Cleveland State Law Review

Volume 50 | Issue 3 Note

2003

The Classified Information Protection Act: Killing the Messenger or Killing the Message

Mitchell J. Michalec

THE CLASSIFIED INFORMATION PROTECTION ACT: KILLING THE MESSENGER OR KILLING THE MESSAGE?

I. INTRODUCTION

> *A popular government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: and a people who mean to be their own governours [sic], must arm themselves with the power which knowledge gives.*[1]

[1]Letter from James Madison to William T. Barry (Aug. 4, 1822), *in* MADISON: WRITINGS, at 790. (Jack N. Rakove, ed., 1999).

"The essence of Government is power; and power, lodged as it must be in human hands, will ever be liable to abuse."[2]

The tension between the competing interests of the government's need to keep secrets in the interest of national security and the interests of free speech and a free press existed since the beginning of the republic. It is generally recognized that certain aspects of the business of government must be performed in secrecy, particularly in the context of national security and foreign affairs.[3] In certain scenarios, the Court acknowledged the necessity to restrain the freedom of speech and the press in the interests of national security and defense.[4]

Because the very essence of our constitutional government is based upon the proposition of an informed electorate, it is imperative that the government give great deference not only to an individual's right to freely criticize and debate public policy, but also to the press' right to freely publish, in order to provide the public with the information necessary for that debate.[5] In addition, openness in government is critical because there have been situations where the government's insistence on secrecy served to reduce its credibility among its citizens, and many complain that the executive branch, acting in its own self-interest, often abuses the classification system.[6] As Justice Douglas once stated:

> As has been revealed by such exposes as the Pentagon Papers, the My Lai massacres, the Gulf of Tonkin 'incident' and the Bay of Pigs invasion, the government usually suppresses damaging news but highlights favorable

---

[2]James Madison, Speech before the Virginia State Constitutional Convention (Dec. 1, 1829), *in* MADISON: WRITINGS, at 824. (Jack N. Rakove, ed., 1999).

[3]*See* U.S. Const. art. II § 2, cl. 1-2. (granting the President the power as Commander-in-Chief of the military and the power to make treaties); THE FEDERALIST No. 64 (John Jay) (recognizing the President's authority to make treaties carries a concomitant power to conduct such negotiations in secret); Bruce E. Fein, Symposium, *Access to Classified Information: Constitutional and Statutory Dimensions*, 26 WM. & MARY L. REV. 805 (1985) (stating the generally-held proposition that government secrecy is not only essential in the areas of military weapons, troops and tactics, but also in the area of foreign relations, treaties and executive agreements. Furthermore, Fein contends that secrecy in government is not incompatible with constitutional values, as evidenced by the fact that much of the deliberation over the passage of the Constitution was conducted in secret).

[4]*See* Schenck v. United States, 249 U.S. 47 (1919). Justice Holmes' famous opinion, which stated, "The question in every case is whether the words are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent. It is a question of proximity and degree." *Id.* at 52. Holmes' opinion also indicated that while restraints on speech are generally not allowed, they operate on a sliding scale, with the restrictions being most severe in times of war, when the survival of the nation itself is at stake.) *Id. See also,* Near v. Minnesota, 283 U.S. 697, 716 (1931) (stating "No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of sailing dates of transports or the number or location of troops").

[5]*See*, *e.g.*, David H. Topol, Note, *United States v. Morison: A Threat to the First Amendment Right to Publish National Security Information,* 43 S. C. L. REV. 581 (1988).

[6]*See*, *e.g.*, Benjamin S. Du Val, Jr., *The Occasions of Secrecy*, 47 U. PITT. L. REV. 579 (1986).

> news. In this filtering process the secrecy stamp is the official's tool of suppression which in '99 ½' of the cases would present no danger to national security.[7]

In recent years, there have been complaints from a variety of sources that national security is continually compromised by a succession of leaks of classified information by government employees to the press.[8] George Tenet, Director of the Central Intelligence Agency (hereinafter "CIA"), complained publicly that "the executive branch leaks like a sieve"[9] and that the harm caused by these leaks "abuses the security of Americans."[10] The most compelling reasons set forth for preventing leaks are that leaks provide valuable intelligence information to America's adversaries; they compromise the government's ability to further its legitimate policies by allowing for "vetoes by leak;" they endanger intelligence sources and methods and potentially endanger the lives of agents; they make other countries less willing to cooperate with the United States, because they believe they cannot rely on the government's ability to keep diplomatic or intelligence secrets; and in some cases, they allow the government itself to manipulate public opinion by leaking partial information when it serves its purposes.[11] Max Frankel, former editor of the *New York Times*, best expresses the converse view. While he acknowledged the culture of "leaks" in Washington, which exists as a small network of government officials who routinely share classified information with reporters,[12] Frankel stated, "[w]ithout the use of 'secrets' ... there could be no adequate diplomatic, military and political reporting of the kind our people take for granted, and there could be no mature system of communication between the government and the people."[13]

Thus, the debate rages on between both sides, with varying degrees of force on whether the prevalence of "leaks" of classified information through the press to the public work to do more harm than good to the government and the nation as a whole. Professors Harold Edgar and Benno Schmidt, who were among the first to examine the subject, best framed the conundrum faced by those in government when they asked, "[h]ow can those who would shape our institutions respond to the threats and

---

[7]Gravel v. United States, 408 U.S. 606, 641-2 (1972) (Douglas, J. dissenting).

[8]*See generally,* Symposium, *The First Amendment and National Security*, 43 U. MIAMI L. REV. 61, 64-5 (1988) (comments by Professor Holzer decrying the rampant disclosure of classified information to the press for various purposes).

[9]Vernon Loeb, *Senate Bill Aims to Curb News Leaks; Revealing Classified Data Would Be Felony*, WASHINGTON POST, June 14, 2000 at A37.

[10]*Id*.

[11]*See*, *e.g.*, Michael L. Charlson, *The Constitutionality of Expanding Prepublication Review of Government Employee's Speech*, 72 CALIF. L. REV. 962 (1984); Edward L. Xanders, *A Handyman's Guide to Fixing National Security Leaks: An Analytical Framework for Evaluating Proposals to Curb Unauthorized Publication of Classified Information*, 5 J.L. POL. 759 (1989).

[12]Theodore F. Kommers, Symposium, *Increased Press Access to Government Information—Limiting the Range of Government Classification*, 6 NOTRE DAME J.L. ETHICS & PUB. POL'Y 217, 229 (1992).

[13]*Id.*

complexity of the modern world, and continue to respect our constitutional traditions of separation of powers and of informed freedom of expression on issues critical to democratic governance?"[14] Another scholar effectively framed the controversial nature of the issue as, "[t]he problem of national security leaks is not susceptible to easy solution because not all leaks are inherently harmful, and some leaks result in the furtherance of democratic ideals ... draconian measures to plug leaks pose a serious threat to genuine First Amendment concerns and will always generate fervent criticism."[15]

Currently, the House of Representatives introduced H.R. 2943 (hereinafter "The Classified Information Protection Act"),[16] which would amend section 798 of the Espionage Act[17] to criminalize the "willful and knowing" disclosure of "properly classified" information by any person who is a current or former "officer or employee of the United States" or "any other person" with current or former authorized access to classified information to "any person who is not authorized access to such classified information, knowing that such person is not authorized"

---

[14]Harold Edgar & Benno C. Schmidt, Jr., *Curtiss-Wright Comes Home: Executive Power and National Security Secrecy,* 21 HARV. C.R.-C.L. L. REV. 349, 350 (1986) [hereinafter *Curtiss-Wright Comes Home*].

[15]Xanders, *supra* note 11, at 760.

[16]The Classified Information Protection Act of 2001, H.R. 2943, 107th Cong. (2001) [hereinafter *The Classified Information Protection Act*]. The text of the bill reads as follows:

> Section 798 (A). UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION
>
> (a) Prohibition – Whoever, being an officer or employee of the United States, a former or retired officer or employee of the United States, any other person with authorized access to classified information, or any other person formerly with authorized access to classified information, knowingly and willfully discloses, or attempts to disclose, any classified information acquired as a result of such person's authorized access to classified information to a person (other than an officer or employee of the United States), who is not authorized access to such classified information, knowing that the person is not authorized access to such classified information, shall be fined under this title, imprisoned for not more than 3 years, or both.
>
> (b) Construction of Prohibition. Nothing in this section shall be construed to establish criminal liability of disclosure of classified information in accordance with applicable law to the following:
>
> (1) Any justice or judge of a court of the United States established pursuant to article III of the Constitution…
>
> (2) The Senate or House of Representatives, or any committee or subcommittee thereof, or joint committee thereof, or any Member of Congress.
>
> (3) A person or persons acting on behalf of a foreign power (including an international organization) if the disclosure –
>
> (A) is made by an officer or employee of the United States who has been authorized to make the disclosure; and
>
> (B) is within the scope of such officer's or employee's duties.
>
> (4) Any other person authorized to receive classified information.

[17]*Id.* 18 U.S.C.A. §§ 792-799 (West 2001).

such access.[18] Violation of this proposed law would result in a fine of $10,000, imprisonment of up to three years, or both.[19]

The purpose of this Note is to discuss the adequacy of existing statutory and administrative protections for classified information, examine how the agencies responsible for protecting this information implemented controls, and how the courts interpreted these existing protections. This Note argues that the failure of the government to prevent "leaks" is not necessarily a failure of the existing scheme, but rather a failure of the government to apply current controls. Furthermore, it demonstrates that the Classified Information Protection Act is an unnecessary, overbroad, and in some cases, ineffective alternative to the existing protections, with a great potential for abuse. If the bill is passed, it would undoubtedly serve to chill important debate on matters of public interest. Finally, this article will mention some possible alternatives to the bill, which could be implemented to protect the government's legitimate need for secrecy while balancing the First Amendment rights of government employees and the press.

II. LEAKS OF "SECRETS:" FIRST AMENDMENT CONCERNS

A. Pentagon Papers*: The First Attempt to Prevent Publication of Secrets*

In 1971, the two competing interests of government secrecy versus the First Amendment reached a flashpoint with the extraordinary case, *New York Times v. United States* ("Pentagon Papers").[20] The dispute arose out of the publication of a top-secret study about the United States' role in Vietnam since the Truman Administration, which was leaked to the press by Daniel Ellsberg.[21] Ellsberg was a defense department analyst who helped author the study, and therefore, had authorized possession of the document.[22] The document, that Ellsberg was authorized to keep in his home, was removed for copying by Anthony Russo.[23] The study was subsequently published in both the *New York Times* and the *Washington Post*.[24] The document revealed, among other things, that the executive branch followed a pattern of deception against the public regarding its intentions to commit troops to Vietnam and ultimately served to raise public sentiment against the war effort.[25]

The case was decided, not with respect to the constitutional issues relating to the punishing of Ellsberg and Russo for communicating information relating to

---

[18]*See The Classified Information Protection Act*, *supra* note 16.

[19]*Id.*

[20]403 U.S. 713 (1971) (per curiam).

[21]Jereen Trudell, Note, *The Constitutionality of Section 793 of the Espionage Act and its Application to Press Leaks,* 33 WAYNE L. REV. 205, 209, and n. 17 (1986).

[22]*Id.*

[23]*Id*.

[24]*Id*.

[25]Microsoft Encarta Encyclopedia, CD-ROM, 2000 edition. Search Term: Pentagon Papers.

government policy-making, but rather on whether the government could enjoin reporting news that was obtained through unauthorized transfer of secret documents.[26] The Court found that prior restraints against publication of information, classified or not, even if illegally obtained, are presumptively invalid unless the government meets its "heavy burden" of justification for the injunction.[27] The case left open, however, the possibility that the press may be punished criminally after classified information is published.[28] It also left undecided the question of whether the government could constitutionally punish current and former government employees who leak classified information to the press.[29]

B. Government Employee as Speaker (or Leaker?): First Amendment Considerations

The calculus changes somewhat when the government attempts to impose restrictions on the "ordinary" political speech of government employees. In *Pickering v. Board of Education*,[30] the Court recognized that, a public employee does not relinquish First Amendment rights to comment on matters of public concern merely by virtue of his employment status.[31] The Court also recognized, however, that the government as an employer may have different interests than the government as sovereign and, therefore "the problem in any case is to arrive at a balance between the interests … as a citizen in commenting on matters of public concern and the interests of the State as an employer in promoting the efficiency of the public services it performs through its employees."[32] In *Connick v. Myers*,[33] the Court held that when matters are not of public concern, the government employee's First Amendment rights, while not relinquished, are nonetheless significantly less than in their capacities as private citizens.[34] As the Court stated, "to presume that all matters that transpire within a government office are of public concern would mean that virtually every remark – and certainly every criticism directed at a public official – would plant the seed of a constitutional case."[35]

---

[26]Trudell, *supra* note 21, at 209.

[27]*The Pentagon Papers*, 403 U.S. at 714.

[28]*Id.* at 733. Justice White stated the "failure by the Government to justify prior restraints does not measure its constitutional entitlement to a conviction for criminal publication." *Id.*

[29]Trudell, *supra* note 21, at 209.

[30]391 U.S. 563 (1968).

[31]*Id.*

[32]*Id.* at 568.

[33]Connick v. Myers, 461 U.S. 138 (1983). This case arose out of the firing of an assistant district attorney who circulated a questionnaire to other employees after she was informed of a transfer to a different section of the court. The questionnaire involved such matters as office transfer policy, employee morale, the possible formation of an employee grievance committee and whether or not other employees received pressure within the office to work on political campaigns. *Id.*

[34]*Id*.

[35]*Id*. at 149.

Resolution of the issue of disclosure of classified information by government employees should also ultimately return to the central premise of *Pickering* and its progeny. The Court stated, "whether a [government] employee's speech addresses a matter of public concern must be determined by the content, form and context of a given statement, as revealed by the whole record."[36] As such, any proposed changes to the laws regarding disclosure of classified information must take into account a balancing formula derivative of the *Pickering* rule between the employee's interest in speaking about matters of public concern and the government's compelling interest in protecting our nation's security.[37] As will be discussed later in this Note, when the government speaker discloses classified national security information, even for matters clearly in the public concern, the Court's balancing the interests of the government and the employee becomes almost a fiction. If the Classified Information Protection Act of 2001 is enacted, it will, by its very terms, in combination with existing judicial decisions on the subject, effectively render moot any principled effort to apply *Pickering*. This would be a grave error.

III. HISTORY OF THE CLASSIFIED INFORMATION PROTECTION ACT: OLD WHINE, NEW BOTTLE?

The Classified Information Protection Act was proposed on September 21, 2001 by Congressman David Vitter, and was immediately referred to the House Judiciary Committee.[38] The introduction of the bill took place after an identical provision in the Senate, sponsored by Richard Shelby, Vice Chairman of the Senate Intelligence Committee,[39] was withdrawn from consideration as an amendment to the Senate's version of the Intelligence Authorization Act of 2002 on September 5, 2001.[40] Originally, a hearing was scheduled before the Senate Intelligence Committee on the same day the proposed amendment was withdrawn.[41] The hearing was to discuss the measure, and would have included testimony from both the Attorney General and the Director of the CIA.[42] The hearing was abruptly cancelled, after much opposition from members of Congress and interest groups, including the press and civil libertarians.[43]

---

[36] *Id.* at 147-48.

[37] *Pickering,* 391 U.S. at 568.

[38] H.R. 2943, 107th Cong. (2001).

[39] S. 1428, 107th Cong. (2001).

[40] *See* Walter Pincus & Vernon Loeb, *White House Still Undecided on Proposal to Limit Leaks; Measure would Criminalize disclosure of Classified Data,* WASHINGTON POST, August 23, 2001, at A23. (describing the proposal and a scheduled hearing on September 5, 2001 on the proposed measure).

[41] *See* Walter Pincus, *Bid to Crack Down On Leaks is Put Off; White House not Ready to Back Plan,* WASHINGTON POST, September 5, 2001, at A02; Jim Lobe, *Politics U.S.: Bush Backs Off Secrecy Bill*, INTER PRESS SERVICE, Sept. 5, 2001 (on file with LEXIS, News Library, Wire Service Stories File).

[42] *See* Pincus & Loeb, *supra* note 40.

[43] *See* Pincus & Loeb, *supra* note 40.

Ironically, an identical provision was tacked onto the Intelligence Authorization Act the previous year, that passed through both Houses of Congress with very little debate.[44] While initially supported by members of the administration, after further consideration, President Clinton vetoed it.[45]

The proposed anti-leak provision in the 2001 Senate Bill was replaced by a section authorizing the creation of an interagency task force, to determine whether the new law is needed.[46] According to the provision, the Attorney General is to lead the review and is to be assisted by the Secretary of Defense, the Secretary of State, the Departments of Defense and Energy and other agencies that have responsibility for handling classified information.[47] The amendment to the Act will also require the task force to report to Congress by the statutorily mandated deadline of May 1, 2002. The Intelligence Authorization Act of 2002 was passed as amended, and the House Version of that bill was signed into law on December 28, 2001.[48] Because the Attorney General is now authorized to conduct an investigation, it is appropriate that discussion turns to the existing legal administrative and judicial mechanisms for protecting classified information. In the interim, the Classified Information Protection Act that contains identical language to the Senate's original rider to the Intelligence Authorization Act of 2002 stands at the ready should the Commission recommend that new legislative protection against leaks is necessary.[49]

IV. FIXING THE LEAKS: WHAT'S CURRENTLY IN THE STATUTORY TOOLBOX?

According to a Congressional study, there are five major categories of government information protected by government secrecy.[50] These include national defense information, foreign relations information, information relating to government law enforcement investigations, proprietary commercial information relating to the maintenance of commercial advantage, and information relating to personal privacy.[51] The first two categories of information relate to what is commonly defined as "national security information" and are the focus of most of the current statutory protections.[52] They are also the primary focus for analysis here.

---

[44]*See* Pincus & Loeb, *supra* note 40.

[45]*Id.*

[46]*See* S. 1428, 107th Cong. § 307 (2001).

[47]*See* Jerry Seper, *Ashcroft Creates Interagency Task Force on Security Leaks*, WASHINGTON TIMES, December 16, 2001, at A3.

[48]Intelligence Authorization Act of 2002, Pub. L. No. 107-108, § 310 Stat. 1394, 1401 (2001).

[49]H.R. 2943, 107th Cong. (2001)

[50]*Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy*, 103rd. Cong., Report Pursuant to Public Law 236 (Comm. Print 1997) [hereinafter *Moynihan Report*]. The Report is the result of the second comprehensive study in forty years to look at the methods costs and benefits of government secrecy. It was the result of a bipartisan effort, and made several recommendations on how to improve the protection on essential classified information in the post Cold-War era. *Id.*

[51]*Id.*

[52]*Id.*

Gorin v. United States[53] defined "National defense" information. The Court characterized it as a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[54] Since *Gorin,* this concept of national defense information has been consistently applied in all cases involving unauthorized disclosure, whether such disclosure was to a foreign agent or power or to the press.[55] It is also the linchpin in evaluating many of the primary statutory protections against leaks of information, and is one of the key reasons that individuals favoring the new legislation consider current statutes insufficient.[56]

The first and arguably most important of the provisions protecting the secrecy of national security information is the Espionage Act,[57] which proscribes various conduct, from "harboring or concealing" persons who one "knows or has reasonable grounds to believe or suspect has committed" acts of espionage defined in sections 793 or 794,[58] to various prohibitions against violating regulations promulgated by the Administrator of NASA.[59]

A. Section 793 of the Espionage Act

There are several provisions of the Espionage Act, that arguably have implications to the leaking of classified information to the press. The section of primary importance, that is most readily applicable to the leaking of government secrets to the press, is section 793.[60] This section consists of six major provisions covering two different kinds of prohibited activity, both traditional espionage and other disclosures of national defense information. Violating any of these provisions is subject to a fine and/or imprisonment for a period of up to 10 years.[61] Currently, the few major prosecutions against "leakers" of national defense information have been tried under this section. Further examination of the prohibitions embodied in the code, as well as how courts interpreted the terms, will demonstrate how courts interpreted the statute to apply to leaks of classified information to the press.

Subsections 793 (a) and (b) are constructed to impose criminal penalties on individuals who "for the purpose of obtaining information respecting the national

---

[53]312 U.S. 19 (1941).

[54]*Id* at 28.

[55]*See*, *e.g.*, United States v. Morison, 844 F.2d 1057 (4th Cir. 1988), cert. denied 488 U.S. 908 (1988); *Pentagon Papers*, 403 U.S. 713 (1971) (per curiam).

[56]*See*, *e.g.*, Pincus & Loeb, *supra* note 39. The authors quote a position paper prepared by the Intelligence Committee in 2000 which maintained that current law does not cover "leaked intelligence information regarding sources and methods, counter-narcotics, counterintelligence capabilities and liaison relationships with foreign intelligence groups because they don't fall within the accepted definition of national defense information." *Id.*

[57]18 U.S.C.A. §§ 792-799 (West 2001).

[58]18 U.S.C.A. § 792 (West 2001).

[59]18 U.S.C.A. § 799 (West 2001).

[60]18 U.S.C.A. § 793 (West 2001).

[61]*Id*.

defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation."[62] By their structure and language, these subsections are designed to punish cases of espionage or, more accurately, the activities in contemplation of espionage activity,[63] such as the famous case of *United States v. Rosenberg*,[64] where the defendants were convicted of conspiring to steal, deliver and transfer nuclear secrets to representatives of the Soviet Union.[65]

Subsection 793 (a) prohibits an individual from entering upon, flying over, or otherwise obtaining information relating to "vessels, aircraft, work of defense, navy yard, naval station ... building, office, laboratory, station or other place connected with the national defense ... or any prohibited place so designated by the President by proclamation in time of war or national emergency, information as to which the President has determined would be prejudicial to the national defense" and with the "intent that the information would be used to the injury of the United States or to the advantage of any foreign nation."[66] Subsection 793(b) applies the same purpose and intent standards to the individual who "copies, takes, makes, or obtains, or attempts to copy, take make or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected to the national defense."[67] Professors Edgar and Schmidt argue convincingly, that focusing on the obtainer's state of mind as to the eventual use of the information, is consistent with Congressional purpose to punish only those who have the intent to injure the United States.[68] If this particular formula is followed, then it is clear that these particular subsections are not applicable to the individual who gathers the information and reports it to the press. The absence of a single case under sections 793(a) and (b) involving prosecution of persons who leak information related to the national defense to the press, while not conclusive, seems to bear out that Edgar and Schmidt's interpretation is correct.

Subsection 793(c)[69] applies the same purpose standard, that is, to obtain information relating to the national defense, to the *receipt or acquisition* of a broad range of materials or information "connected to the national defense, knowing or having reason to believe, at the time he receives or obtains, or attempts to receive or

---

[62]18 U.S.C.A. §§ 793(a) – (c) (West 2001).

[63]*See generally,* Harold and Benno C. Schmidt, Jr. *The Espionage Statutes and Publication of Defense Information,* 73 COLUM. L. REV. 929 (1973) (discussing the legislative histories of the Espionage Act of 1917, and it's predecessor statute, the Defense Secrets Act of 1911) [Hereinafter *The Espionage Statutes*].

[64]195 F.2d 583 (2d Cir. 1952).

[65]*Id.*

[66]18 U.S.C.A. § 793(a) (West 2001).

[67]18 U.S.C.A. § 793(b) (West 2001).

[68]*See The Espionage Statutes, supra* note 63, at 997-98.

[69]*See* 18 U.S.C § 793(c) (the specific materials connected to the national defense, and referred to in this section of the statute include "any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance or note").

obtain that it has been or will be obtained ... contrary to the provisions of this chapter."[70] A literal reading of the statute appears to do away with the intent standard. In that sense, it would be much like the proposed Classified Information Protection Act,[71] in that no standard of intent to harm the United States or advantage a foreign nation is present.

Professors Edgar and Schmidt argue that the legislative history of section 793 demonstrates that Congress intended subsection (c) to be read with the same culpability standards as subsections (a) and (b), although they admit that the language of the statute does not inform such an interpretation.[72] They also argue, that even if the statute is read literally, that the scope of the statute is dependent on other factors, the most important of which is that it prohibits the receipt of only tangible items.[73] Furthermore subsection (c) requires that the receipt of such items is only criminal if the recipient is aware that they were obtained in violation of subsections 793 (a) and (b).[74] They also note, if subsections (d) and (e) are construed by the courts to include information released for the purpose of public debate, will influence the interpretation of subsection (c). The effect of this construction would make the receipt of any tangible document or note a crime, even if there is no conspiratorial relationship between the provider of the information and the recipient.[75] Such a strict constructionist interpretation of the section would implicate the First Amendment rights of the press if the reporter was aware that the document he received was illegally taken.

As will be discussed, there is support for such a reading in the limited case law relating to the subject. However, if such a reading is followed, it would, while viewed in combination with subsections (a) and (b), have the bizarre effect of criminalizing the press for receiving and printing the information in cases such as *Pentagon Papers*,[76] while sparing the person who obtained the information from criminal punishment, because the requisite intent of harm to the United States or advantage to a foreign nation cannot be easily proven. On the other hand, the standard of proof needed to subject the recipient to criminal penalties is arguably less, because while the recipient may not have actual knowledge of the violation, they may have reason to believe that the statute has been violated if they receive pictures, notes or other materials relating to defense installations or instrumentalities.

Subsections of 793 (d) and (e) may be treated together for the purposes of discussion, because while each proscribes a different type of behavior, each is similar in that subsection 793 (d) provides that "whoever, lawfully having possession of, access to, or control over any document, writing…or note relating to the national defense, or information relating to the national defense, which information the possessor knows or has reason to believe *could be used* (emphasis added) to the

---

[70] *Id.* (emphasis added).

[71] *See* H.R. 2943, 107th Cong. (2001).

[72] *The Espionage Statutes, supra* note 63,at 1059.

[73] *Id.*

[74] *Id.*

[75] *Id.* at 1060.

[76] 403 U.S. at 713.

injury of the United States,"[77] and subsequently either willfully communicates to another person who is also not authorized to possess it or fails to return it to a party who is authorized is subject to criminal penalties.[78] The language of subsection 793 (e) is identical, except that the terms of the offense are applied to those who have *unauthorized* possession of the writings or other materials.[79] The interesting thing about these statutes is that they retain the element of willful communication, but the specific intent requirement is markedly absent, much like in the current formulation of the proposed statute.[80] In addition, because the prohibition on "communication" or retention in subsections (d) and (e) is to "any person not entitled to receive it,"[81] it arguably implicates not only the First Amendment rights of the employee, but also those of the press. Moreover, when subsections (d) and (e) are read broadly, then under subsection (c)'s prohibitions, members of the press could arguably be subject to criminal liability if they "had reason to believe," that their source obtained the information in violation of subsections (d) and (e).

Professors Edgar and Schmidt maintain that Congress did not intend for disclosure of defense information and subsequent publication to fall under the ambit of subsection (d) and (e)'s prohibitions.[82] Furthermore, they state "while the legislative record is reasonably clear that a broad reading is not intended…(and) is almost certainly unconstitutionally vague and overbroad,"[83] the language of the subsections "does not lend itself to any one confined reading as a means of saving them."[84] In the limited case law that exists on prosecution of leaks of classified information to the press under sections 793 (d) and (e), one court refused to accept the argument and successfully convicted an individual for disclosing classified information to the press.[85]

The last subsection, 793(f) states that a person authorized to possess various kinds of documents or other items relating to the national defense, who through "gross negligence" allows these items to be illegally removed, lost or *abstracted* from his possession without notifying his superior officer, is subject to fine or imprisonment.[86] This provision could also arguably be used to prosecute "leakers" like Ellsberg, who allowed the documents in his possession to be copied for publication.[87]

---

[77]18 U.S.C.A. § 793(d) (West 2001).

[78]*Id*.

[79]18 U.S.C.A. § 793(d) (West 2001).

[80]*Compare* 18 U.S.C.A. §§ 793(d) and (e) (West 2001) *with* H.R. 2943, 107th Cong. (2001).

[81]18 U.S.C.A. §§ 793(d) - (e) (West 2001).

[82]*The Espionage Statutes, supra* note 63, at 1000.

[83]*Id*.

[84]*Id*.

[85]United States v. Morison, 844 F.2d 1057 (4th Cir. 1988), *cert. denied*, 488 U.S. 908 (1988).

[86]18 U.S.C.A. § 793(f) (West 2001).

[87]*See* Trudell, *supra* note 21, at 216.

B. Other Espionage Act Provisions and their Relevance to Press Leaks

Three other sections of the Espionage Act implicate the First Amendment by prohibiting "publication" in certain circumstances. Section 798 prohibits a person from "knowingly and willfully" communicating, "*publishing"* or using "in any manner prejudicial to the United States, any classified cryptographic or communications information or information relating to any device used for cryptographic or communications intelligence" to an unauthorized person.[88] In analyzing the scope of a particular section of a statute, it should be viewed in relation to all of the other sections to determine its meaning. Professors Edgar and Schmidt point out that section 798 is violated merely on the showing of a knowing and willful communication, while no intent to harm or disadvantage the United States is necessary for conviction.[89] Furthermore, the appearance of the term "publishes" implies that for this particular class of information, it is meant to operate as a ban on public speech.[90]

Looking at all of the provisions of section 793, alongside section 798, it would appear that section 793 was not meant to cover publication of defense information, and therefore, the First Amendment rights of the press to publish other information relating to the national defense are not implicated. Because it is clear that communications intelligence information falls under the larger umbrella of national defense information,[91] breaking that subclass of information out separately in another section seems like surplusage if section 793 in fact, covers publication. Furthermore, this one possible reading of sections 793 and 798, appears to indicate, that for, at least this one particular class of national defense information, the press could be criminally liable, not only for publication of this information, but theoretically for its receipt under subsection 793 (c).

There are two final sections of the Espionage Act, that implicate the First Amendment right of government employees and the press by specifically referring to publication. Sections 795[92] and 797,[93] referred to as the photographic statutes,[94] prohibit the taking and subsequent publication of photographs of military or naval installations if they are defined by the President as vital to the national defense and therefore protected against the general dissemination of information. After thirty days following such a determination by the President, anyone taking photographs of these installations and publishing them, unless specifically authorized by the commander of the installation, and subject to censorship by a proper authority, is subject to a criminal penalty.[95] These statutes therefore authorize prior restraints, in the form of pre-publication review, in contrast to the general presumption against it

---

[88]18 U.S.C.A. § 798 (West 2001).

[89]*The Espionage Statutes*, *supra* note 63, at 1000.

[90]*Id*.

[91]*Id*.

[92]18 U.S.C.A. § 795 (West 2001).

[93]18 U.S.C.A. § 797 (West 2001).

[94]*The Espionage Statutes*, *supra* note 63, at 1069.

[95]*Id.*

in the *Pentagon Papers*[96] case, and also allow for the extraordinary remedy of post-publication criminal punishment against the press or any other person who publishes them.[97] According to the legislative history of the statutes, it is unclear whether Congress was aware at the time the statutes were passed, that they were also meant to authorize prior review of top-secret documents relating to these vital installations. In other words, it is unclear whether the top-secret nature of these facilities was imputed to any photographic or graphical representation already existing.[98] Like section 798 and the Classified Information Protection Act,[99] no intent to injure the United States or to advantage a foreign nation is required to create criminal liability under these statutes.

C. Other Specialized Statutes Prohibiting Disclosure

There are a few other specialized statutes, that bear mention because they either explicitly restrict disclosures of certain types of information, or they have been applied to punish these disclosures. Some of these statutes are narrowly drawn, and reach modes of behavior that Congress did not believe fell under the purview of the Espionage Statutes. Many of them were specifically enacted in response to the publication of national security information.[100] Others have been construed to enable the government to prosecute both a government employee who leaks classified information, and to impose prior restraints against not only the government employee as a speaker communicating or publishing on his own, but also against the press when they serve as the channel through which such communications are made to the public.

Although by no means an exhaustive treatment, the following discussion centers on these other important statutes, which were enacted to prohibit specific disclosures by government employees, and how they implicate the First Amendment. As will become evident, most of the statutes were ad hoc responses to specific events, which

---

[96]*Pentagon Papers*, 403 U.S. at 713 (1971).

[97]*See* 18 U.S.C.A. § 795 (West 2001); 18 U.S.C.A. § 797 (West 2001).

[98]*The Espionage Statutes, supra* note 63, at 1071.

[99]H.R. 2943, 107th Cong. (2001).

[100]The Intelligence Identities Protection Act of 1982, 50 U.S.C.A. §§ 421-426 (West 2001) [Hereinafter The Intelligence Identities Protection Act]. The Act created a prohibition against disclosure of identities of covert agents operating on behalf of the United States to "any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States." *Id.* The Act in section 421 (a) provides penalties in the form of fines or imprisonment for up to 10 years, in the case where the individual has authorized access to classified information that identifies covert agents. In section 421 (b), if a person learns the identity of a covert agent through classified information which does not necessarily identify a covert agent explicitly, and subsequently makes the disclosure to an unauthorized person, they are subject to fine and imprisonment up to a period of 5 years. Section 421 (c) contains a provision criminalizing persons with a fine and or imprisonment of up to three years, when they engage in a "pattern of activities intended to identify and expose covert agents". This penalty applies even if such individual does not have access to, nor uses classified information in identifying those agents. *Id.*

brought the scope of coverage of the Espionage Act into question. In light of the variety of prohibitions that have been promulgated over the years and the scant amount of case law interpreting and enforcing these statutes, it is unsurprising that Congress now is proposing a reform as sweeping and potentially chilling as the Classified Information Protection Act.

The first of these statutes is the Intelligence Identities Protection Act,[101] which arose after the publication of two books, *Dirty Work 1: The CIA in Western Europe* and *Dirty Work 2: The CIA in Africa,* by former CIA Agent Philip Agee,[102] and the magazines "Counterspy" and "Covert Information Bulletin" that purported to identify covert agents operating in foreign countries.[103] Following publication of the names of alleged covert agents in the magazines, two attacks took place. A month after being identified in "Counterspy" as the CIA station chief in Athens, Greece, Richard Welch was murdered.[104] In a later incident, after the editors of "Covert Information Bulletin" identified an embassy official as a CIA operative, an unsuccessful attempt was made on his life.[105] Because the CIA alleged that even in the absence of the attacks, the activities of these publishers and former insiders compromised the integrity of intelligence operations abroad, and because Congress did not believe that existing statutes were adequate protection, the Intelligence Identities Protection Act was enacted.[106]

It is clear that keeping the identity of CIA operatives in foreign countries secret presents one of the more critical issues relating to national security, particularly because it concerns the integrity of the United States' intelligence sources and methods. As such, this is presumed to be a legitimate aim by most commentators and scholars.[107] In addition, it is arguable that from the definition of "national defense" set forth in *Gorin* and section 793, that the identities of covert agents do not readily fall under the ambit of that definition, unless one broadly reads the phrase "related to national preparedness."[108] Because *Gorin* itself encourages the use of "broad connotations,"[109] then arguably, the Espionage Statutes apply. If one adopts the narrower interpretation, however, then none of the Espionage Statutes clearly apply to this situation. After careful deliberation, Congress accepting the more narrow interpretation, enacted the legislation, which it believed closed a loophole in the existing statutory scheme.

Another statute, that creates criminal penalties for the dissemination of certain types information is 18 U.S.C. § 952, governing diplomatic codes and

---

[101]*Id.*

[102]Susan D. Charkes, Note, *The Constitutionality of the Intelligence Identities Protection Act,* 83 COLUM. L. REV. 727, 754 n.4 (1983).

[103]*Id.* at 728.

[104]*Id.* at 754, n.7.

[105]*Id.*

[106]*Id.* at 729.

[107]*See* Xanders, *supra* note 11, at 782-83.

[108]*Gorin*, 312 U.S. at 28.

[109]*Id.*

transmissions.[110] Section 952 prohibits government employees who "without authorization" willfully "publish or furnish to another" diplomatic codes, information prepared or transmitted in such codes or "any matter obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States" and punishes violators with a fine or imprisonment of up to 10 years.[111] Interestingly, this is one of the few provisions, like section 798, where Congress criminalized *publication*, as opposed to communication, lending further credence to the theory that the term "communication," does not include publication. Another possible, and more benign explanation why this statute specifically criminalizes publication may have less to do with the distinction and more with the quick and ill-considered legislative response, that often results from government embarrassment.

This statute was, like the Intelligence Identities Protection Act, enacted in response to publication of a book entitled *The American Black Chamber*, published by Herbert Yardley, a former director of a State Department division responsible for breaking diplomatic codes.[112] The book contained not only descriptions of code breaking procedures, but also included decoded messages intercepted from the Japanese government in 1921.[113] The publication of the book not only led to strained relations between the two governments, but also led to the adoption of a new code system by Japan.[114] When the government learned that Yardley was about to publish a second book, Congress hurriedly passed section 952 to prevent further damage from the potential disclosure of diplomatic codes and messages,[115] but not before the prohibition was significantly narrowed from its original scope, which included individuals who were not employees of the government, due to the potential effects on freedom of the press.[116]

Congress responded again to the perceived lack of coverage of the Espionage Statutes in relation to atomic energy and weapons when it enacted the "Restricted Data" statutes in 1954[117] to prevent disclosures of information under the control of the Atomic Energy Commission (now the Nuclear Regulatory Commission) to unauthorized individuals.[118] Section 2274 of Title 42 is the key provision, and prohibits any person with lawful or unlawful "possession of, access to, control over or being entrusted with any document, writing, sketch, photograph, plan, model, appliance, note or information involving or incorporating restricted data"[119] from

---

[110] 18 U.S.C.A. § 952 (West 2001).

[111] *Id.*

[112] *The Espionage Statutes, supra* note 63, at 1060-61.

[113] *Id.* at 1061.

[114] *Id.*

[115] *Id.*

[116] *Id.* at 1062.

[117] 42 U.S.C.A. §§ 2271-2281 (West 2001).

[118] *See The Espionage Statutes, supra* note 63, at 1075.

[119] 42 U.S.C.A. § 2274 (West 2001).

either "communicating transmitting or disclosing"[120] or any attempt to do so, to "any individual or person ...with the intent to injure the United States or advantage any foreign nation."[121] Subsection 2274 (a) follows the form of a prohibition of classic espionage behavior, and provides stiff penalties of up to life imprisonment and or a fine of up to $100,000.[122] Section 2274 (b) carries the same prohibitions as section (a), but reduces the culpability standard from intent to reason to believe, and provides for a fine of $50,000 and/or imprisonment of not more than ten years.[123] Professors Edgar and Schmidt argue that the split in culpability standards in subsection (b) when coupled with the absence of a willful intent to communicate the information, as is required in the Espionage Statutes, demonstrate Congress' intent to punish disclosure of nuclear secrets on the mere showing of recklessness or even negligence.[124] If this is true, it is indicative of the seriousness in which Congress viewed potential harm, in relation to other "garden variety" types of national defense information. The question remains, however, as to why Congress did not merely amend the Espionage Statues to include a special category of penalty for information controlled by the Nuclear Regulatory Commission, rather than enact an entirely separate statute. What it indicates, if nothing else, is the complexity of the problem of protecting government secrets and the complete lack of coherent standards, which inevitably lead to confusion and lack of effective enforcement.

Section 783 of Title 50 is yet another provision enacted by Congress to guard against disclosure of classified information by government employees. Section 783 (a) prohibits government officers or employees from communicating "any information of a kind which shall have been classified by the President or by the head of any department, agency or corporation with the approval of the President as affecting the security of the United States"[125] to "any person such officer or employee knows or has reason to believe to be an agent or representative of any foreign government" without specific authorization from the President or other specified authority.[126] Section 783 (b) makes it criminal for an "agent or representative of a foreign government knowingly to obtain or receive or attempt to obtain or receive from any officer"[127] classified information unless special authorization was received from "the head of the department, agency or corporation having custody or control over such information."[128] The penalty for violation of any provision within the statute is a fine of up to $10,000 and imprisonment of up to

---

[120]42 U.S.C.A. § 2274(a) (West 2001).

[121]*Id*.

[122]*Id*.

[123]42 U.S.C.A. 2274(b) (West 2001).

[124]*See The Espionage Statutes*, *supra* note 63, at 1075.

[125]50 U.S.C.A. § 783(a) (West 2001).

[126]*Id*.

[127]50 U.S.C.A. § 783(b) (West 2001).

[128]*Id*.

ten years.[129] Like the Restricted Data statutes, the "reason to believe" language seems to indicate that recklessness or negligence may suffice to convict.

Finally, there is one last statute that the government attempted to apply against government employees who have leaked classified information. Section 641 of Title 18 is a statute designed to punish persons whom embezzle or convert any "record, voucher, money or thing of value" for their own use or the use of another.[130] The punishment under the statute is a fine or imprisonment up to ten years, unless the value of the "property" is less than $1,000, in which case the penalty is a fine or imprisonment of up to one year.[131]

In summary, the perceived problems with the statutes are threefold. First, due to their ad hoc nature and the number of statutes enacted, it is difficult to determine which statutes, if any, should apply to government employees who leak information to the press. Second, the statutes provide little guidance in their language for how courts should apply them in such situations. Judges tend to defer to the executive branch because there is no clear congressional guidance and judges are concerned about fashioning doctrine in areas where they have little expertise.[132] Third, this coupled with the fact that the government has rarely attempted to prosecute employees who leak classified information to the press under these statues, means that the statutes have not, in many instances, been tested to see if they are effective against those who leak classified information.

V. USING WHAT'S IN THE TOOLBOX—PROSECUTIONS OF "LEAKERS" UNDER EXISTING LAW

The applicability of the statutes discussed in the previous section is, for the most part, open to speculation, because they have been used on only two occasions to pursue prosecution against a government employee who leaked classified information to the press. The first case, involving the prosecutions of Ellsberg and Russo for leaking the Pentagon Papers to the *Washington Post*, was dismissed, without a hearing on its merits.[133] The second case, *United States v. Morison,*[134] is extraordinarily important, because it demonstrates the reasoning one court used to

---

[129]50 U.S.C.A. § 783 (West 2001).

[130]18 U.S.C.A. § 641 (West 2001).

[131]*Id.*

[132]*See* Eric E. Ballou & Kyle E. McSlarrow, *Plugging the Leak: The Case for a Legislative Resolution of the Conflict Between the Demands of Secrecy and the Need for an Open Government,* 71 VA. L. REV. 801 (1985) (hereinafter *Plugging the Leak*). The authors set forth two underlying purposes for the court's deference to the Executive; a concern about separation of powers, recognizing that the Executive Branch's primarily responsibility for national defense and foreign policy, as well as what the authors describe as judiciary's self-perceived "institutional incompetence", whereby the courts will not interfere unless there is a separate constitutional issue. *Id.* at 828-29.

[133]Topol, *supra* note 5, at 588. Topol notes that after the Government was not granted the injunction against the New York Times and the Washington Post, they attempted to pursue prosecution against Ellsberg and Russo for their roles in the Pentagon Papers episode, but the case was dismissed as the result of "extreme government misconduct." *Id.*

[134]*Morison*, 844 F.2d at 1057.

apply existing statutes to exactly the situation the Classified Information Protection Act purports to correct, that is, leaks of classified information from a government employee to the press. It also marks the first successful, and as it turns out, only prosecution by the government of any person under sections 793 (d) and (e), as well as under the section 641 conversion statute for leaking information to anyone who was not an agent of a foreign government.[135]

Morison was employed at the Naval Intelligence Support Center for ten years with a Top Secret Security Clearance.[136] In contemplation of receiving this clearance, he signed a Non-Disclosure Agreement and was given clear instruction into the proper procedures for determining both who was authorized to receive disclosure and the consequences for failing to comply with these procedures.[137] He later, with the approval of the Navy, became engaged as a consultant with *Jane's Fighting Ships*, a British annual specializing in reporting on current developments in international naval operations.[138] The Navy approved the arrangement on the condition that Morison would not use classified information on the U.S. Navy, or "extract unclassified data on any subject and forward it to *Jane's*."[139] Morison's arrangement with *Jane's*, prior to committing the act for which he was prosecuted, was informal, with *Jane's* paying him varying amounts for the information supplied.[140]

The arrangement eventually became a point of contention between Morison and his superiors and, as a result, when Morison learned that *Jane's* was to begin publishing a weekly magazine, he arranged a meeting with *Jane's* editor, Derek Wood, to discuss the possibility of employment with the new venture.[141] At the meeting, Wood asked about an explosion at a Soviet naval shipyard, and stated that he believed the explosion was very serious.[142] Morison indicated that the explosion was far more serious than had been reported and offered to provide additional material to Wood if he was interested, though no compensation was discussed at the time.[143] Wood indicated that he would like to see additional information relating to the explosion and, pursuant to that end, Morison provided approximately three pages of background material about the base where the explosion occurred,[144] at least some of which was later found to have been extracted from a secret report found in Morison's home.[145] Morison also provided Wood information about two other

---

[135] *Id.*

[136] *Id.* at 1060.

[137] *Id.*

[138] *Id.*

[139] *Morison*, 844 F.2d at 1060.

[140] *Id.*

[141] *Id.* at 1060-61.

[142] *Id.* at 1061.

[143] *Id.*

[144] *Morison*, 844 F.2d at 1061.

[145] *Id.* at 1062.

explosions, which had previously occurred there, as well as information about a similar explosion that took place in East Germany.[146] Subsequent to sending this material, Morison discovered on the desk of another analyst, a satellite photograph of a Soviet carrier under construction at the shipyard where the explosion took place.[147] Morison took these photographs from his co-worker's desk, cut off the borders indicating that the photos were both classified and were taken according to a secret method, and mailed them to Wood.[148] The photographs were subsequently published in *Jane's* and eventually, *The Washington Post*.[149] Morison received $300 for his services.[150] Once published, the Navy conducted an investigation, which eventually pointed to Morison. When initially confronted with the evidence against him, Morison denied having taken the photographs.[151]

Morison was eventually convicted on two counts under sections 793 (d) and (e). Section (d) was applied as to the photographs, as he arguably had authorized possession. Section (e) was applied as to the secret reports, because he had retained them without authorization. Morison challenged these convictions on the grounds that sections 793 (d) and (e) did not apply to his actions because they, like the other provisions of the Espionage Act, if properly read, applied only to cases involving classic espionage.[152] He argued that, by virtue of the fact that he disclosed information to the press and not a foreign agent or government, his actions did not fall under the ambit of the statutes.[153]

The court refused to accept these arguments, relying instead on the "plain language" of each section, particularly the language "to a person not entitled to receive it" to uphold Morison's conviction under 793 (d) and (e).[154] The court additionally stated that because the statutes should be construed *in pari materia* with the other provisions of the act,[155] and because the language under section 794 covers communication to a foreign agent or government, that section 793 cannot apply strictly to classic espionage, but rather to the distinct offenses of communication to unauthorized persons and unauthorized retention.[156] The court believed that section

---

[146]*Id.* at 1061.

[147]*Id.*

[148]*Id.*

[149]*Morison*, 844 F.2d at 1062.

[150]*Id.* at 1061.

[151]*Id.* at 1062.

[152]*Id.* at 1063.

[153]*Id.*

[154]*See Morison*, 844 F.2d at 1063 (finding that "The language of the two statutes includes no limitation to spies or to 'an agent' of a foreign government' either as to the transmitter or the transmittee of the information and they declare no exemption in favor of one who leaks to the press. It covers 'anyone'. It is difficult to conceive any language more definite and clear.")

[155]*Id.* at 1064.

[156]*Id.* at 1065.

793, while broad and general in its scope could be used to prosecute government employees who leak information to the press, if the proper limiting instructions are used.[157]

Morison made an additional argument that subsections 793(d) and (e) did not apply to him. He argued that there had been only one previous attempt to prosecute anyone who had disclosed to a party other than an agent of a foreign government (Ellsberg and Russo), and that case was dismissed, whereas the sections had previously only been applied successfully against individuals who disclosed information to agents of foreign governments.[158] Therefore, he argued, the failure to prosecute anyone else for disclosing information to a person other than an agent of a foreign government meant that the statute did not apply to non-espionage disclosures.[159] The court rejected this argument, holding that the lack of prosecution was not because of any lack of applicability of the statute, but rather a reflection of both the difficulty of proving violations under these sections, as well as the government's problem of "balancing the need for prosecution against the possible damage that a public trial will require by disclosure of vital national interest secrets."[160] The court also rejected Morison's First Amendment arguments under the statute by stating that the First Amendment is not meant to "confer a license on either the reporter or his news source to violate valid criminal laws."[161]

In addition to upholding the conviction of Morison under sections 793(d) and (e), the court also upheld his conviction under section 641, for converting the satellite photographs, which the court ruled were government property, that the defendant converted for his own use.[162]

If a literal reading of the statutory language is accepted, Morison's conviction under the statute is proper, at least in regard to sections 793 (d) and (e), because Morison arguably had "reason to believe that the information could be used to the injury of the United States or the advantage of a foreign nation,"[163] because the items he transmitted, clearly indicated that they involved the use of intelligence sources and methods. In addition, though this is not relevant to the terms of the statute itself, Morison's motivations for committing his acts also seem more within the realm of traditional espionage behavior than someone leaking information to expose government wrongdoing. Despite Morison's subsequent claims that his purpose was "to alert the public that the Soviet Union was preparing to vastly expand its naval reach, and that he took no payment for the photographs,"[164] the trial court found evidence to the contrary. As Judge Russell stated, "the record affords substantial

---

[157]*Id.* at 1070-73.

[158]*Morison*, 844 F.2d at 1066.

[159]*Id.*

[160]*Id.* at 1067.

[161]*Id.* at 1069 (quoting Justice White in *Branzburg v. Hayes,* 408 U.S. 665 (1972))..

[162]*Id.* at 1077.

[163]18 U.S.C.A. §§ 793(d)-(e) (West 2001).

[164]Vernon Loeb, *Clinton Ignored CIA in Pardoning Intelligence Analyst; Clemency for Only Official Convicted of Leaking Classified Information to Media Draws Criticism*, WASHINGTON POST, Feb. 17, 2001 at A06.

evidence... that the defendant in this case was not fired by zeal for public debate ... he was motivated not by patriotism and the public interest, but by self-interest."[165] This was a result of Morison volunteering the information to Wood as part of an effort to help him secure a job with *Jane's*, as opposed to motivation to uncover government misconduct or alert the public to a danger that could not be communicated by other means. In the sense that the evidence pointed in this direction, Morison's behavior is not much different from the "classic spy," who in many instances is motivated, if not by hatred for the United States and its policies, than at least by personal gain. Finally, though Judge Wilkinson's concurrence states that the First Amendment implications of Morison's prosecution under the statute should not be so quickly dismissed, because "the undeniable effect of the disclosure was to enhance public knowledge and interest in the projection of Soviet sea power,"[166] disclosure to a British publication of limited circulation would not likely serve to foster debate among United States citizens, except in the most limited circles.

The court's upholding of the conviction under section 641 by contrast is more problematic. By defining the photograph as a "thing of value" the *Morison* court stretches the terms literal meaning, as the statute itself specifically defines the term "value" as "face, par, or market value, or cost price, either wholesale or retail, whichever is greater."[167] Because the government cannot readily place a market value on a satellite photograph, or perhaps because Morison received $300 after the fact or because he received compensation for his contributions to *Jane's* as a matter of pattern or practice, it appears that the court's application of the term "thing of value" is, at best, a strained interpretation of the statutory language. Other courts, however, are sharply divided on the actual scope of the phrase, with some courts refusing to discuss section 641 on its merits when the defendant is convicted on other charges.[168] Furthermore, the applicability of both section 793 and section 641 against leaks of classified national security information to the press was thrown into serious doubt, when on his last day in office, President Clinton pardoned Morison creating a firestorm of criticism within the intelligence community.[169]

As will be discussed, though the statute is flawed, prosecution under section 793 represents a far better alternative to the blanket prohibitions of the Classified

---

[165]*Morison*, 844 F.2d at 1077.

[166]*Id.* at 1081.

[167]18 U.S.C.A. § 641 (West 2001).

[168]*See generally* United States v. Truong Dinh Hung 629 F.2d 908 at 927 (4th Cir. 1980) (stating that "because § 641 would disturb the structure of the criminal prohibitions Congress has erected to prevent some, and only some, disclosures of classified information, the general anti-theft statute should not be stretched to penalize the unauthorized disclosure of classified information.") *See also* Boyce v. United States, 594 F.2d 1246 (9th Cir. 1979). The propriety of conviction under § 641 not reached since he was convicted under §§ 793, 794, and 798 and sentences ran concurrently. *Id. But see*, United States v. Lambert 446 F. Supp. 890 (D. Conn. 1978) (finding that information derived form a DEA computer was both a thing of value and a record under § 641 and therefore the statute could be applied to convict, with proper limiting instructions.)

[169]*See* Loeb, *Clinton Ignored CIA in Pardoning Intelligence Analyst*, *supra* note 164, at AO6.

Information Protection Act for prosecution of government employees who leak classified information to the press. Ideally, an amendment to section 793, if narrowly tailored to specific acts of disclosure, would be a far better alternative, because it does not abandon the scienter requirement.

VI. NON-STATUTORY TOOLS TO PREVENT DISCLOSURE: PREPUBLICATION REVIEWS AND ADMINISTRATIVE SANCTIONS

The government has other means to protect against leaks of classified national defense information by government employees. Congress has given authority to the heads of agencies, under several statutes to promulgate measures to protect classified national security information and explicitly created certain sanctions to protect them.[170] The primary statute and the greatest source of adjudication is section 403 of Title 50 (The National Security Act), which describes the authority of the Director of the CIA.[171]

More frequently used controls over an employee's disclosure of classified information, particularly within the context of the CIA, are pre-publication review agreements. These agreements provide, as a pre-condition of employment, that prospective employees agree not to disclose any classified information that they may learn through the course of their employment. Generally, the agreements have been adjudicated in the context of former agency employees.[172]

The first major challenge on First Amendment grounds to these non-disclosure agreements occurred in the Fourth Circuit case, *Marchetti v. United States*.[173] In *Marchetti*, the plaintiff, a fourteen year employee of the CIA, signed an agreement when he joined the agency agreeing not to divulge classified information without the express authorization of the Director or his authorized representative, and Marchetti also signed a secrecy oath when he resigned.[174] After his resignation, Marchetti wrote a novel about an agency very similar to the CIA.[175] He also wrote articles for

---

[170]*See generally* 50 U.S.C.A. § 435 (West 2001) (Congress not only grants the President the ability to establish procedures protecting classified information by means of executive order, but also grants the heads of agencies with control over classified information to deny or terminate security clearances in the interests of national security. *Id.*); 5 U.S.C.A. § 7532 (West 2001) (authorizing the Secretary of Defense authority to terminate or suspend employment of any National Security Agency officer or employee "in the interests of the United States" or "in the interests of national security").

[171]The National Security Act of 1947, 50 U.S.C.A. § 403 (West 2001) (giving the director of the CIA the authority to prescribe appropriate security measures for agency employees and contractors, take measures to protect intelligence sources and methods, and terminate the employment of any officer and employee in the interests of national security).

[172]*See*, *e.g*., Snepp v. United States, 444 U.S. 507 (1980); Marchetti v. United States, 486 F.2d 1309 (4th Cir. 1972).

[173]486 F.2d 1309.

[174]*Id*. at 1312. The relevant part of the secrecy agreement read as follows: "I do solemly swear that I will never divulge, publish or reveal either by word, conduct, or by any other means, any classified information…except in the performance of my duties…unless specifically authorized in writing, in each case, by the Director of Central Intelligence, or his authorized representatives." *Id.*

[175]*Id*. at 1313.

magazines and conducted interviews relating to his experiences as an agent, which the government claimed contained classified information,[176] and also submitted a proposal to a publishing house for a non-fiction account of his experiences as an agent.[177] The government subsequently sought a temporary restraining order against Marchetti for publishing classified information in violation of his secrecy agreement and secrecy oath, until such time as the agency could review the content of his proposed book to determine that he did not divulge classified information.[178] Marchetti then challenged the order as a violation of his First Amendment rights to criticize the government.[179] Unlike in the *Pentagon Papers*, the court relied on contract theory to uphold the prior restraint imposed by the secrecy agreement Marchetti signed as a condition of employment, but refused to uphold the secrecy oath, on the basis that there was no consideration for that agreement.[180] The court concluded that the secrecy agreement was a valid exercise of the CIA's authority to protect intelligence sources and methods as authorized by the National Security Act.[181] The court, in declining enforcement of the secrecy oath, stated that Marchetti should be allowed the ability, like other citizens to criticize the government to the extent that his criticisms do not disclose classified information that is not already in the public domain.[182] Furthermore, while the court stated that Marchetti's right to publish should not be unduly delayed, and that he should be able to challenge any action of the CIA disapproving publication in court, it effectively foreclosed this remedy by declaring its belief that, in general, courts were incompetent to adjudicate the propriety of classification in matters of foreign intelligence.[183]

The courts have subsequently determined that, while *de novo* review is authorized by the Freedom of Information Act, the agency's determination should be upheld for information that is "properly classified or classifiable,"[184] and that the classification scheme established by executive order should be reviewed by balancing the government's substantial interest in assuring the secrecy of intelligence operations against the former agent's First Amendment interest in public disclosure,

---

[176]*Id.*

[177]*Marchetti*, 466 F.2d at 1313.

[178]*Id.* at 1311.

[179]*Id.* at 1312.

[180]*Id*. at 1311.

[181]*Id.* at 1316.

[182]*Marchetti*, 466 F.2d. at 1317.

[183]*Id.* at 1317 – 18.

[184]Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir. 1975). *Colby* was a companion case to *Marchetti*, in which the publisher sought to challenge the propriety of the CIA classification scheme and made clear that the presumption was heavily in favor of the classifying agency. The court recognized that information in a classified document, regardless of the level of sensitivity, takes on the character of the most sensitive information contained in the document, and it is irrelevant whether such information was classified at the time of the agent's service or at some time thereafter, as long as he had knowledge of the information at the time he served. *Id.*

thus requiring that the agency only show a logical relationship between the censored information and the reasons for classification.[185]

The problem with such prepublication review schemes is that no statute authorizes them. Section 403-3 of Title 50 merely states that the Director shall "protect intelligence sources and methods from unauthorized disclosure."[186] In light of First Amendment concerns, this grant of authority, because of its non-specific terms, is especially broad. This, coupled with the fact that courts are reluctant to second-guess the Executive Branch, allows them free rein to apply this scheme against any views it may deem contrary to its mission. As Professors Edgar and Schmidt noted:

> We do not view this system of prior restraints as necessarily unsound as a matter of policy, although we have doubts. Nor do we believe that the courts should invalidate such a program on First Amendment grounds if Congress authorized it in reasonably clear terms … Private employment contracts frequently impose secrecy obligations which courts routinely enforce…on the other hand, one can be sure that a prepublication clearance system with the CIA will be a disaster to core First Amendment values…the problems endemic to wholesale administrative censorship will flourish in this context; and doubts will be resolved in favor of suppression … bureaucratic self-interest will result in selective enforcement … and decisions will be made behind a veil of secrecy … the process will be expensive, debilitating and chilling.[187]

Many of these fears came to fruition in *Snepp v. United States*.[188] Frank Snepp was a former CIA agent who, like Marchetti, signed a secrecy agreement upon hire and signed another secrecy agreement upon his employment termination.[189] Snepp subsequently published a book, *Decent Interval*, based upon his experiences as an agent and criticized CIA activities in South Vietnam.[190] Unlike Marchetti, however, who submitted his manuscripts to the CIA for review prior to publication, Snepp did not.[191] The government stipulated that Snepp did not violate his agreement by virtue of publication of classified material, but rather because he breached a trust by virtue of the agreement, by not submitting any manuscripts to the pre-publication review to which he agreed.[192] At the time, Snepp received $60,000 in advance payments from his publisher.[193] The Supreme Court, in a startling per curiam opinion, held that

---

[185]McGehee v. Casey, 718 F.2d 1137 (D.C. Cir. 1983).

[186]50 U.S.C.A. § 403-3(c)(7) (West 2001).

[187]*See Curtiss-Wright Comes Home*, *supra* note 14, at 367-68.

[188]Snepp, 444 U.S. at 507.

[189]*Id*. at 508.

[190]Anthony R. Klein, Comment, *National Security Information: It's Proper Role and Scope in a Representative Democracy*, 42 FED. COMM. L.J. 433 at 443 (1990).

[191]*See Curtiss-Wright Comes Home*, *supra* note 14, at 371.

[192]*Snepp*, 444 U.S. at 510.

[193]*Id.* at 508.

Snepp, though he had not published any classified information, had deliberately violated his position of trust with the CIA by failing to submit his manuscript for prepublication review.[194] Relying on the trial testimony of Stansfield Turner, then director of the CIA, the Court agreed with the lower court's finding that by failing to give the agency the opportunity to determine whether the book's disclosure of unclassified information would compromise any classified information within the agency, Snepp compromised the effectiveness of the agency's operations,[195] though it was later admitted that Snepp was singled out for prosecution, as opposed to others, because his publication criticized the CIA.[196] The Court approved a constructive trust against Snepp, whereby Snepp was required to disgorge any profits he received from the publication of the book to the CIA.[197]

Justice Stevens, in response to this extraordinary remedy, strongly dissented, claiming that the Court had fashioned a remedy inconsistent with existing contract, statutory, or common law,[198] which enabled the Court to impose penalties for alleged injuries that were not contemplated in the agreement.[199] Justice Stevens was additionally troubled by the Court dismissal of Snepp's First Amendment rights by asserting a remedy that was not consonant with existing jurisprudence concerning prior restraints.[200] By doing so, the Court essentially gutted the ruling of the Pentagon Papers in relation to the speech rights of government employees who merely have access to classified information. From this precedent, any agency that classifies information, can impose similar restraints on their employees through invocation of secrecy agreements.

In addition, each agency dealing with classified information has its own regulations authorized by statute for dealing with employees who disclose classified information, with penalties ranging from revocations of security clearances to suspension or dismissal from employment.[201] Unlike the pre-publication review scheme used by the CIA, these regulations do not implicate the Court's presumption, strong or not, against prior restraints, though they are arguably consistent with the rule set forth in *Pickering* and *Connick,* because the statutes authorizing them contain due process for the employee sanctioned.[202] As such, these regulations are the most common form of discipline used against employees who "leak" information.

---

[194]*Id*. at 511.

[195]*Id*. at 511-12.

[196]Klein, *supra* note 190, at 444.

[197]*Snepp*, 444 U.S. at 514.

[198]*Id*. at 517.

[199]*Id*. at 522.

[200]*Id*. at 526.

[201]*See*, *e.g.*, Du Val *supra* note 6, at 672-3. Du Val maintains that informal and administrative sanctions are the principal methods of controlling dissemination of classified information. *Id.*; Charlson, *supra* note 11, at 1014-15. (existing sanctions include revocation of security clearances and discharge from employment).

[202]*See*, *e.g.*, Department of Navy v. Egan, 484 U.S. 518 (1987).

VII. THE CLASSIFIED INFORMATION PROTECTION ACT – FIXING LEAKS WITH A HAMMER?

Amid this morass of statutes, agency regulations and secrecy agreements, and judicial interpretations over key statutory terms since the original Espionage Statutes were enacted in 1917, comes the proposal for a new anti-leak statute, the Classified Information Protection Act of 2001. The best way to examine the likely effects of this statute, both intended and unintended, is to examine the plain language of the bill, because the legislative history is minimal. There are two reasons for this approach. First, because the bill is an amendment to the Espionage Statutes, and the courts have, for the most part, regardless of the legislative history, looked to the plain meaning of the text for guidance. Second, the legislative history for the proposed bill is virtually non-existent. In the absence of any debates on record for the current version of the bill, the small amount of legislative record for the vetoed Senate bill from 2000[203] will have to suffice, but it lends little to the discussion.[204]

A. Who Does the Statute Cover?

The initial question to be answered is, who is the statute supposed to cover? The relevant text of the statute reads, "Whoever, being an officer or employee of the United States, a former or retired officer or employee of the United States, any other person with authorized access to classified information or any other person formerly with access to classified information."[205] According to the definitions section, officer or employee are defined in 5 U.S.C. §§ 2104 and 2105. Section 2104 defines "officer" as a "justice or judge of the United States and an individual who is required by law to be appointed in the civil service"[206] by the President, a court, an agency head, or the secretary of a Military department, if they are performing a federal function.[207] "Employee" is likewise defined as an individual engaged in a federal function who is appointed by any of the following; the President, Congress, a member of the uniformed service, any other employee as defined by the section, the head of a Government-controlled corporation, or an adjutant general.[208] This is an extremely broad classification and could include anyone from the current or former Secretaries of Defense, all the way down to the lowest level bureaucrat.

The prohibition further applies against "any other person with authorized access, or any other person formerly with authorized access" to classified information.[209] The statute defines "authorized" as those:

> Having authority or permission to have access to the classified information pursuant to the provisions of a statute, Executive order, regulation or directive of the head of any department or agency who is

---

[203] S. 2507, 106th Congress (2001).

[204] *See* 146 Cong. Rec. S 9684 (daily ed. October 3, 2000) (statement of Sen. Biden).

[205] *See* H.R. 2943, 107th Cong. (2001).

[206] 5 U.S.C.A. § 2104 (West 2001).

[207] *Id.*

[208] 5 U.S.C.A. § 2105 (West 2001).

[209] *See* H.R. 2943, 107th Cong. (2001).

> empowered to classify information, an order of any United States court, or a provision of any Resolution of the Senate or Rule of the House of Representatives which governs release of classified information by such House of Congress.[210]

This is also impermissibly vague. According to this definition, the statute would theoretically cover independent contractors and scientific researchers working on defense or intelligence related technology, but not technically officers or employees. The statute is probably meant to cover these individuals. The statute, as written however, if taken to admittedly unusual extremes, could theoretically also apply to members of Congress and certainly members of their legislative staff, because in many cases, their authority or permission to have access to such information is based upon statutes, Executive orders, regulations or directives.

Because it is clear that Congress did not intend to make itself criminally liable under the bill, the "cure" for leaks that the statute allegedly provides may well be incomplete, as evidenced by a recent episode. In two separate incidents since the September 11 attacks, members of Congress themselves ran afoul of the President for disclosing allegedly "classified information" to the press. In the first instance, the administration criticized Senator Orrin Hatch, who, after attending a classified briefing, disclosed to the media that he had seen concrete evidence linking the attacks to Osama bin Laden.[211] The other instance arose from a statement made by Senator Shelby, the original sponsor of the leak legislation, that Americans could expect further terrorist attacks following military action in Afghanistan.[212] While most now agree that the information disclosed in the second incident was not technically classified, the Bush administration used these incidents as basis of a threat to restrict access to military and intelligence data, to eight ranking members of Congress,[213] before eventually relenting.

These episodes illustrate three points. First, if these disclosures were, in fact, disclosures of classified information, whether damaging to national security or not, it would have made it a crime for "officers" and "employees" but not for members of Congress, whose act of leaking information is more likely to be politically motivated than that of an executive branch bureaucrat. Second, it illustrates how relatively benign disclosures can potentially take on the character of a crime under the statute, especially where information is obviously in the public's interest to know, thus bringing into question concerns of overbreadth. Third, despite the fact that courts give great deference to the judgment of the Executive Branch in matters of national security, it calls into serious question whether the Executive's reasoning for classifying this type of information is legitimate under the circumstances, because the public's interest in knowing the details of this information is more compelling than the government's interest in keeping it secret.

---

[210] *Id.*

[211] Editorial, *Leaking and Spinning*, ST. PETERSBURG TIMES, October 12, 2001, at 18A.

[212] Sara Fritz, *Bush Backs Down on Stopping Leaks*, ST. PETERSBURG TIMES, October 11, 2001, at 1A.

[213] *Id.*

B. What Does the Statute Cover?

The second question is, what does the statute cover? This provides potentially greater problems. The statute prohibits willful disclosure or attempts to disclose, "*any* classified information to a person other than an officer or employee of the United States, knowing that the person does not have authorized access to such classified information."[214] The only intent requirement in the statute is willful communication to an unauthorized person. Therefore, disclosures to the press or the public would be punishable under the statute, thus implicating First Amendment rights. Unlike section 793 (d) of the Espionage Act, there is no requirement that the person have knowledge or even reason to believe that the information could be used to the injury of the United States. Thus, any disclosure is punishable, regardless of the degree of harm, and the government does not have to prove any harmful purpose. This would open the door to selective prosecution because the government could, at its election, quietly punish by sanction those disclosures that do not bring the policies of the Executive branch into question, while allowing for prosecution of people like Ellsberg, whose disclosure, in retrospect caused no identifiable damage to national security, but merely called into question the actions of the Executive branch and certainly was relevant for the purposes of informed debate of government policy. As one commentator noted, "Congress should be guided by the principle that liability should extend only to the conduct that is likely to harm national security…when someone is subject to a criminal sanction, there should be no reasonable doubt as to the harmful consequences of his act.[215]

C. What Constitutes Classified Information?

Finally, there is the issue of "classified information." It is widely accepted that the classification system, as it is currently constituted, has a tendency to overclassify information.[216] The former head of the Information Security Oversight Office noted that there were over 8 million secrets classified in 1999 alone.[217] Furthermore, there was, until recently, no principled means of declassifying information.[218] As a result, the declassification of information, that would be subject to the statute lags far behind the ability to declassify it.

One absurd example of the failure to declassify is that the total intelligence budget for 1947 remained classified as of 2000.[219] Thus under the statute, as literally construed, a former employee of the CIA who had access to this information when classified and later disclosed it could be subject to prosecution. While it is fairly safe to say that courts and prosecutors would not punish the individual under such

---

[214]*See* H.R. 2943, 107th Cong. (2001).

[215]*See Plugging the Leak*, *supra* note 132, at 855.

[216]*See*, *e.g.*, Xanders *supra* note 11, at 768-69; *Moynihan Report, supra,* note 50, at xxi (Summary of Findings and Recommendations).

[217]David Wise, Editorial, *The Secrecy Police Will be Back Soon*, LOS ANGELES TIMES, December 10, 2000, at M2.

[218]The Public Interest Declassification Act of 2001, 106 P.L. 567 (2000).

[219]Steven Aftergood, Commentary, *The Big Chill; Anti-Leak Proposal Threatens Good Government*, WASHINGTON TIMES, August 27, 2001, at A19.

circumstances, there may be situations where other types of information of more recent vintage remain classified, which the former employee would not appreciate. Publication would subject a former employee to pre-publication review as under *Snepp*. However, if a former employee gave an interview to a magazine like Marchetti, could the employee be subject to criminal penalty under the new statue? Under the proposed bill, he most likely would.

The other side of the equation is the classification system itself. Because the responsibility for classification of information has largely been delegated to the President, he is generally free to make his own determinations as to the amount and level of classification required. Since the beginning of the use of Executive orders governing classification of national security information, each succeeding administration has a different idea of the parameters of what should be classified.[220] Given this fact, if H.R. 2943 is enacted, there would be "an egregious effect on First Amendment freedoms ... not only would such measures allow the secrecy-oriented executive branch to subordinate ... the public's need for open debate, but under the current approach to classification, invariable First Amendment interests would become subject to the vicissitudes of consecutive administrations."[221]

Another complicating factor is the broad discretion within agencies in determining when or whether to classify information. As one report stated, as of 1997, an estimated three million government and industry employees today have the potential ability to mark information as classified.[222] This raises some interesting dilemmas. As former Secretary of Defense Cohen noted in a recent article,

> [I]nformation can be classified in one context and not be (or appear not to be) in another … it is not uncommon for different agencies to assign different classification levels to essentially the same information, and in some cases, information that one agency might determine to be unclassified might be considered classified by another agency.[223]

This, combined with the courts' reluctance to second-guess the propriety of classification at the agency level,[224] creates practical difficulties in enforcement. The question becomes, does the government pursue prosecution on the basis of which department the employee works in? If the purpose of the statute is to protect classified information, the statute ultimately fails, because it cannot be applied against an individual for whom the information is not classified and then punish unfairly the individual for whom the information is classified. In summary, because the Executive branch both creates the guidelines for classification and is responsible for punishment, enactment of H.R. 2943 gives reason to "doubt the wisdom of the

---

[220]*See generally*, *Moynihan Report, supra* note 50, at 11-12 (for a discussion of the key differences between Executive Orders that have been in effect since 1951).

[221]Xanders, *supra* note 11, at 772.

[222]*Moynihan Report*, *supra* note 50, at 31.

[223]William S. Cohen, Editorial, *National Secrets, Too Frequently Told*, NEW YORK TIMES, September 5, 2001, at A19.

[224]*See*, *e.g.*, McGehee v. Casey, 718 F.2d 1137 (D.C. Cir. 1983); Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962); *Boyce*, 594 F.2d at 1246.

fox to define the parameters of – not to mention guard – the chicken coop."[225] As currently formulated, the statute operating in the context of the classification system as it exists, would exert a chill on legitimate speech and would be akin to using a hammer to fix a leak – an inappropriate and ineffective tool, given the circumstances.

VIII. CONCLUSION

Clearly, under the existing framework of the executive classification system, the Classified Information Protection Act sweeps too broadly and would chill discourse by adversely affecting the citizen's legitimate right to speak on matters of public interest, and would interfere with the ability of the press to inform the populace. Therefore, the bill should be rejected. This is not to say that the government does not have a legitimate need to protect national security interests. There are, however, already many more narrowly tailored statutes on the books, which protect the most critical kinds of information from disclosure. Atomic secrets are protected. Cryptological information is protected. The identities of agents are protected. National Defense information, broadly defined in *Gorin*, is protected. The espionage statutes have been used against government employees who leaked sensitive information to the press. Administrative sanctions are in place, but it is unclear the extent to which they are used, because those matters are secret. As John Martin, formerly the top official for the Justice Department responsible for supervision of the investigation of leaks and espionage stated, "the real problem with leaks has not been a lack of statutory sanctions but the lack of will on the part of agency heads and Cabinet secretaries to enforce security regulations."[226]

According to an Intelligence Committee position paper supporting the original version of the Classified Information protection Act, current law does not cover "leaked intelligence information regarding sources and methods, counter-narcotics, counterintelligence capabilities and liaison relationships with foreign intelligence groups, because they don't fall within the definition of the term 'national defense information.'"[227] If that is true, then why not propose specific statutes, like the Intelligence Identities Protection Act, which narrowly target specific identifiable threats to national security, rather than a blanket prohibition on speech? Entirely new statues can be written or Congress can amend terms, such as "national security information," within the statutes. Not only would this eliminate guesswork on the part of the courts but it would, preserve the important requirement that the person have knowledge or reason to believe that the information can be used to the injury of the United States.[228]

The only other alternative to save such a broad statute would be for Congress to take the lead in setting forth a consistent and principled framework governing Executive classification decisions.[229] The argument has been made that, of all our institutions, Congress is best equipped to balance the needs for secrecy and the need

---

[225]*See Curtiss-Wright Comes Home, supra* note 14, at 354.

[226]Pincus & Loeb, *supra* note 40.

[227]*Id*.

[228]18 U.S.C.A. § 793(d) (West 2001). This formulation would be consistent with the section 793(d) scienter requirement.

[229]*See Moynihan Report, supra* note 50, at xxii-xxiii (discussing one such framework.)

for information to fuel public debate, as it is most sensitive and accountable to democratic principles.[230] When considering matters of government secrecy, Congress and the Executive would be wise to follow the admonition of Justice Douglas when he said, "Secrecy in government is fundamentally anti-democratic, perpetuating bureaucratic errors. Open debate and discussion of public issues are vital to our national health."[231]

MITCHELL J. MICHALEC[232]

[230] *See*, *e.g.*, *Plugging the Leak*, *supra*, note 132.

[231] *Pentagon Papers*, 403 U.S. at 724.

[232] J.D., Cleveland-Marshall College of Law, December 2002. The author wishes to thank his wife, Patty and children, Katie, Emily and Colin for their love, encouragement and support during law school. He would also like to gratefully acknowledge the contributions of Deborah Klein, Legal Writing Instructor, in the preparation of this Note.