in another state pursuant to military orders. Therefore, the servicemember would know exactly how to maintain or change his or her home state residence. Second, the Armed Forces would know precisely how to instruct servicemembers to maintain their home state residences or acquire a new one. Third, all interested parties would benefit from a bright line rule, avoiding potential litigation efforts and expense where residence or domicile is at issue.

In cases where the servicemember has not complied with both of these requirements, a court could then look to other factors in order to discern the member's intent, keeping sight of the general spirit of the SSCRA.

B. *Back door taxation of military salary: Increased state income taxation on the nonmilitary spouse.*

Additionally, Congress should complete the Section 574 protections by amending the SSCRA to establish similar "residence" protections for military family members who accompany their sponsors to their duty stations. Such amendment is particularly necessary in light of the unfortunate Tenth Circuit Court of Appeals decision in *United States v. Kansas*.[73] In fact, one military attorney predicted, in 1983, that more states would test the SSCRA in exactly this way.[74] The issue was framed succinctly:

> Congress enacted the SSCRA to afford those in military service a wide variety of protections. The taxation of military

[73] 810 F.2d 935 (10th Cir. 1987).
[74] *See* Captain Robert L. Minor, *Inclusion of Nonresident Military Income in State Apportionment-of -Income Formulas: Violation of the Soldier's and Sailor's Civil Relief Act?,* 102 MIL. L. REV. 97 (1983) [hereinafter Minor].

> income by any state other than the servicemember's home state is clearly prohibited. To assume Congress would permit duty states to indirectly collect taxes which they are barred from assessing directly pierces and diminishes the federal legislative protection. To require a nonmilitary wage earner married to a military servicemember to carry a greater tax burden reduces the disposable income of the one individual taxpayer and the military couple.[75]

Notably, twelve years before *Karsten* reached the Kansas Court of Appeals, the United States District Court for the District of Kansas held that, "the Kansas tax laws do not operate in conflict with the Soldiers' and Sailors' Civil Relief Act."[76] In that case, the United States sued in Federal Court seeking a determination that the SSCRA preempted Kansas from considering a nonresident servicemember's military income for the purpose taxing a resident military spouse at a higher rate than if she were single.[77] The District Court held that the SSCRA did not preempt state tax law in that regard, but noted that "[o]f course, this interpretation does not serve the broadly stated purpose of protecting military personnel from the burdens of supporting state government."[78]

The United States appealed to the Tenth Circuit, which affirmed the District Court's holding that the SSCRA did not preempt the state tax law at issue, and noted:

> [N]either the legislative history nor the plain language of the SSCRA prohibits the use of the described military income in formulas which set rates of taxation on other income. The United States steadfastly maintains that the potentially higher rates on Kansas source income constitute "an

[75] Minor, *supra* note 74, at 106.
[76] United States v. Kansas, 580 F. Supp. 512 (D. Kan. 1984).
[77] *Id.*
[78] *Id.* at 516.

> indirect tax on the military compensation of nonresident military personnel." [79]

The Tenth Circuit left open the possibility of a successful challenge based on principles of Constitutional equal protection. "The obvious further inquiry is whether the potentially higher tax on Kansas taxable income constitutes a denial of due process or equal protection. The United States did not pursue any equal protection argument . . ." [80] The equal protection argument is that a Kansas resident, who is married to a nonresident servicemember, will pay a higher percentage of income tax than a person married to a Kansas resident with no taxable income. This arguably treats military dependents differently than other Kansas residents and, in an equal protection challenge, Kansas would have to show that it had a rational basis for application of its tax laws in this way. [81] The United States Supreme Court has held that "inequalities that result not from hostile discrimination, but occasionally and incidentally in the application of a [tax] system that is not arbitrary in its classification, are not sufficient to defeat the law." [82]

Other jurisdictions have followed Kansas' lead and are taxing military spouses at a rate higher than other residents. The higher state tax rates are achieved by including the servicemember's military pay when calculating the non-military spouse's income. [83] Obviously, these taxing schemes concern the military community. Nothing short of congressional action will prevent States from imposing these unfair taxing schemes. An Army judge advocate predicted this trend in 1983, when the United States first brought suit in the Federal District Court of Kansas challenging that state's practice of taxing a military spouse at a higher rate than a person married to a civilian. [84]

For example, the State Board of Equalization of California, using curious legal reasoning, has upheld this exact practice. In one case, the California Tax Board stated, "[c]ontrary to the appellant's contentions that respondent's determination unfairly taxes the wife's nonresident income, this method is the precise one prescribed by Revenue and Taxation Code section

---

[79] United States v. Kansas, 810 F.2d 935, 938 (10th Cir. 1987).
[80] *Id.*
[81] *See* Davis v. Michigan, 489 U.S. 803 (1989) (noting that a challenged tax provision was not unconstitutional under an equal protection analysis because the discrimination at issue was justified under a rational basis test.).
[82] Lunding v. New York Tax Appeals Tribunal, 522 U.S. 287 (1998) (citing Maxwell v. Bugbee, 250 U.S. 525 (1919)).
[83] *See In re* Boone, 1993 CAL TAX LEXIS 287, No. 92A-0830-CS (Cal. State Bd. of Equalization Oct. 28, 1993).
[84] *See* Minor, *supra* note 74.

17041."[85] The appellants' contention, however, was *not* that the Franchise Tax Board applied the wrong section of the code; it was that the code "unfairly taxed the wife's nonresident income."[86] The Board also stated "the use of this method does not result in the wrongful taxation of nonresident military income. It merely causes the appellants to pay California taxes on their California-source income at a rate commensurate with their total income."[87] How these two statements are logically consistent with each other, or with the SSCRA, is unclear, especially considering that the SSCRA states "income or gross income" recognizing the difference, and capturing both within its ambit. However, courts that have considered the issue of indirect tax of military pay levied against a servicemember's spouse, have refused to recognize the indirect tax of nonresident military income as a violation of the SSCRA. These decisions highlight the need for a legislative remedy.

To illustrate the impact of indirect taxation on a military family, consider the following example. Based on the year 2000 California state income tax tables,[88] a California resident who earned $50,000 in taxable income in 2000, married to another California resident with no taxable income, has $1,070 of income tax liability on that California income.[89] However, if the same California resident was married to a nonresident military member who also earned $50,000 of income (not taxable by California), the California resident would then have to pay $2,560 on the $50,000 of California income.[90] Since the only variable in the equation is the otherwise nontaxable out-of-state military income, which may also be taxed by the servicemember's home state, California is indirectly taxing out-of-state military income in violation of the Soldier's and Sailor's Civil Relief Act.[91]

In a case which did not involve military members or the SSCRA, a Justice on the New York Court of Appeals refuted the argument that a state could constitutionally tax a nonresident's income by taxing a resident's income

[85] *In re* Oyster, 1996 CAL TAX LEXIS 75, No. 94R-0593 (Cal. State Bd. of Equalization Apr. 11, 1996).
[86] *Id.*
[87] *Id.*; *See also In re Boone*, 1993 CAL TAX LEXIS 287.
[88] Interview with LT Joshua Nauman, JAGC, USNR, Tax Officer, Naval Legal Service Office Southwest, conducted on March 22, 2001. For the purpose of this article, LT Nauman prepared fictitious tax returns [Appendices A & B] by completing identical California 540 resident tax form and California Non-resident or Part year resident forms (filing jointly, with no children), varying only the residence of the military spouse and the non-resident military income.
[89] Appendix A.
[90] Appendix B
[91] *Id.*

at a higher rate. In a strongly worded dissent in *Brady v. New York*,[92] Justice Hancock wrote:

> No State may impose a tax on income earned outside of the State by a nonresident. That is settled constitutional law. . . . The question in this case is whether by considering the nontaxable out-of-State income in determining the tax rate on the New York income, the State is, in reality, taxing the out-of-State income and doing indirectly what it cannot do directly. The answer to the question, of course, is the one dictated by logic and common sense: the State is taxing the outside income. Including it results in a higher tax bracket and the nonresident pays more tax on the New York income.[93]

Justice Hancock aptly states, from a constitutional perspective, a principle of fairness that should apply in the absence of special statutory protection: states should not tax, directly or indirectly, the income of nonresidents. However, when one superimposes the SSCRA protections over a particular state's statutory scheme, given the proper application of federal preemption of state tax law by the SSCRA, states should not be able to tax the income of nonresident servicemembers, directly or indirectly.

To correct this injustice to nonresident servicemembers, Congress should add an additional subsection to SSCRA Section 574 that would read.

> For the purpose of taxation of any person's income, or gross income, by any state, territory, possession, or political subdivision of any of the foregoing, or by the District of Columbia, no state, territory, possession, or political subdivision

---

[92] 607 N.E.2d 1060 (N.Y. 1992) (Hancock, J., dissenting).

[93] *Id.* The *Brady* case did not involve nonresident servicemen therefore the New York Court of Appeals was not considering the SSCRA. The issue of SSCRA preemption did not arise. The Bradys were New Jersey residents with New York income. The majority opinion cited the 10th Circuit for the proposition that taxing nonresidents at a higher rate was constitutional. Additionally, in another case the Supreme Judicial Court of Maine cited United States v. Kansas, 810 F.2d 935 (10th Cir. 1987), for the proposition that it rejected Constitutional violations, including Equal Protection, despite the fact that the Tenth Circuit expressly did not undertake an equal protection analysis because the United States did not raise the argument. *See* Stevens v. State Tax Assessor, 571 A. 2d. 1195 (Super. Ct. Me. 1990).

> of any of the foregoing, or the District of Columbia may consider nonresident military income as a basis for taxation of any person, or in calculating that rate of taxation of the income of any person.

Amendment of this subsection to SSCRA, Section 574, as indicated above, would force some states, notably Kansas and California, to change the way in which they collect income taxes from spouses of military members stationed there. This would bring those states back in line with the original intent of Congress in enacting the Soldiers' and Sailors' Civil Relief Act of 1940--prohibiting states from taxing the military income of nonresident servicemembers.

III. The existing public and private sector interest rate subsidies of military personnel should be strengthened and expanded.

A provision of the SSCRA promoting military readiness by providing a direct financial benefit to servicemembers is the six-percent interest cap.[94] This provision provides that any pre-service debt (that is, any debt incurred prior to the debtor's entry onto active duty) may not, during any period of active duty, bear interest at a rate higher than six-percent. Thus, under the present form of the law, an active duty servicemember may cap his or her interest rate for most pre-service obligations at six-percent. Any interest over the six-percent cap is forgiven; it does not accrue.[95] The Act states:

> No obligation or liability bearing interest at a rate in excess of six-percent per year incurred by a person in military service before that person's entry into active duty shall, during any part of the period of military service, bear interest at a rate in excess of six-percent per year unless, in the opinion of the court, upon application thereto by the obligee, the ability of such person in military service not materially affected by reason of such service, in which case the court may make such order as in its opinion may be just. As used in this section the term "interest" includes service

[94] *See* 50 U.S.C. Appx. § 526 (2001).
[95] *Id.*

> charges, renewal charges, fees, or any other charges (except bona fide insurance) in respect of such obligation or liability.[96]

By its own terms, this section only applies to pre-service debts. By enacting this section, Congress tacitly acknowledged that military pay is typically below that of the civilian private and public sectors. In its present form, the section provides financial protection for reservists called to active duty, as well as a benefit to new military recruits.

Practical application of this provision is significant. For example, a recruit who reports to military basic training subsequent to signing a financing agreement for a car purchase may reduce that interest rate to six-percent upon entering active duty--the first day of boot camp. Additionally, recalled reservists may cap the interest on all secured and unsecured loans and mortgages, as well as credit card accounts, at six-percent for the duration of the period activated, including regular or special periods of training and weekend drills.

The Act imposes the burden on the creditor to commence a civil action to seek relief from this section. Thus, the creditor who does not wish to lose profit (made up of interest on the obligation exceeding six-percent) must sue the servicemember and show that the servicemember's ability to pay is "not materially affected" by his or her entry into military service in order to capitalize interest at a rate greater than six-percent.[97] A subsequent section of the SSCRA provides criminal sanctions against a creditor who repossesses a servicemember's collateral absent a court order--giving teeth to the interest rate cap.[98]

Though this section has been largely effective at accomplishing Congress' purpose, there are several ways Congress could positively affect military readiness by strengthening and expanding this section. The following proposals would allow existing servicemembers to focus on their military duties, rather than on financial problems and the concurrent civil litigation

---

[96] 52 U.S.C. Appx. § 526 (2001).
[97] *Id.*
[98] 52 U.S.C. Appx. § 526 (2001); S*ee also* Pacific Finance Corporation v. Gilkerson, 217 S.W.2d 440 (Civ. App. Tex 1948) (noting that "[i]f [the serviceman] was in fact the owner of the car in question at the time of its seizure on that date, the repossession of the car by Pacific Finance Corporation, without resorting to suit and judgment, was unlawful and the awarding of the judgment for damages for the conversion of his car would be warranted . . . ").

associated with them, and would also provide the military with a powerful incentive for recruiting and retention.

A. Congress should unambiguously articulate a Private Right of Action to enforce the six-percent provision.

Predictably, the consumer credit industry vigorously opposes this provision, and may be expected to oppose any attempt by Congress to strengthen the six-percent provision.[99] The perfect example of creditor opposition to this provision can be found in a recent federal case in Illinois: *Moll v. Ford Consumer Finance Co. Inc.*[100]

In *Moll*, despite the plain language of the statute, Ford Consumer Finance argued that Congress did not intend to provide a private right of action to servicemembers where creditors refuse to reduce the interest rate on a pre-service debt to six-percent.[101] The U.S. District Court for the Northern District of Illinois flatly denied Ford's assertion that the SSCRA provides only "defensive relief."[102] Ford argued that Mr. Moll, a reservist activated for service during the Persian Gulf War, lacked standing to sue Ford for refusing to lower the interest rate on his car loan to six-percent while he was serving in the Persian Gulf. Ford contended that the six-percent provision was applicable where a creditor brings an action to enforce the underlying obligation--debt collection or repossession. The District Court disagreed, holding that under the United States Supreme Court's decision in *Cort v. Ash*[103] a private right of action was recognized, allowing a plaintiff to enforce the six-percent provision. Ford's motion to dismiss was denied. The District Court also rejected Ford's

---

[99] *See, e.g.*, Robert M. O'Toole, Senior Staff Vice President, Mortgage Bankers Association of America, Prepared Statement Before the Comm. on Veterans' Affairs Subcomm. on Education, Training and Housing, Hearings on Pending Veterans' Legislation (Aug. 2, 1995) (transcript available on LEXIS, Federal News Service) (urging the 104th Congress to "adjust the interest rate to a more realistic [higher] level").

[100] *See* Moll v. Ford Consumer Finance Co. Inc., 1998 U.S. DIST. LEXIS 3638, No. 97 C 5044 (E.D. Ill. Mar. 16, 1998) (mem.).

[101] *Id.*

[102] *Id.*

[103] 422 U.S. 66 (1975). The U.S. Supreme Court in *Cort v. Ash* outlined a four part test to determine the existence of a private right of action under a federal statute. The prongs are: (1) whether the plaintiff is a member of the class for whose benefit the statute was enacted; (2) whether there is any indication that Congress intended to create or deny such a remedy; (3) whether an implied remedy is consistent with the underlying purpose of the statute; and (4) whether the cause of action is one traditionally relegated to state law. *See Id.*

contention that the Act only limits the amount of interest recoverable.[104]

Although a relatively recent decision, the *Moll* case has been followed by at least two other federal courts, brought by a *pro se* litigant, Mel M. Marin.[105] In *Marin v. Armstrong*, Mr. Marin alleged that Transouth Financial Corporation and others violated his rights under the SSCRA "in a scheme intended to harass him to the point of death."[106] The Federal District Court for the Northern District of Texas incorporated the *Moll* analysis into its decision, correctly stating that "without a private cause of action there would be no way for a servicemember to ensure that his rights were protected under the section"[107]

Emboldened by his victory in Texas, Mr. Marin then sued Citibank in New York for similar violations of the SSCRA.[108] The District Court Judge dismissed his complaint *sua sponte*, holding that the SSCRA did not provide a private right of action.[109] Undaunted, Mr. Marin appealed to the Second Circuit Court of Appeals, arguing that the dismissal was improper and providing the court with the "Findings, Conclusions, and Recommendation" of the prior decision in Texas.[110] The Second Circuit vacated the District Court's dismissal and remanded the case.[111]

After the *Moll* and *Marin* decisions it seems that the intended private right of action is being upheld, at least in the Second, Fifth, and Seventh Circuits. Congress, however, should foreclose all debate about this by enacting an additional subsection to Section 526 which would explicitly state that a private right of action is available to any

---

[104] *See Moll*, 1998 U.S. DIST. LEXIS 3638.
[105] Marin v. Armstrong, 1998 U.S. DIST. LEXIS 22792, No. CA 3:97-CV-2784-D (N.D. Tex Sep. 1, 1998) (reporting the Federal Magistrate's recommended findings of fact and conclusions of law on the Def.'s Mot. to Dismiss). Marin v. Citibank, 2000 U.S. APP LEXIS 3789, No. 98-7976 (2d Cir. Mar. 10, 2000) (unpublished).
[106] *Marin v. Armstrong*, 1998 U.S. DIST. LEXIS 22792.
[107] *Id.*
[108] *Marin v. Citibank*, 2000 U.S. APP LEXIS 3789 (unpublished).
[109] *See Id.*
[110] *Marin v. Citibank*, 2000 U.S. APP LEXIS 3789 (unpublished).
[111] *See Id.* Mr. Marin's impressive *pro se* crusade continued throughout the 1990s. *See* Marin v. Crawford, 1996 U.S. APP. LEXIS 30863, No. 96-1068 (6th Cir. Nov. 22, 1996) (unpublished) (holding that Mr. Marin was not entitled under the SSCRA to stay a Chapter 7 bankruptcy proceeding of Ares Industries, where Mr. Marin was one of over 140 unsecured creditors of the debtor corporation).

servicemember who seeks to enforce the SSCRA six-percent provision. Given military members' low incomes and the concomitant restricted access to the courts, this new subsection should provide for recovery of attorneys' fees, litigation costs, and punitive damages for noncompliance on the part of the creditor. This would better effect Congress' purpose in enacting this section of the SSCRA and ultimately decrease litigation in this area, enabling servicemembers to focus their energies on their respective missions, rather than on civil litigation.

B. *Congress should expressly include federal student loans in the six-percent provision.*

Congress should address the tension between low military income and multi-thousand dollar educational debt. The provision of the SSCRA that allows servicemembers to cap *any* pre-service financial obligations at six-percent annual rate of interest does not apply to federally guaranteed student loans.[112] A section of the Higher Education Act (HEA) states:

> Usury laws inapplicable. *No provision of any law of the United States* (other than this act) of any State (other than a statute applicable to such State's student loan insurance program) which limits the rate or amount of interest payable on loans shall apply to a loan –
>
> (1) Which bears interest on the unpaid principal balance at a rate not in excess of the rate specified in this part; and,
>
> (2) Which is insured by the United States under this part.[113]

This section of the statute arguably conflicts with Section 526 of the SSCRA which states that "*No obligation or liability bearing interest* at a rate in excess of six-percent per year incurred by a person in

[112] *See* Higher Education Act, 20 U.S.C. § 1078(d) (2001) [emphasis added].
[113] 20 U.S.C. § 1078(d) (2001) [emphasis added].

military service before that person's entry into service shall . . . bear interest at a rate in excess of six-percent per year . . . . "[114]

Though the SSCRA is not a "usury law" within the meaning of the HEA, Congress has not carved out an exception to the SSCRA for federal student loans. Congress does seem to have intended to preempt the SSCRA with the Higher Education Act according to the Department of Education's standard form letter sent in reply to servicemembers' requests to lower student loan interest rates. The Department of Education's form letter thanks the servicemember for his or her "inquiry regarding the Direct Loan interest and the Soldiers' and Sailors' Civil Relief Act" and concludes, "while we appreciate your situation, Direct Loan borrowers' interest rates are not affected by the Soldiers' and Sailors' Civil Relief Act."[115]

Congress could fulfill important national objectives by amending the Higher Education Act to allow military members to cap their interest at six-percent on federal student loans. First, in accordance with the express purposes of the SSCRA, allowing servicemembers to reduce the interest on such loans increases military readiness by alleviating financial hardships incurred by those servicemembers with educational debt incurred prior to entry into military service. "Increasing military readiness" is an oft-used term by military proponents which means, in part, "increasing retention and recruiting."[116] Put simply, when servicemembers are not buried in federal student loan debt they are more likely to join the military and stay in for a longer period of time. Second, this type of amendment to the HEA would likely decrease the number of defaults on federal student loans by lowering student loan payments for active duty military. With more affordable payments, it might also obviate the need for "hardship deferrals" while simultaneously generating more revenue for the federal student loan program

There is ample history of Congressional action amending the Higher Education Act to encourage recruiting and retention in certain professions. Congress has amended the HEA to authorize the

---

[114] 50 U.S.C. Appx. § 526 (2001).
[115] *See* Letter from the Department of Education to Author: "Interest Rate Unaffected by the Soldiers' and Sailors' Civil Relief Act" (May 23, 2000) (on file with author.)
[116] *Fiscal Year 2002, Dep't of Def. Budget: Hearing of the Def. Subcomm.*, 107th Cong. (statement of Gen. Hugh Shelton, Chairman, Joint Chiefs of Staff) (transcript available on LEXIS, Federal News Service, Sept. 5, 2001) [hereinafter Shelton Testimony].

Secretary of Education to institute a program to *forgive*, not merely cap the interest on student loans to encourage people to enter certain professions.[117] Section 1078-10, in Title Twenty of the United States Code is entitled "Loan Forgiveness for Teachers." Section 1078-10 states, "[I]t is the purpose of this section to encourage individuals to enter and continue in the teaching profession."[118] The section provides that "the Secretary [of Education] shall carry out a program, through the holder of the loan, of assuming the obligation to repay a qualified [federal student loan].[119]

Similarly, the subsequent section, enacted with the dual purposes of encouraging recruiting and retention of child care providers states that its dual purposes are: (1) "to bring more highly trained individuals into the early child care profession;"[120] and, (2) "to keep more highly trained child care providers in the early child care field for longer periods of time."[121] This section also provides for a program of loan forgiveness.

If Congress' desire is to boost military recruiting and retention, Congress should afford military servicemembers the same professional status as teaching and early childcare with respect to student loans. Congress should amend the HEA to authorize the Secretary of Education to develop a program to forgive federal student loans for individuals who enlist or who are commissioned in the armed forces. Failing that, Congress should amend both the HEA and the SSCRA to allow military servicemembers to cap their interest rate on student loans at six-percent. Obviously, the former proposal is the stronger one. However given the financial hardships associated with military service under the current pay structure, any relief would be welcomed by servicemembers.[122]

C. *Congress should amend the SSCRA to provide interest rate relief for post-entry debts.*

One way Congress could expand existing protections of the SSCRA to increase recruiting, improve retention, and ensure better

---

[117] *See* 20 U.S.C. § 1078-10 (2001).
[118] *See* 20 U.S.C. § 1078-10 (2001).
[119] *See Id.*
[120] *See Id.* at § 1078-11(a)(1) (2001).
[121] *See Id.* at § 1078-11(a)(2) (2001).
[122] Shelton Testimony, *supra* note 116.

readiness throughout the military is to amend the Act to allow active duty servicemembers to cap post-enlistment loans at some reasonable rate of interest. This could be a variable rate, tied to the prime rate, to provide an incentive to lenders to encourage them to make loans to military members. Given the consumer credit industry's vigorous opposition to the six-percent cap, as reflected in the *Moll* and *Marin* decisions, intense opposition to any proposed expansion of this protection is likely.

However, some post-enlistment interest rate protection for servicemembers is clearly necessary. According to the 2001 military pay chart, a typical enlisted sailor or Marine, fresh out of boot camp, will make $1169.10 in base pay per month,[123] which is taxable at both the federal and state levels. As these servicemembers are most often eighteen or nineteen-years-old, with little or no consumer credit history, they are typically not able to obtain car loans from automobile manufacturer finance companies, and are thus forced to contract with a finance company which will only grant credit at a much higher than market interest rate because the loans are considered "high risk." For servicemembers who live in low housing availability areas, such as San Diego, a car is necessary in order to get to work every day.[124]

Car dealerships located near military bases in the San Diego area prey upon the junior enlisted personnel, advertising in the base newspaper with such grabbers as: "Attention E-1 and Up,"[125] "No Credit, Bad Credit, Bankruptcy OK, Repos OK,"[126] offering "$10 down"[127] and inviting sailors and Marines to "call for a free ride to dealership."[128] During the period of March-August, 2000, a typical interest rate for a junior enlisted sailor at any of the used car dealerships or "iron lots"[129] in San Diego varied between 14.9% and 22%.[130] Even at a fair price most sailors will not be able to afford the

---

[123] *See* Defense Finance and Accounting Service, *2001 Monthly Basic Pay Table*, at http://www.dfas.mil. (last visited 6 Nov. 2000) (based on the basic pay for an E-2).
[124] Some of the military housing in San Diego is located over ten miles from the Naval Base in an area not serviced efficiently by public transportation.
[125] *See* NAVY COMPASS, Nov. 2, 2000, at 17.
[126] *See Id.* at 25.
[127] *See Id.* at 17.
[128] *See Id.* at 17.
[129] Interview with Supervising Investigator Joe Ney, California Department of Motor Vehicles Investigations and Audits Division, in San Diego, Cal. (November, 2000) (explaining that "iron lots" are used car lots that specialize in vehicles with salvage titles) [hereinafter Ney Interview].
[130] Various used car auto-loan contracts of file with the author.

principal and interest payments required under the contract. The reality is that used car dealerships commonly sell used cars at well above blue book value. To complicate matters further, junior enlisted personnel oftentimes lack the knowledge and life experience to be sophisticated consumers,[131] even where the required Federal Truth in Lending Act disclosures have been made.[132]

As is common throughout the industry, car dealerships located near military bases sell the executed contracts to finance companies who attach a security interest in the car as collateral,[133] then collect the payments. The finance charge constitutes the finance company's profit. Because many junior enlisted personnel have no credit or bad credit, they are often told they will be unable to secure financing through mainstream banking institutions and must therefore contract with lenders who finance "high risk" loans. This practice is predatory insofar as it is the car dealer who secures the financing for the buyer, often receiving a discount on the rate. This scheme deprives the unsophisticated military buyer of the ability to negotiate the best deal possible, because he or she has little or no control over the financing options.[134]

Because of a United States Supreme Court decision,[135] state usury laws,[136] where they exist, are ineffective in preventing this predatory practice of dealer secured "high risk" financing. In *Marquette National Bank of Minneapolis v. First Omaha Service Corp*, the Court, held that the under the National Bank Act,[137] a nationally chartered bank need only comply with the usury law of the state where the bank is located, not the state where a bank customer

---

[131] Interview with LT David A. Norkin, JAGC, USNR, a Navy Legal Assistance Attorney, in San Diego, Cal. (February 16, 2001.).
[132] 15 U.S.C. § 1601 (2001) (requiring sellers disclose: (1) identity of the creditor; (2) amount financed; (3) annual percentage rate; (4) finance charges; (5) payment schedule; (6) total payments; (7) late payment/prepayment penalties; (8) security interest; and (9) any demand features).
[133] *See* U.C.C. § 9-203 (2001).
[134] Ney Interview, *supra* note 130.
[135] *See* Marquette National Bank of Minneapolis v. First Omaha Service Corp, 439 U.S. 299 (1978).
[136] *See, e.g.*, CONN. GEN. STAT. § 37-4 (2001) (setting a maximum interest rate in the State of Conn. of 12% but exempting commercial lenders). California, like many other states, has no statutory maximum interest rate.
[137] 12 U.S.C. § 85 (2001).

resides.[138] Thus, many banks are physically sited in states which do not have a maximum interest rate, though they provide loans to consumers in all states.[139] In fact, shortly after the *Marquette* decision, the legislatures in Delaware and South Dakota abolished usury caps on credit card lending.[140] This sparked intense competition for credit card business among the states, and the results have been widespread interest rate deregulation, as well as a corresponding rise in consumer bankruptcy.[141]

To illustrate how ineffective state consumer protection laws are for dealer secured "high risk" financing, the First Circuit Court of Appeals confronted the "headlong collision between a state consumer protection law and a federal banking law" with respect to credit card fees.[142] In *Greenwood Trust Company v. Commonwealth of Massachusetts* the First Circuit addressed the "novel legal question: can a federally insured bank, chartered in Delaware, charge its Massachusetts credit card customers a late fee on delinquent accounts, notwithstanding a Massachusetts statute explicitly prohibiting the practice?"[143] The Court of Appeals reversed the District Court's decision holding the bank could not charge such fees, ruling that the federal banking laws preempt state consumer protection statutes.[144] The United States Supreme Court has also held that "interest" can include "late payment fees."[145]

---

[138] *See Marquette,* 439 U.S. 299. Justice Brennan noted that when the National Bank Act passed the House of Representatives in 1864, it imposed a uniform maximum interest rate of 7% and stated that "such a provision, of course, would have eliminated interstate inequalities among national banks resulting from differing state usury rates." *See Id.*, at 318, n.31.

[139] *See* David A. Moss and Gibbs A. Johnson, *The Rise of Consumer Bankruptcy: Evolution, Revolution, or Both?,* 73 AM. BANKR. L.J. 311 (Spring 1999). The authors note that the 1978 U.S. Supreme Court decision in *Marquette* was the beginning of interest rate deregulation on credit card interest rates. Further, the authors state "[t]his created an enormous incentive for credit card issuers to move their operations to states with high usury caps and for state legislatures to ease or eliminate their consumer-credit usury laws (so as to attract credit card companies)." [hereinafter Moss & Johnson]. *Id.* at 334.

[140] *See Id*. at 334.

[141] *See* Lawrence M. Ausubel, *Credit Card Defaults, Credit Card Profits, and Bankruptcy*, 71 AM. BANKR. L.J. 249 (Spring 1997) (noting that in 1996, credit card defaults exceeded 3.5 percent, the highest rate since 1973, and that personal bankruptcy filings rose 31% in the quarter ending in September 1996 as compared to the year before.).

[142] *See* Greenwood Trust Co. v. Commonwealth of Massachusetts, 971 F.2d 818, (1st Cir. 1992).

[143] *Id*. at 820.

[144] *See Id.*

[145] *See* Smiley v. Citibank, 517 U.S. 735 (1996).

Thus, it is clear that federal banking laws pre-empt state consumer protection statutes regarding interest rates on commercial loans and credit card fees. Therefore, if servicemembers are to have any interest or credit protection at all, it will have to come from Congress. Amending the SSCRA to allow servicemembers to cap all loans, not just pre-service loans, would, in effect, result in a federal usury law with respect to military members. Such a law would provide comprehensive protection for servicemembers' finances.

IV. Conclusion: Congressional legislative action is needed to prevent further erosion of SSCRA protections. An expansion of the existing protections would result in substantially improved military readiness.

Military members volunteer to serve the country's national security interests, oftentimes under arduous conditions and for lower pay than they could earn in the civilian sector.[146] The Federal Government, state governments, as well as commercial entities which profit from extending credit to military members, all share responsibility to adequately protect servicemembers financial affairs. To this end, Congress should amend the SSCRA to settle, once and for all, the disparate state and federal court interpretations of the SSCRA provisions discussed in this article. The tax provision should be modified to prevent states from wrongfully taxing the nonresident military member's income or taxing the servicemember's spouse at a higher rate in order to recoup some of the nonresident servicemember's income. Essential to any such amendment would be a clarification of the terms "domicile" and "residence," since the *Mitchell* standard has never been easy to apply with respect to nonresident servicemembers.

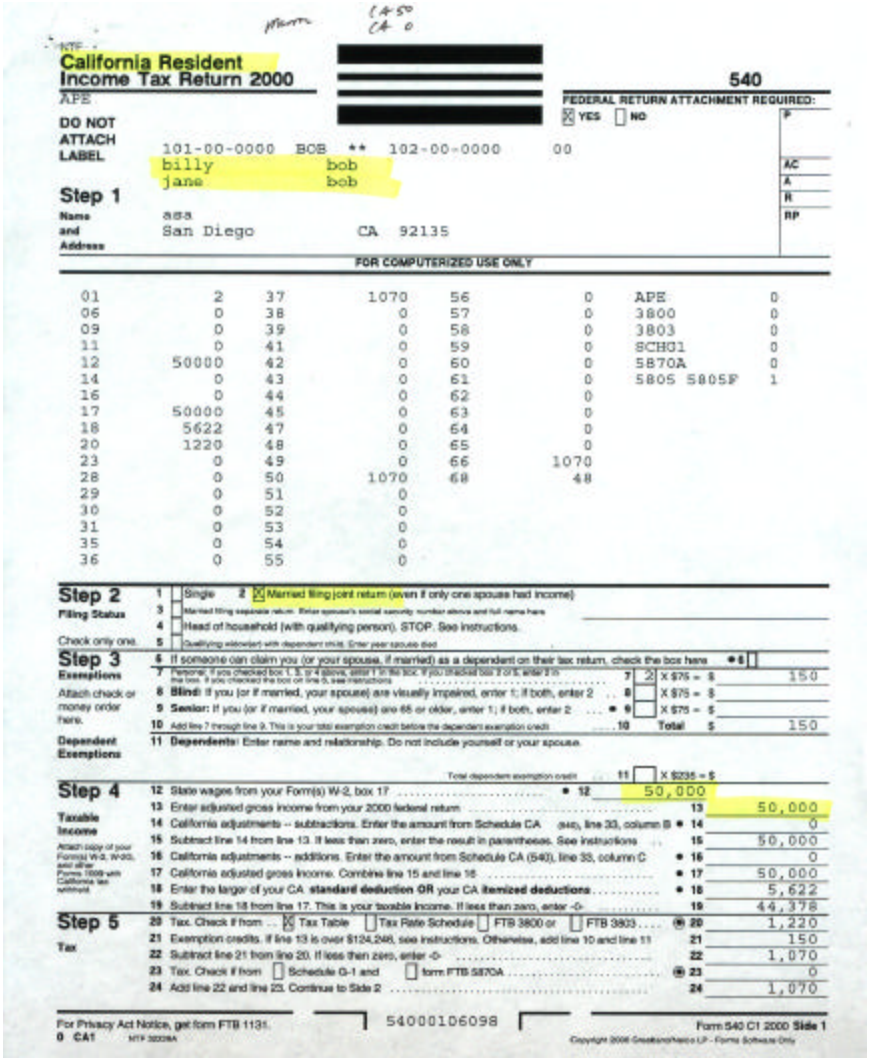
Congress should also act to clarify and expand the six-percent interest section, in order to promote recruiting and retention

[146] *See, e.g.*, James Dao, *Defense Dep't. Panel seeks Changes to Keep Military Personnel*, N.Y. TIMES, June 13, 2001, at A20 ("An advisory panel to Secretary of Defense Donald H. Rumsfeld said today that the military was losing too many of its experienced and skilled people because of low pay, poor housing and rigid retirement rules . . . ."). *See* Joe Haberstroh, *On the Waters; Coast Guard: Still "Always Ready"?*, NEWSDAY, N.Y., October 7, 2001, A31 ("[T]he Coast Guard, like other branches of the military, is having increasing difficulty retaining its more seasoned members. Low pay is the main reason, the Coast Guard has said.").

throughout the military. Allowing military members to cap pre-service federal student loans at six-percent would relieve some of the financial burden of substantial debt. Enacting the equivalent of a federal usury law, with respect to military members, would decrease predatory interest rate arrangements, particularly among junior enlisted personnel--the population most at risk for long-term credit ramifications from defaulting on high interest contracts. Put simply, when servicemembers and their families have interest rate protections, as well as access to courts to enforce private rights of action against creditors who refuse to abide by the law, military units will be better prepared to meet their missions.

Congress recognized, in 1864, that the government owed members of the armed forces a certain level of civil protection. Given that the national economy has expanded enormously in both gross domestic product and complexity, Congress should update and expand the Soldiers' and Sailors' Civil Relief Act's financial protection provisions to counteract federal, state and private sector targeting of military members and their military income. Given the recent court decisions in the area of state income taxation, strong, clear amendments to the SSCRA would provide the "Civil Relief" promised to the military by Congress.

Appendix A



California Resident Income Tax Return 2000

540

APE

[redacted]

FEDERAL RETURN ATTACHMENT REQUIRED: [X] YES [ ] NO

DO NOT ATTACH LABEL

101-00-0000 BOB ** 102-00-0000 00

billy bob

jane bob

Step 1 Name and Address

aaa

San Diego CA 92135

FOR COMPUTERIZED USE ONLY

01	2	37	1070	56	0	APE	0
06	0	38	0	57	0	3800	0
09	0	39	0	58	0	3803	0
11	0	41	0	59	0	SCH01	0
12	50000	42	0	60	0	5870A	0
14	0	43	0	61	0	5805 5805F	1
16	0	44	0	62	0		
17	50000	45	0	63	0		
18	5622	47	0	64	0		
20	1220	48	0	65	0		
23	0	49	0	66	1070		
28	0	50	1070	68	48		
29	0	51	0				
30	0	52	0				
31	0	53	0				
35	0	54	0				
36	0	55	0				

Step 2 Filing Status — Check only one.

1 [ ] Single 2 [X] Married filing joint return (even if only one spouse had income)

3 [ ] Married filing separate return. Enter spouse's social security number above and full name here.

4 [ ] Head of household (with qualifying person). STOP. See instructions.

5 [ ] Qualifying widow(er) with dependent child. Enter year spouse died.

Step 3 Exemptions — Attach check or money order here.

6 If someone can claim you (or your spouse, if married) as a dependent on their tax return, check the box here ● 6 [ ]

7 Persons. If you checked box 1, 2, or 4 above, enter 1 in the box. If you checked box 3 or 5, enter 2 in the box. If you checked the box on line 5, see instructions. 7 [2] X $75 = $ 150

8 **Blind:** If you (or if married, your spouse) are visually impaired, enter 1; if both, enter 2 8 [ ] X $75 = $

9 **Senior:** If you (or if married, your spouse) are 65 or older, enter 1; if both, enter 2 ● 9 [ ] X $75 = $

10 Add line 7 through line 9. This is your total exemption credit before the dependent exemption credit 10 Total $ 150

Dependent Exemptions

11 **Dependents:** Enter name and relationship. Do not include yourself or your spouse.

Total dependent exemption credit 11 [ ] X $235 = $

Step 4 Taxable Income — Attach copy of your Form(s) W-2, W-2G, and other Forms 1099 with California tax withheld.

12	State wages from your Form(s) W-2, box 17	● 12 50,000	
13	Enter adjusted gross income from your 2000 federal return	13	50,000
14	California adjustments -- subtractions. Enter the amount from Schedule CA (540), line 33, column B	● 14	0
15	Subtract line 14 from line 13. If less than zero, enter the result in parentheses. See instructions	15	50,000
16	California adjustments -- additions. Enter the amount from Schedule CA (540), line 33, column C	● 16	0
17	California adjusted gross income. Combine line 15 and line 16	● 17	50,000
18	Enter the larger of your CA **standard deduction OR** your CA **itemized deductions**	● 18	5,622
19	Subtract line 18 from line 17. This is your taxable income. If less than zero, enter -0-	19	44,378

Step 5 Tax

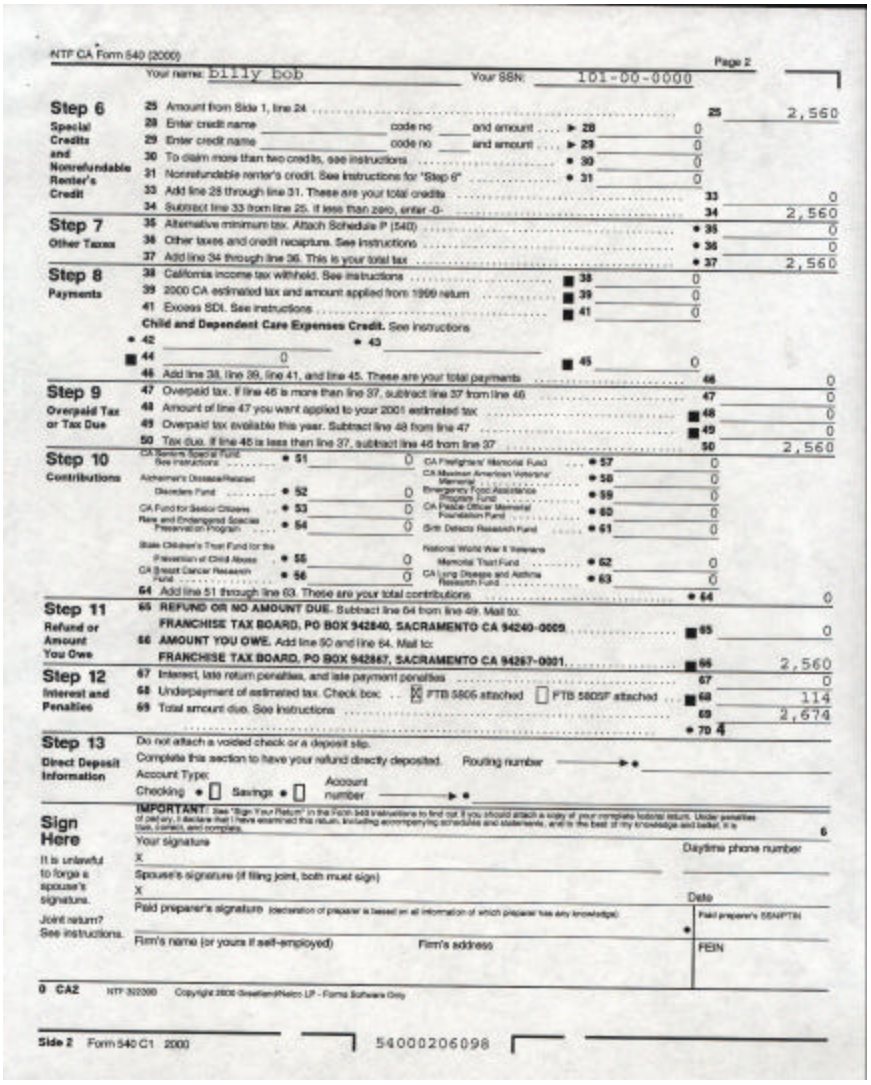
20	Tax. Check if from [X] Tax Table [ ] Tax Rate Schedule [ ] FTB 3800 or [ ] FTB 3803	● 20	1,220
21	Exemption credits. If line 13 is over $124,246, see instructions. Otherwise, add line 10 and line 11	21	150
22	Subtract line 21 from line 20. If less than zero, enter -0-	22	1,070
23	Tax. Check if from [ ] Schedule G-1 and [ ] form FTB 5870A	● 23	0
24	Add line 22 and line 23. Continue to Side 2	24	1,070

For Privacy Act Notice, get form FTB 1131.

0 CA1 MTF 32039A

54000106098

Form 540 C1 2000 **Side 1**



NTF CA Form 540 (2000) Page 2

Your name: billy bob Your SSN: 101-00-0000

Step 6 Special Credits and Nonrefundable Renter's Credit

25 Amount from Side 1, line 24 — 25: 2,560
28 Enter credit name _____ code no ____ and amount ▸ 28: 0
29 Enter credit name _____ code no ____ and amount ▸ 29: 0
30 To claim more than two credits, see instructions • 30: 0
31 Nonrefundable renter's credit. See instructions for "Step 6" • 31: 0
33 Add line 28 through line 31. These are your total credits — 33: 0
34 Subtract line 33 from line 25. If less than zero, enter -0- — 34: 2,560

Step 7 Other Taxes

35 Alternative minimum tax. Attach Schedule P (540) • 35: 0
36 Other taxes and credit recapture. See instructions • 36: 0
37 Add line 34 through line 36. This is your total tax • 37: 2,560

Step 8 Payments

38 California income tax withheld. See instructions ■ 38: 0
39 2000 CA estimated tax and amount applied from 1999 return ■ 39: 0
41 Excess SDI. See instructions ■ 41: 0
Child and Dependent Care Expenses Credit. See instructions
• 42 _____ • 43 _____
■ 44 0 ■ 45: 0
46 Add line 38, line 39, line 41, and line 45. These are your total payments — 46: 0

Step 9 Overpaid Tax or Tax Due

47 Overpaid tax. If line 46 is more than line 37, subtract line 37 from line 46 — 47: 0
48 Amount of line 47 you want applied to your 2001 estimated tax ■ 48: 0
49 Overpaid tax available this year. Subtract line 48 from line 47 ■ 49: 0
50 Tax due. If line 46 is less than line 37, subtract line 46 from line 37 — 50: 2,560

Step 10 Contributions

CA Seniors Special Fund. See instructions • 51: 0
Alzheimer's Disease/Related Disorders Fund • 52: 0
CA Fund for Senior Citizens • 53: 0
Rare and Endangered Species Preservation Program • 54: 0
State Children's Trust Fund for the Prevention of Child Abuse • 55: 0
CA Breast Cancer Research Fund • 56: 0
CA Firefighters' Memorial Fund • 57: 0
CA Museum American Veterans' Memorial • 58: 0
Emergency Food Assistance Program Fund • 59: 0
CA Police Officer Memorial Foundation Fund • 60: 0
Birth Defects Research Fund • 61: 0
National World War II Veterans Memorial Trust Fund • 62: 0
CA Lung Disease and Asthma Research Fund • 63: 0
64 Add line 51 through line 63. These are your total contributions • 64: 0

Step 11 Refund or Amount You Owe

65 **REFUND OR NO AMOUNT DUE.** Subtract line 64 from line 49. Mail to: **FRANCHISE TAX BOARD, PO BOX 942840, SACRAMENTO CA 94240-0005** ■ 65: 0
66 **AMOUNT YOU OWE.** Add line 50 and line 64. Mail to: **FRANCHISE TAX BOARD, PO BOX 942867, SACRAMENTO CA 94267-0001** ■ 66: 2,560

Step 12 Interest and Penalties

67 Interest, late return penalties, and late payment penalties — 67: 0
68 Underpayment of estimated tax. Check box: ☒ FTB 5806 attached ☐ FTB 5805F attached ■ 68: 114
69 Total amount due. See instructions — 69: 2,674
• 70 4

Step 13 Direct Deposit Information

Do not attach a voided check or a deposit slip.
Complete this section to have your refund directly deposited. Routing number ▸•
Account Type: Checking • ☐ Savings • ☐ Account number ▸•

Sign Here

IMPORTANT: See "Sign Your Return" in the Form 540 instructions to find out if you should attach a copy of your complete federal return. Under penalties of perjury, I declare that I have examined this return, including accompanying schedules and statements, and to the best of my knowledge and belief, it is true, correct, and complete. 6

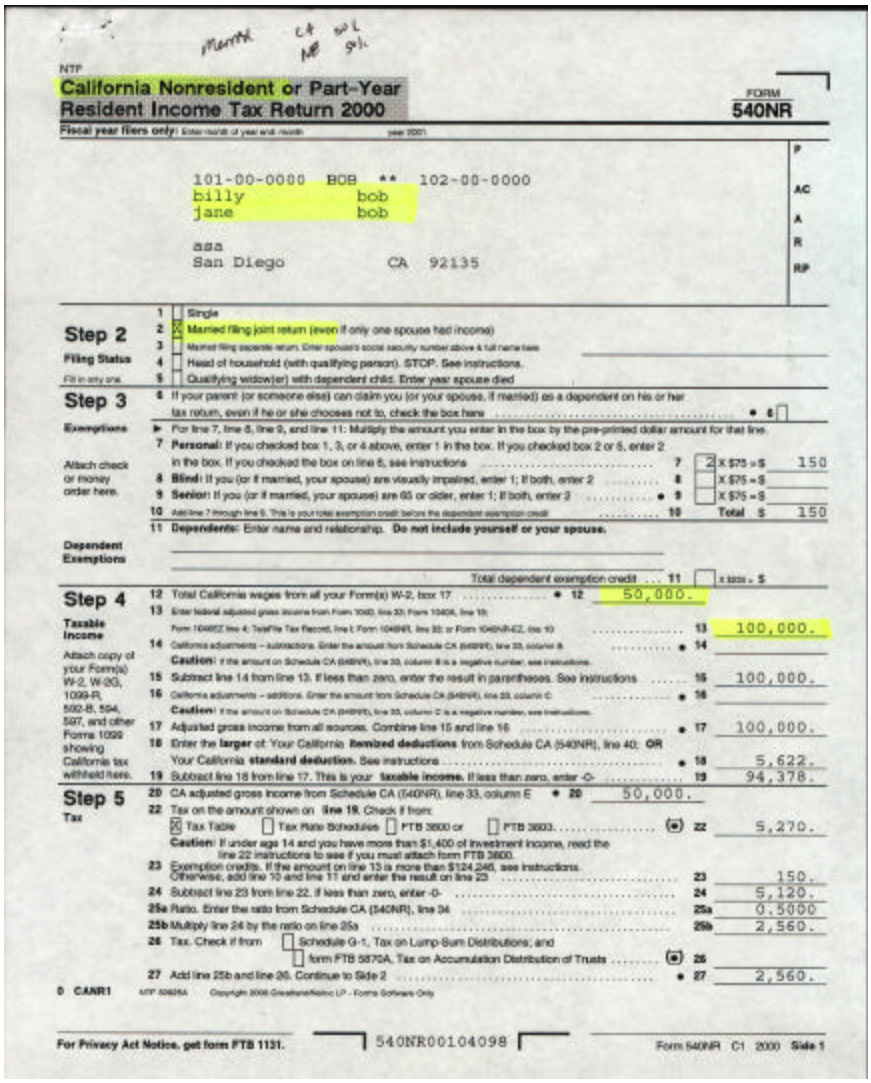
It is unlawful to forge a spouse's signature.

Your signature — Daytime phone number
X
Spouse's signature (if filing joint, both must sign) — Date
X
Paid preparer's signature (declaration of preparer is based on all information of which preparer has any knowledge) — Paid preparer's SSN/PTIN •
Joint return? See instructions.
Firm's name (or yours if self-employed) — Firm's address — FEIN

0 CA2 NTF 322000 Copyright 2000 Greatland/Nelco LP - Forms Software Only

Side 2 Form 540 C1 2000 54000206098

Appendix B



NTP

California Nonresident or Part-Year Resident Income Tax Return 2000

FORM **540NR**

Fiscal year filers only: Enter month of year end: month ____ year 2001

101-00-0000 BOB ** 102-00-0000
billy bob
jane bob

aaa
San Diego CA 92135

P
AC
A
R
RP

Step 2 Filing Status Fill in only one.

1 ☐ Single
2 ☒ Married filing joint return (even if only one spouse had income)
3 ☐ Married filing separate return. Enter spouse's social security number above & full name here.
4 ☐ Head of household (with qualifying person). STOP. See instructions.
5 ☐ Qualifying widow(er) with dependent child. Enter year spouse died

Step 3 Exemptions

Attach check or money order here.

6 If your parent (or someone else) can claim you (or your spouse, if married) as a dependent on his or her tax return, even if he or she chooses not to, check the box here ☐ 6
▶ For line 7, line 8, line 9, and line 11: Multiply the amount you enter in the box by the pre-printed dollar amount for that line.
7 **Personal:** If you checked box 1, 3, or 4 above, enter 1 in the box. If you checked box 2 or 5, enter 2 in the box. If you checked the box on line 6, see instructions 7 [2] X $75 = $ 150
8 **Blind:** If you (or if married, your spouse) are visually impaired, enter 1; if both, enter 2 8 [ ] X $75 = $
9 **Senior:** If you (or if married, your spouse) are 65 or older, enter 1; if both, enter 2 9 [ ] X $75 = $
10 Add line 7 through line 9. This is your total exemption credit before the dependent exemption credit 10 Total $ 150

Dependent Exemptions

11 **Dependents:** Enter name and relationship. **Do not include yourself or your spouse.**

Total dependent exemption credit 11 [ ] X $309 = $

Step 4 Taxable Income

Attach copy of your Form(s) W-2, W-2G, 1099-R, 592-B, 594, 597, and other Forms 1099 showing California tax withheld here.

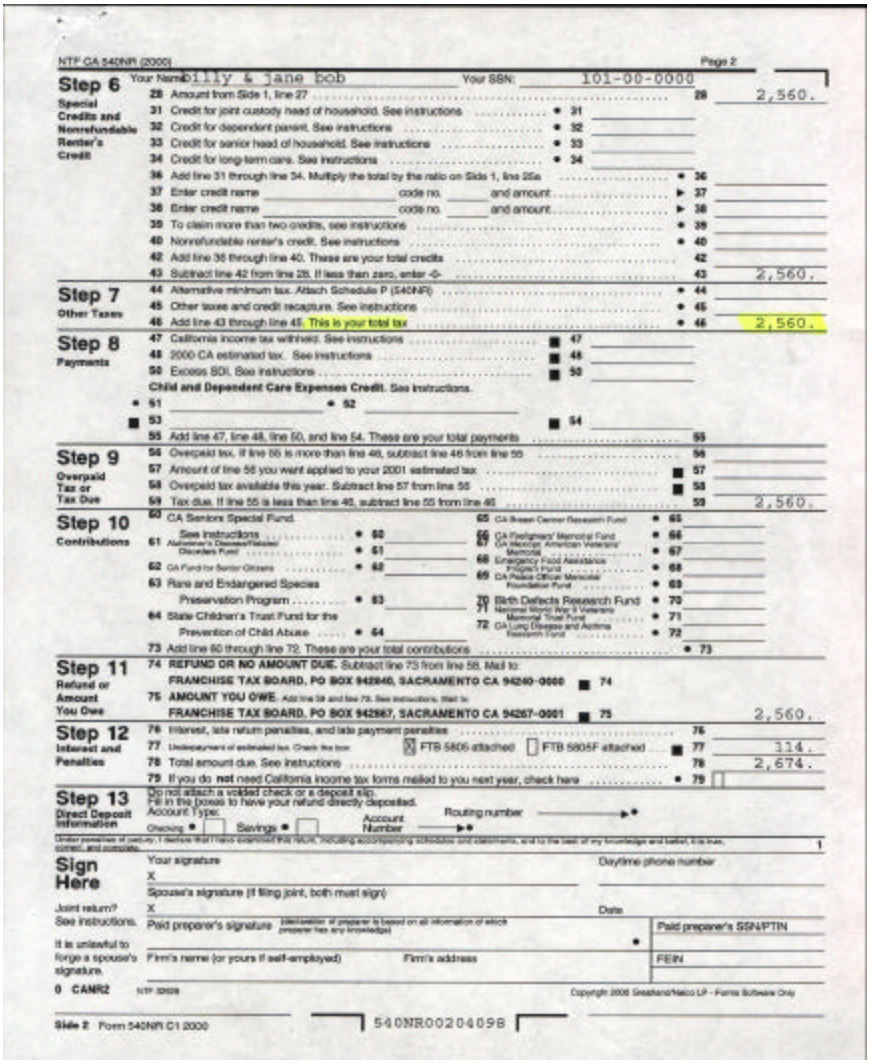
12 Total California wages from all your Form(s) W-2, box 17 12 50,000.
13 Enter federal adjusted gross income from Form 1040, line 33; Form 1040A, line 19; Form 1040EZ line 4; TeleFile Tax Record, line L; Form 1040NR, line 33; or Form 1040NR-EZ, line 10 13 100,000.
14 California adjustments – subtractions. Enter the amount from Schedule CA (540NR), line 33, column B 14
Caution: If the amount on Schedule CA (540NR), line 33, column B is a negative number, see instructions.
15 Subtract line 14 from line 13. If less than zero, enter the result in parentheses. See instructions 15 100,000.
16 California adjustments – additions. Enter the amount from Schedule CA (540NR), line 33, column C 16
Caution: If the amount on Schedule CA (540NR), line 33, column C is a negative number, see instructions.
17 Adjusted gross income from all sources. Combine line 15 and line 16 17 100,000.
18 Enter the **larger** of: Your California **itemized deductions** from Schedule CA (540NR), line 40; **OR** Your California **standard deduction.** See instructions 18 5,622.
19 Subtract line 18 from line 17. This is your **taxable income.** If less than zero, enter -0- 19 94,378.

Step 5 Tax

20 CA adjusted gross income from Schedule CA (540NR), line 33, column E 20 50,000.
22 Tax on the amount shown on **line 19.** Check if from: ☒ Tax Table ☐ Tax Rate Schedules ☐ FTB 3800 or ☐ FTB 3803. (e) 22 5,270.
Caution: If under age 14 and you have more than $1,400 of investment income, read the line 22 instructions to see if you must attach form FTB 3800.
23 Exemption credits. If the amount on line 13 is more than $124,246, see instructions. Otherwise, add line 10 and line 11 and enter the result on line 23 23 150.
24 Subtract line 23 from line 22. If less than zero, enter -0- 24 5,120.
25a Ratio. Enter the ratio from Schedule CA (540NR), line 34 25a 0.5000
25b Multiply line 24 by the ratio on line 25a 25b 2,560.
26 Tax. Check if from ☐ Schedule G-1, Tax on Lump-Sum Distributions; and ☐ form FTB 5870A, Tax on Accumulation Distribution of Trusts (e) 26
27 Add line 25b and line 26. Continue to Side 2 27 2,560.

0 CANR1 MTP 50626A

For Privacy Act Notice, get form FTB 1131. 540NR00104098 Form 540NR C1 2000 Side 1



NTF CA 540NR (2000) Page 2

Step 6 Special Credits and Nonrefundable Renter's Credit

Your Name billy & jane bob Your SSN: 101-00-0000

28	Amount from Side 1, line 27		2,560.
31	Credit for joint custody head of household. See instructions	• 31	
32	Credit for dependent parent. See instructions	• 32	
33	Credit for senior head of household. See instructions	• 33	
34	Credit for long-term care. See instructions	• 34	
36	Add line 31 through line 34. Multiply the total by the ratio on Side 1, line 28a	• 36	
37	Enter credit name _____ code no. ____ and amount	▶ 37	
38	Enter credit name _____ code no. ____ and amount	▶ 38	
39	To claim more than two credits, see instructions	• 39	
40	Nonrefundable renter's credit. See instructions	• 40	
42	Add line 36 through line 40. These are your total credits	42	
43	Subtract line 42 from line 28. If less than zero, enter -0-	43	2,560.

Step 7 Other Taxes

44	Alternative minimum tax. Attach Schedule P (540NR)	• 44	
45	Other taxes and credit recapture. See instructions	• 45	
46	Add line 43 through line 45. This is your total tax	• 46	2,560.

Step 8 Payments

47	California income tax withheld. See instructions	■ 47	
48	2000 CA estimated tax. See instructions	■ 48	
50	Excess SDI. See instructions	■ 50	
	Child and Dependent Care Expenses Credit. See instructions.		
• 51	• 52		
■ 53		■ 54	
55	Add line 47, line 48, line 50, and line 54. These are your total payments	55	

Step 9 Overpaid Tax or Tax Due

56	Overpaid tax. If line 55 is more than line 46, subtract line 46 from line 55	56	
57	Amount of line 56 you want applied to your 2001 estimated tax	■ 57	
58	Overpaid tax available this year. Subtract line 57 from line 56	■ 58	
59	Tax due. If line 55 is less than line 46, subtract line 55 from line 46	59	2,560.

Step 10 Contributions

60	CA Seniors Special Fund. See instructions	• 60	65	CA Breast Cancer Research Fund	• 65
61	Alzheimer's Disease/Related Disorders Fund	• 61	66	CA Firefighters' Memorial Fund	• 66
62	CA Fund for Senior Citizens	• 62	67	CA Medal of Honor/American Veterans' Memorial	• 67
63	Rare and Endangered Species Preservation Program	• 63	68	Emergency Food Assistance Program Fund	• 68
64	State Children's Trust Fund for the Prevention of Child Abuse	• 64	69	CA Police Officer Memorial Foundation Fund	• 69
			70	Birth Defects Research Fund	• 70
			71	National World War II Veterans Memorial Trust Fund	• 71
			72	CA Lung Disease and Asthma Research Fund	• 72
73	Add line 60 through line 72. These are your total contributions				• 73

Step 11 Refund or Amount You Owe

74	**REFUND OR NO AMOUNT DUE.** Subtract line 73 from line 59. Mail to: **FRANCHISE TAX BOARD, PO BOX 942840, SACRAMENTO CA 94240-0000**	■ 74	
75	**AMOUNT YOU OWE.** Add line 59 and line 73. See instructions. Mail to: **FRANCHISE TAX BOARD, PO BOX 942867, SACRAMENTO CA 94267-0001**	■ 75	2,560.

Step 12 Interest and Penalties

76	Interest, late return penalties, and late payment penalties	76	
77	Underpayment of estimated tax. Check the box: ☒ FTB 5806 attached ☐ FTB 5805F attached	■ 77	114.
78	Total amount due. See instructions	78	2,674.
79	If you do **not** need California income tax forms mailed to you next year, check here	• 79 ☐	

Step 13 Direct Deposit Information

Do not attach a voided check or a deposit slip.
Fill in the boxes to have your refund directly deposited.
Account Type: Checking • ☐ Savings • ☐ Routing number ▶• Account Number ▶•

Under penalties of perjury, I declare that I have examined this return, including accompanying schedules and statements, and to the best of my knowledge and belief, it is true, correct, and complete. 1

Sign Here

Your signature X Daytime phone number

Spouse's signature (if filing joint, both must sign) X Date

Joint return? See instructions.

Paid preparer's signature (declaration of preparer is based on all information of which preparer has any knowledge) • Paid preparer's SSN/PTIN

It is unlawful to forge a spouse's signature.

Firm's name (or yours if self-employed) Firm's address FEIN

0 CANR2 NTF 32428

Side 2 Form 540NR C1 2000 540NR00204098

LOSS OF NUMBERS

Eugene R. Fidell* **and Jay M. Fidell****

Until 1999, when President Clinton abolished it, "loss of numbers" was a permissible court-martial sentence in the sea services. Although this historical footnote may appear at first glance to be little more than some "inside baseball" for military lawyers, in fact it is highly pertinent in the conversation now taking place in naval circles and elsewhere about accountability. Abolition of loss of numbers is one of those events that seem inconsequential at the time but later prove either to be or to reflect trends of far greater significance. There is no shortage of these events in the military justice context.

One example, familiar only to the cognoscenti, is an obscure 1990 amendment to the Uniform Code of Military Justice. The Code originally provided that judges of the United States Court of Military Appeals[1] (known since 1994 as the United States Court of Appeals for the Armed Forces) had to be "appointed from civilian life."[2] Starting in 1956, the term "civil life" was used,[3] but in 1990, to remove any doubt in connection with a then-existing vacancy, Congress not only changed "civil" back to "civilian" but also made its meaning crystal clear by expressly stating that persons who are retired from the armed forces after 20 or more years of active service (whether or not on the retired list) are not considered to be in civilian life for the purpose of eligibility for appointment.[4] The implications of that clause have yet to be fully explored, but they certainly have to do with the extent to which military justice

---

* *Lieutenant Commander, U.S. Coast Guard Reserve (Retired); President, National Institute of Military Justice; Partner, Feldesman, Tucker, Leifer, Fidell & Bank LLP, Washington, D.C. The positions and opinions stated in this article are those of the authors and do not represent the views of the United States Government, the Department of Defense, the Department of Transportation, or the United States Navy.*

** *Lieutenant Commander, U.S. Coast Guard Reserve (Retired); Partner, Bendet, Fidell, Sakai & Lee, Honolulu, Hawaii.*

This article was initially published, in abbreviated form, as Loss of Numbers was a Punishment, 127 Nav. Inst. Proc. 72 (Aug. 2001).

[1] On Oct. 5, 1994, the National Defense Authorization Act for fiscal year 1995, Pub. L. No. 103-337, 108 Stat. 2663 (1994), renamed the United States Court of Military Appeals the United States Court of Criminal Appeals for the Armed Forces (the CAAF).

[2] Act of May 5, 1950, 64 Stat. 129 (1950), UCMJ art. 67(a)(1).

[3] Act of Aug. 10, 1956, ch. 1041, § 1, 70A Stat. 60 (art. 67(a)(1)); Act of Nov. 29, 1989, 103 Stat. 1570 (UCMJ art. 142(b)(1)).

[4] National Defense Authorization Act for Fiscal Year 1991, Pub. L. No. 101-510, § 541(f), 104 Stat. 1485, 1565 (1990); UCMJ arts. 142(b)(1), -(4).

is distinct from civilian criminal justice, and whether a basically civilian appellate orientation is a good idea, a bad idea, or necessary to the sound elaboration of military jurisprudence and the need to foster public confidence in the administration of military justice.

A second example of obscure action with potent symbolic and practical implications is Congress' repeal, in the same 1990 legislation, of the part of Article 36(b) that had long required changes to the MANUAL FOR COURTS-MARTIAL to be submitted to the Senate and House Armed Services Committees.[5] The repeal was explained as a paperwork reduction measure, thus suggesting that no useful purpose had been served by bringing MANUAL changes to the attention of the committees through which Congress exercises its constitutional authority to "make Rules for the Government and Regulation of the land and naval Forces."[6] The amendment has been noted with alarm as an erosion of meaningful civilian oversight,[7] but there is no evidence that Congress has been disposed to revisit the issue.

The most recent example of these obscure but important actions occurred in 1999. Tucked away in that year's changes to the MANUAL FOR COURTS-MARTIAL[8] was an amendment deleting Rule for Courts-Martial 1003(b)(4), which had been the basis for the court-martial punishment of loss of numbers.[9] Although loss of numbers had once been a permissible punishment even in the Army, it was rarely used by that service,[10] and from the beginning of the UCMJ era it was applicable only in the Navy, Marine

---

[5] National Defense Authorization Act for Fiscal Year 1991, Pub. L. No. 101-510, § 1301(4), 104 Stat. 1485, 1668 (1990).

[6] U.S. Const. art. I, § 8, cl. 14.

[7] Kevin J. Barry, *Modernizing the MANUAL FOR COURTS-MARTIAL Rule-Making Process: A Work in Progress*, 165 MIL. L. REV. 237, 266 n.109, 274 n.143 (2000); Eugene R. Fidell, *Going on Fifty: Evolution and Devolution in Military Justice*, 32 WAKE FOREST L. REV. 1213, 1216 n.12 (1997) ("The power to repudiate a MANUAL provision has never been exercised, and indeed, it appears that the responsible committees of Congress have never played a significant role with respect to oversight of the President's power under UCMJ art. 36(b)."). Eugene R. Fidell, *Judicial Review of Presidential Rulemaking Under Article 36: The Sleeping Giant Stirs*, 4 MIL. L. RPTR. 6049, 6058 (1976).

[8] Exec. Order No. 13,140, § 1(e)(1), 64 Fed. Reg. 55,115 (Oct. 6, 1999).

[9] MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 1003(b)(4) (1998 ed.) [hereinafter MCM] had read: "*Loss of numbers, lineal position, or seniority*. These punishments are authorized only in cases of Navy, Marine Corps, and Coast Guard officers[.]" The accompanying official "Discussion" was equally terse: "All losses of numbers will be numbers in the appropriate lineal list." MCM *supra* (1998 ed.), at II-125. The 1999 Executive Order renumbered the balance of R.C.M. 1003(b), so there remains an R.C.M. 1003(b)(4), but the text is simply that previously found in R.C.M. 1003(b)(5). *See* MCM *supra* (2000 ed.) at II-126.

[10] WILLIAM WINTHROP, MILITARY LAW AND PRECEDENTS 414 (2d ed. 1920, repr. 1979).

Corps and Coast Guard.[11] As a cultural matter it had become quintessentially a sea services punishment, like "bread and water."[12] The cases bear this out: while occasionally adjudged in shoreside settings,[13] loss of numbers had a distinctly nautical ring. Indeed, while its use was not so limited,[14] it probably had come to be associated above all with crimes of command, such as hazarding a vessel or related derelictions.

Among those who suffered this punishment were Captain Edward L. Beach (father of the author of RUN SILENT, RUN DEEP), who was sentenced to a loss of 20 numbers while commanding USS MEMPHIS (CL-13) in 1916. (The Secretary of the Navy later reduced the sentence to loss of five numbers.) Commanding officers of USS INDIANAPOLIS (CA-35), USS MISSOURI (BB-63), USS BASILONE (DDE-824), USCGC WINNEBAGO (WPG-40), USCGC OWASCO (WHEC-39), USCGC CUYAHOGA (WIX-157) and USCGC MESQUITE (WLB-305) all lost numbers as well, although in the last cited incident the conviction was overturned on appeal and the captain wound up at admiral's mast.[15] The executive officer of USS PRESTIGE (MSO-465) lost numbers after a 1958 grounding, but this was set aside because the commanding officer had been acquitted. Loss of numbers certainly had a lot of history behind it. That history reflected a set of expectations based not so much on selection boards painstakingly comparing fitness reports as on a more mechanical process by which senior officers would more or less inexorably advance upwards through the list as the grim reaper created vacancies around and—better yet—above them.

---

[11] MCM *supra* note 9 (1951), ¶ 126*i*; MCM *supra* note 9 (1969) (rev.), ¶ 126*i*. Loss of *seniority*, as opposed to loss of *numbers*, was not a permissible punishment in the Coast Guard. United States v. Albritton, 30 C.M.R. 750 (Treas. Gen. Counsel 1961).

[12] *See* MCM *supra* note 9, pt. V, ¶ 5.c.(5) (2000) (authorizing confinement on bread and water or diminished rations at non-judicial punishment proceedings conducted under UCMJ art. 15). *See also* DEP'T OF THE NAVY, MANUAL OF THE JUDGE ADVOCATE GENERAL § 0111.C (directing that confinement on bread and water may not be imposed on persons in pay grade E-4 or above). Confinement on bread and water is not an authorized court-martial punishment. *See* MCM *supra* note 9, R.C.M. 1003(b) (2000) (listing authorized court-martial punishments).

[13] *See, e.g.*, United States v. Boudreaux, 33 M.J. 649, 650 (N.M.C.M.R. 1991) (en banc), *aff'd*, 35 M.J. 291, 292 (1992), *cert. denied*, 507 U.S. 952 (1993).

[14] *See, e.g.*, United States v. Robinson, 1991 CMR LEXIS 429, No. 90-3103 (N.M.C.M.R. Mar. 15, 1991) (per curium) (referring to a loss of numbers as part of the sentence that was awarded to a disbursing officer who conspired with a ship's disbursing clerk in a bogus advance pay scheme).

[15] The sentence in the *Mesquite* case could not have been fully implemented in any event because officers are carried on the active duty promotion list in order of date of rank and seniority and there is no authority to change a regular officer's date of rank. It was therefore determined that the sentence could be executed only to the extent that the accused would become the most junior of those lieutenant commanders with his date of rank.

Despite the Navy's tradition of resistance to military justice reforms,[16] abolition of loss of numbers is one it affirmatively sought. Why did it do so? The explanation included in the Joint Service Committee's 1997 notice of proposed rulemaking identified no pressing need for action. Rather, it treated the matter as simply clearing away a provision that was misunderstood and served little purpose:

> Although loss of numbers had the effect of lowering precedence for some purposes, e.g., quarters priority, board and court seniority, and actual date of promotion, loss of numbers did not affect the officer's original position for purposes of consideration for retention or promotion. Accordingly, this punishment was deleted because of its negligible consequences and the misconception that it was a meaningful punishment.[17]

Was this a valid reason? One of the leading treatises makes you wonder. It indicates that loss of numbers generally "adversely affected the officer in terms of obtaining quarters *and in actual promotion in rank*."[18] The National Institute of Military Justice commented: "While NIMJ intuitively agrees that this traditional punishment can now be dispensed with, we would feel more confident on this score if data on the actual imposition of loss of numbers were made available."[19] Subsequently released internal records show that the Bureau of Naval Personnel had already estimated that there were one or two loss of numbers cases per year,[20] but that estimate was not made known to the public at the time, and the proposal continued to wend its way through the protracted Executive Branch approval process. In the ensuing few years no

---

[16] *See generally* JAMES E. VALLE, ROCKS & SHOALS: ORDER AND DISCIPLINE IN THE OLD NAVY 1800-1861, 277 (1980).

[17] Notice of Proposed Amendments to the MANUAL FOR COURTS-MARTIAL, 62 Fed. Reg. 24,640, 24,642 (May 6,1997).

[18] DAVID A. SCHLUETER, MILITARY CRIMINAL JUSTICE: PRACTICE AND PROCEDURE § 16-3(F), at 727 (5th ed. 2000) (emphasis added). For example, even the loss of numbers Captain Beach, Sr. suffered made it unlikely he would ever attain flag rank.

[19] Letter from Captain Kevin J. Barry, USCG (Ret), National Institute of Military Justice [hereinafter "NIMJ"], to Lieutenant Colonel Paul Holden, Jr., JA, USA, Joint Service Comm. on Military Justice, at 6 (Jul.10, 1997) (on file with authors).

[20] DEP'T OF THE NAVY, OFFICE OF THE JUDGE ADVOCATE GENERAL, REPORT OF THE PROCESS ACTION TEAM ON IMPROVING MILITARY JUSTICE LEGAL PROCESSES, 70 (Mar. 15, 1996) (The authors wish to thank the Joint Service Committee on Military Justice for affording us access to this information.).

one has sought to reinstate loss of numbers as a court-martial punishment. Indeed, scarcely anyone has even noticed the change.

Were we all too casual? Is abolition of loss of numbers more important than we thought? For one thing, it brought the services a notch closer for military justice purposes, making the Uniform Code that much more uniform.[21] For another, it put less daylight between the punishment powers of a court-martial and those of a flag officer in command. Since, especially for crimes of command, dismissal or brig time are highly unlikely to be adjudged in a court-martial, and since involuntary separation can be effected through a board of officers (unless the offender chooses to retire or otherwise "go quietly"), abolition of loss of numbers means that essentially the same sanctions—notably, letters of reprimand—can be imposed at admiral's mast as are likely to emerge from a court-martial.

The net effect of abolition, therefore, coupled with the rise of administrative measures such as removal from promotion lists, detachment for cause, retirement grade determinations, and the like, seems to be either to mark or to accelerate the demise of the general court-martial as the forum of choice for the administration of justice in cases involving crimes of command by naval officers.

This evolution may make sense, but it is worth pondering since it is not without cost. It entails a rejection of the court-martial apparatus with all of its highly-touted protections for the individual (proof beyond a reasonable doubt, cross-examination of witnesses, "blue ribbon" juries, resolution of legal issues by a trained judiciary, to name a few) that have been developed especially over the last 50 years,[22] as well as loss of the incalculable benefit of increased public confidence that justice has been done. Shifting a category of cases from the trial forum to a command-focused forum of, if anything, even greater antiquity, seems anomalous. Moreover, shifting to what may seem a more lenient forum a category of cases in which the accused is always an officer can be expected to generate consternation among enlisted personnel, not to mention the public. A court-martial can still reduce an enlisted member's pay grade; it can no longer even reduce an officer's seniority *within* a pay grade. The separate disciplinary treatment of officers and enlisted

[21] *Cf.* United States v. Rencher, 1998 CCA LEXIS 151, ACM 32655, (A.F. Ct. Crim. App. Feb. 20, 1998) *review denied*, 50 M.J. 214 (1998) (citing loss of numbers as illustration of how the services' "separate and diverse missions . . . dictate different needs and emphases on the many facets of good order and disciplin[e]").
[22] The UCMJ took effect on May 31, 1951.

personnel has become a little more separate, and crimes of command have seemingly been decriminalized, the UCMJ notwithstanding.

Beyond all these considerations lies the loss of something even more elusive. The Joint Service Committee's explanation for abolition was right on a certain level: loss of numbers had become virtually a museum piece. It was essentially a 19th or even an 18th century sanction struggling to survive in a 21st century Navy. It had a certain anachronistic quality that tied the naval present to the naval past. Indeed, it also had an unmistakably ritualistic ring to it, like the old requirement that holiday colors be displayed when a general court-martial was in session. Even today, precise seniority has consequences at every turn, not simply for deciding who gets to be president of a court or board or who gets which quarters, but also, which ship renders passing honors and who salutes whom. Issues of seniority continue to pervade naval life. At the risk of sounding like old fogies, given all this, were we too hasty in throwing loss of numbers over the side? Will we one-day regret having done so?

CIVILIANS IN WAR

edited by Simon Chesterman
Lynne Reinner Publishers, London, 2001[1]

Laurie R. Blank[2]

Ninety percent of all casualties in conflicts in the 1990s were civilians, predominantly women and children. In contrast, only 5 percent of all casualties in World War I were civilians, a number that grew to 50 percent in World War II. This staggering increase in the devastation war brings upon civilian populations has led to new efforts to promote adherence to international humanitarian law in both international and internal armed conflicts. Early codifications of international humanitarian law, including the Hague Conventions of 1899 and 1907, sought to relieve the suffering of war by regulating the conduct of combatants and paid little, if any, attention to the protection of civilians. In the aftermath of the "total war" of World War II and its catastrophic effects on civilians, the 1949 Geneva Conventions included provisions for the protection of civilians, notably the Fourth Geneva Convention on the Protection of Civilians in War. Despite this growing understanding of the need to protect civilians in times of armed conflict, the norms and rules codified in that document have not stemmed the tide of atrocities against civilians. Just as international humanitarian law evolved in 1949 in response to the nature of war in the early 20th century, so international humanitarian law must now evolve to meet the new challenges arising out of late 20th century conflict.

---

[1] *Civilians in War* is a project of the International Peace Academy.

[2] *Laurie R. Blank (B.A. Princeton University, 1993; M.A. The Johns Hopkins University Paul H. Nitze School of Advanced International Studies, 1995; J.D. New York University Law School, 1998) is a Program Officer in the Rule of Law Program at the United States Institute of Peace in Washington, D.C.*

Civilians in War provides an important analytical framework for understanding the tools that international and national actors can use to protect civilians from the horrors of war and demonstrates the need to reinvigorate international humanitarian law in response to the changing face of war. Incorporating the work of academics, field practitioners and policymakers from the humanitarian, legal and security arenas, this edited volume focuses on how to use existing principles and practices of international humanitarian law to their fullest in order to offer the most effective protection to civilians in times of war. This book is a highly useful resource for anyone working in the fields of humanitarian assistance, protection and international law and offers a well-developed examination of the challenges today's conflicts pose for those who seek to protect civilians from the ravages of war.

Part One examines the changing concept of belligerents in an attempt to understand how international humanitarian law has evolved in its treatment of and distinction between combatants and civilians. In the first chapter, Karma Nabulsi traces the evolution of the concepts of belligerents and civilians from the Hague Conventions, which made the first distinction between belligerents and civilians, to the Geneva Conventions, which recognized civilians as a distinct category in international law for the first time and granted privileges on the basis of civilian status. Analyzing the complex relationship between combatants and civilians also offers insight into why belligerents commit violations of the laws of war and can help the international community to improve protection of civilians and prevention of atrocities. Guy Lamb uses the conflicts in Namibia and Angola as case studies for the analysis of this question in the second chapter. He identifies four primary factors that contributed to or allowed the commission of atrocities in these conflicts: the isolation of the conflict areas from the world's attention, such that little human rights monitoring and media coverage took place; economic interests that motivated belligerents to prolong the conflict; a culture of impunity and, in some cases, even rewarding individuals for the commission of abuses; and the general lack of accountability on the part of the leadership. At present, few mechanisms exist to encourage or compel belligerent groups to comply with international humanitarian law, especially in their treatment of civilians. Lamb's analysis of why atrocities take place provides a foundation for the development of mechanisms targeted at improving such compliance in the future.

In Part Two, *Civilians in War* addresses possible means for inducing compliance with norms of international humanitarian law by belligerent groups and considers possible incentives for belligerents to respect civilians' rights. In an extremely interesting chapter, Marie-Joëlle Zahar examines the factors

shaping the relationships between belligerents and civilians in conflict regions in order to seek ways to alleviate humanitarian crises and encourage belligerent groups to abide by basic legal principles. The two primary factors are the degree of identification between the belligerents and the civilians and the nature of the economic relations between the two groups. For example, the higher the identification between the belligerents and the civilians, the less likely the belligerents are to harm the civilian population. Similarly, the more the belligerents depend on the civilians economically, the less likely they are to harm the civilians. Zahar then analyzes possible approaches to belligerents in seeking to induce compliance with humanitarian law, depending on where the belligerent-civilian relations fall along her typology: engage the belligerents on humanitarian issues; identify constraints on the use of coercion; use economic arguments to humanitarian ends; and "pull the economic plug" on the belligerents. The following three chapters discuss practical efforts to achieve compliance without force. In the fourth chapter, Pierre Gassman discusses the international community's efforts to engage with belligerents in Colombia on questions of humanitarian law. After a useful discussion of the efforts of the International Committee of the Red Cross (ICRC) to address the needs of the Colombian population, he analyzes the attitudes of the different parties to the conflict toward the ICRC's activities and international humanitarian law. William O'Neill evaluates the different mechanisms the United Nations has at its disposal for ensuring compliance with international humanitarian law in the fifth chapter, in particular the human rights field operation. An analysis of the International Civilian Mission in Haiti, as well as similar operations in Rwanda, Bosnia and Herzegovina, Angola and Sierra Leone, demonstrates that the focus on human rights has shifted from Geneva-based mechanisms to operations on the ground and efforts to strengthen local organizations that can sustain the necessary reporting, oversight and investigation. Finally, the sixth chapter addresses questions of war cleansing and other indigenous rituals that seek to protect children in times of armed conflict. Using examples of children living on the front lines in Mozambique and Angola and the rituals used to cleanse them after participation in conflict, Alcinda Honwana argues for a bottom-up approach to protecting children and enforcing their humanitarian rights.

Part Three focuses on using both legal and military means to enforce compliance with international legal norms. International criminal law as a tool for enforcement is the subject of the seventh and eighth chapters. First, Simon Chesterman offers a useful discussion of the evolution of international criminal law from the Nuremberg trials through the International Criminal Tribunals for the former Yugoslavia and Rwanda and the adoption of the Rome Statute of the International Criminal Court in 1998. He then tackles the more complex

issue of the range of different options for domestic proceedings to address abuses, such as amnesty, lustration, truth commissions and criminal prosecutions, analyzing the choices different countries have made. Second, Judge Navanethem Pillay of the International Criminal Tribunal for Rwanda (ICTR) addresses the legal response to sexual violence in times of conflict and the definitions of rape and sexual violence in international law. Although this chapter provides a thorough analysis of the legal framework, the landmark *Akayesu* case and the jurisprudence of the ad hoc tribunals, one might wish for a more in-depth discussion of the challenges the judges at the ICTR faced in reaching their decisions and the forthcoming challenges for applying international humanitarian law to sexual violence, rape and related abuses. Moving from legal means to the use of military might to enforce international humanitarian law, Adam Roberts studies how humanitarian considerations have been invoked in United Nations debates and documents to trigger international military action. After a factual discussion of several crises in which humanitarian considerations played a role, Roberts weighs the costs and benefits of intervening on humanitarian grounds and concludes by emphasizing two primary challenges: the importance of ensuring that any military intervention itself complies with humanitarian law and the need to combine humanitarian aims with the effective strategic and political management of armed force, a task with which the United Nations and the international community continues to wrestle. This section ends with a chapter in which Edward Luck addresses the problem of ambivalence toward the use of force to enforce international humanitarian law. This ambivalence leads Luck to caution against the heralding of a new age of humanitarian intervention or the use of short-term arrangements to fill the gap in the absence of a reliable multilateral enforcement capacity. Rather, he argues that it is critical that countries build domestic coalitions that are both broad and stable enough to support any action with the necessary power and longevity.

Readers of *Civilians in War*, especially those working in the humanitarian assistance and protection fields, will find a series of useful recommendations and conclusions in the final part of the book. Part Four comprised of two chapters by Claude Bruderlein, by Bruce Jones, and Charles Carter respectively, Part Four attempts to sketch new frameworks for protection of civilians in this new century. First, protection strategies must take into account the changing nature of war and the increasing role of nonstate actors, including armed groups and corporations, in armed conflict. To this end, the international community must re-examine its approach to the protection of civilians and develop mechanisms to induce and enforce compliance with international humanitarian law by all actors in a conflict. Second, any effective protection strategy cannot exist solely at the multilateral

level but must begin at the local level and then be integrated with efforts at the regional level. Third, we must develop a better understanding of belligerent groups in order to develop mechanisms to influence their behavior. Fourth, understanding the needs of civilians is crucial as well, particularly when devising appropriate methods for addressing abuses through domestic or international proceedings. Finally, Jones and Cater end by outlining several areas for new work in research, organizational development and politics that can help lead the international community to a more effective model for the protection of civilians.

Civilians in War is an essential volume for understanding the new challenges we face in implementing and enforcing international humanitarian law in the twenty-first century. Hopefully this will be the springboard for ongoing analysis of how the international community can provide greater protection for civilians in times of war.

HOW TO PREVENT GENOCIDE: A GUIDE FOR POLICYMAKERS, SCHOLARS, AND THE CONCERNED CITIZEN

by John G. Heidenrich
Praeger Publishers, Westport, CT, USA, 2001

Lieutenant Commander Gregory P. Noone, JAGC, USNR[1]

During the 20th century, there were scores of horrific massacres, mass murders, crimes against humanity, war crimes, ethnic cleansings, and genocide. Each event throughout this bloodstained century was a tragedy, effecting thousands if not millions of people, and ultimately altering the course of history and mankind in innumerable ways. The killing of the Tutsis by machete in Rwanda, the Jews by the gas houses and ovens of Nazi Germany, and the deportation of Armenians to nowhere by the Young Turks are the clearest examples of genocide. But what about Stalin's purges where he killed millions of political opponents with particular focus on the Ukrainians, Mao's Cultural Revolution and the Great Leap Forward that resulted in millions of deaths, the Khmer Rouge's stockpiling the "killing fields" with people because they were educated or wore glasses, and the brutality in the Balkans which matched that of history's most evil dictators? Were these genocides? If so, what about Saddam Hussein's treatment of Iraqi Kurds, Argentina's Dirty War, Chile during Pinochet's reign and the "disappeared," Sudan's massacres and deportations of the people of the Nuba mountain area in the name of Jihad, the starving of Biafra's Ibos, and Germany's efforts at the beginning of the century to destroy the Bantu tribe of the native Herero in South-West Africa (now Namibia)?

The many horrific events that occurred during the past one hundred years begs the question of what makes an event a genocide as opposed to an

[1] Lieutenant Commander Gregory P. Noone, JAGC, USNR, (B.A. Villanova University 1987, J.D. Suffolk University Law School 1990) is currently assigned to Office of the Judge Advocate General, United States Navy, International and Operational Law Division Reserve Unit, in Washington D.C. LCDR Noone is a Training Program Officer in the Training Department of the United States Institute of Peace. USIP is an independent, nonpartisan federal institution created by the U.S. Congress to promote research, education, and training on the prevention, management and peaceful resolution of international conflicts. LCDR Noone is also an adjunct professor at Roger Williams University School of Law where he teaches International Law, US Military Law and Legal Policies, and Genocide in the 20th Century. Dr. Diana C. Noone edited this book review.

unconscionable mass murder. In early June of 1994, the Rwanda genocide was entering its third month of horror. The Clinton administration and United States Department of State spokespeople were instructed to brief the press that "acts of genocide may have occurred." Consequently the follow-up question was asked, "How many acts of genocide does it take to make genocide?" Often times policymakers, pundits, scholars and reporters will label one event or another as a genocide. Using the word genocide can be very powerful and compelling. At times it may be used correctly, or it may be used to bolster a point, or to drive home an agenda, or simply to sell more newspapers. More often than not, the word genocide is used because of ignorance as to its actual definition and the serious ramifications associated with using such a powerful word. Each time the term genocide is used incorrectly it devalues the importance and significance of the word and ultimately the tragic events that are actually genocides. Raphael Lemkin, a Polish Jew who immigrated to the United States after the Nazis invaded Poland, actually created the word genocide. Lemkin, in his 1944 book *Axis Rule in Occupied Europe*, maintained that, "New conceptions required new terms." This new word was derived from "the ancient Greek word *genos* (race, tribe) and the Latin *cide* (killing), thus corresponding in its formation to such words as tyrannicide, homicide, infanticide, etc." In other words, no existing word in mankind's vocabulary could adequately describe the Holocaust.[2]

What is genocide? The internationally recognized legal definition of genocide is found in Article II of the 1948 Convention on the Prevention and Punishment of the Crime of Genocide which defines genocide as "any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial, or religious group, as such: (a) Killing members of the group; (b) Causing serious bodily or mental harm to members of the group; (c) Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part; (d) Imposing measures intended to prevent births within the group; (e) Forcibly transferring children of the group to another group." Regardless of how narrow or loose of an interpretation of this definition one uses, the reality is that everyone is impacted not just by the horror of death and destruction, but by the millions of refugees and internally displaced persons, black market trafficking, powerful organized crime, and destabilizing conflicts.

Author John Heidenrich first addresses this controversial issue in his book. However, the author's central focus of *How to Prevent Genocide* is to examine "what can be done in practical terms" to prevent each brewing

[2] Lemkin contributed greatly to the framing and subsequent passage of the 1948 Convention on the Prevention and Punishment of the Crime of Genocide. As an aside, the author Heidenrich dedicates this book to Lemkin, as well as Raoul Wallenberg, the Swedish diplomat and secret U.S. operative who worked to save tens of thousands of Jews from the Nazis.

genocidal crisis. He endeavors to "explore the feasibility, as well as the advantages and disadvantages" of all possible options to "influence a genocidal crisis." Heidenrich attempts to cover a great deal of ground. He examines the psychological, cultural, political and religious beliefs behind killing.

When Heidenrich addresses war crimes and acts of genocide in regard to international law, he provides a brief but excellent discourse on the various international treaties, the international organizations involved, and the current International Criminal Tribunals for the Former Yugoslavia and Rwanda (ICTY and ICTR respectively). However, the author oversimplifies the International Criminal Court (ICC), makes a few errors regarding its powers (including the year the treaty conference occurred) and never attempts to reconcile legitimate opposition to the ICC treaty as written.

In the chapter dedicated to forecasting and detecting genocide, Heidenrich focuses on sources of information from hate literature and propaganda, to information gathered by legitimate media outlets, nongovernmental organizations (NGOs), international governmental organizations, religious groups, and academic researchers. Heidenrich addresses how forms of nonviolent pressure such as diplomacy, economic trade and nonviolent resistance can counter potential genocide. He discusses covert actions against genocide, with a brief discussion on the possible assassination of genocidal leaders as well as other types of covert actions. However, the majority of this section is appropriately dedicated to examining the native and foreign rescuers of the persecuted.

Heidenrich addresses the ethical principles of humanitarian intervention and explores the "relevant schools of thought" of the pertinent question: "Are there legitimate and universal principles for humanitarian intervention?" A brief but excellent description of the differences between peacekeeping and peace enforcement and their respective roles in preventing and/or halting genocide is included. The author discusses the limits of both national military forces and multinational forces and also addresses the issues of airpower in isolation, interposition ("central to the practice of peacekeeping"), partitioning, safe havens, safe zones, non-lethal weapons, and psychological operations to counter propaganda. Next Heidenrich addresses the idea of a standing UN legion, his central recommendation in the book. He details the evolution of the idea of a standing UN legion, often referred to as a UN rapid reaction force, from President Eisenhower to President Clinton. The author maintains that any "momentum" for such an idea was lost on October 3, 1993, in Somalia when 18 U.S. Army Rangers were killed in a fierce daylong battle. However, after Rwanda's genocide the idea of a standing force has been resurrected by a number of countries as one that could have easily prevented the horrors of Rwanda. Heidenrich makes note that many

humanitarian NGOs who have historically been neutral, and in some cases pacifist, are also calling for such a UN legion.

The author examines the feasible options for an international legion of volunteers "combined into a single standing unit available to the Security Council for relatively small scale but still risky missions of importance." The issues of composition, size, recruitment, mission, orientation, weaponry, financing, unit structure, and command and control are reviewed relying upon separate studies undertaken by the UN, Canada, and the Netherlands. He briefly mentions alternative options, including the use of "private military companies." Ultimately, Heidenrich maintains that the best cure to prevent genocide is "vigilant caring individuals both the extraordinary and ordinary, actively work[ing] to uphold everyone's most basic of human rights, locally and internationally." After all, in August 1939, prior to the unprovoked invasion of Poland by Nazi Germany, Hitler remarked, "Who after all is today speaking about the destruction of the Armenians?"

How to Prevent Genocide is an interesting and very well researched book. In fact the author often references quotes, speeches and writings beyond the usual references in this field of study. However, the author occasionally did not give a completely thorough discussion of an issue before wandering off on an intriguing aside. At other times, he appears to be a bit unrealistic, overly psychological, factually sloppy and too idealistic. However, with that said, this book would still be useful to any military lawyer involved in peace operations, overseas deployments, or operational and international law. The author largely accomplishes what he set out to do, which was to provide a helpful historical, legal, and thought provoking book for policymakers, scholars, and concerned citizens.