Plugging the Leak: The Case for a Legislative Resolution of the Conflict between the Demands of Secrecy and the Need for an Open Government
Author(s): E. E. B. and K. E. M.
Reviewed work(s):
Published by: Virginia Law Review
Stable URL: http://www.jstor.org/stable/1073013
Accessed: 09/04/2012 11:13

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.
NOTE

PLUGGING THE LEAK: THE CASE FOR A LEGISLATIVE RESOLUTION OF THE CONFLICT BETWEEN THE DEMANDS OF SECRECY AND THE NEED FOR AN OPEN GOVERNMENT

Several years ago, the Central Intelligence Agency (CIA) secretly financed the construction of a multi-million dollar deep-sea salvage vessel. During the summer of 1974, the vessel was used to recover a Soviet submarine that sank off the coast of Hawaii in 1968.1 The submarine was believed to carry hydrogen-warhead missiles as well as important cryptographic information and code-books. This salvage operation was known as "Project Jennifer."2

Project Jennifer was only a partial success. Although it retrieved one-third of the vessel and several nuclear torpedoes, the CIA could not recover the missiles or codebooks.3 Several reporters obtained information from government officials about the operation. These reporters were subsequently advised by CIA Director William Colby that public disclosure before the completion of the operation would adversely affect the national security.4 In spite of this warning, however, the Los Angeles Times disclosed all of the information it possessed relating to Project Jennifer.5

As a result of the news media's disclosure, Soviet signal vessels soon patrolled the salvage site.6 The CIA abandoned plans to finish the salvage operation both to avoid a confrontation with the Soviets and because the

---

1 N.Y. Times, March 19, 1975, at 1, col. 8. The cost of the operation was believed to be $250 million to $350 million. Id. at 52, col. 1.
2 Id. at 1, col. 8.
3 Id.
4 Id. at 52, col. 1.
5 Id. Publication of secrets in spite of national security concerns is fairly common. The most recent example is the Washington Post's controversial decision to print highly sensitive information regarding upcoming space shuttle missions. Wash. Post, Dec. 19, 1984, at A1, col. 6. This article disclosed information on a new military intelligence satellite, including aspects of its position in orbit. Id. Several news organizations and magazines obtained the information and were asked by Pentagon officials to withhold the stories for national security reasons. N.Y. Times, Dec. 20, 1984, at B12, col. 1. All did so, except the Washington Post. Id.
Soviet presence rendered the operation impractical.\(^7\) To the critics of the operation, Project Jennifer's early termination was undoubtedly welcome. Many critics maintained that the operation jeopardized the fragile detente established with the Soviets.\(^8\) Despite these fears, there was no indication that the Soviets knew of the submarine's location or its attempted salvage. According to CIA Director Colby, the acquisition of the submarine, its missiles, and its codebooks would have "been the biggest single intelligence coup in history."\(^9\) Instead, the news media's disclosure had quite another impact: it deprived the government of the opportunity to acquire valuable intelligence information.

The disclosure by government officials and the publication of the details of "Project Jennifer" provide only one example of unauthorized disclosures of classified information; these leaks are reaching "cascade proportions."\(^10\) Although the disclosures typically are not intended to harm

---

\(^7\) Id. The consequences of disclosure were not limited to the effectiveness of Project Jennifer. The drafting of a United Nations world charter to permit scientific research in the oceans was stymied, in part, because leaders of developing nations pointed to Project Jennifer as evidence that the developed countries seek complete freedom for scientific research primarily to facilitate activities of espionage. See New York Times, March 20, 1975, at 30, col. 4.

\(^8\) N.Y. Times, March 19, 1975, at 1, col. 8.

\(^9\) Id.


Two other well-known instances deserve mention. The first involved disclosures of Stealth, a developmental manned or unmanned aircraft that existing air defense systems cannot intercept because of its limited detectability by radar. Information concerning Stealth technology was a "compartmentalized secret," one of the highest classification levels with special handling requirements. From 1977 until the summer of 1980 the Stealth program received little attention. Suddenly, in August 1980, Aviation Week, the Washington Post, and ABC News carried stories discussing the development of a "Stealth" bomber by the U.S. Id. at 2-3. As one member of the secretly briefed congressional committee complained, "[t]he 3- or 4-minute coverage [by ABC News] of this operation showed charts, drawings, and descriptions of new planes that could penetrate enemy radar. The Nation's viewers were given clearer information than members of the House Armed Services Committee." Leaks of Classified National Defense Information—Stealth Aircraft: Hearings Before the House Investigations Subcomm. of the Comm. on Armed Services, 96th Cong., 2d Sess. 4 (1980) (statement of Rep. Montgomery). As a result, the Carter administration held a press conference and confirmed the existence of the Stealth program, while instituting new security measures to protect the technological information related to the "Stealth" program. Id. at 64-66. The consequence of the disclosures was succinctly summed up by General Ellis, Commander of the Strategic Air Command: "giving the Soviets [—] years advanced warning of a new technology system they must counter is to sound the death knell of that system." Id. at 100 (letter from General Ellis to the Chief of Staff and copy sent to the Secretary of Defense) (numbers deleted for security reasons).

The second well-known disclosure of classified information involved the unauthorized dis-
the United States or to assist a foreign power, they frequently have these results. For example, the disclosure of the details of Project Jennifer irrevocably nullified a governmental decision in the interests of national security. Surprisingly, a criminal prosecution for disclosing government secrets has been initiated only once; a criminal prosecution for publishing government secrets has never been initiated.

This note addresses the problems posed by the unauthorized disclosure of government secrets and analyzes the case for a comprehensive statutory solution that would criminalize the "leaking" and publishing of classified information. Part one discusses the extent to which the unauthorized disclosure and publication of classified information are currently subject to governmental control. Except in certain narrowly defined situations, most unauthorized disclosures and publication of classified information are not grounds for criminal prosecution. Moreover, prepublication control is neither an effective nor constitutionally valid alternative. Part two of the note recognizes the tension between the goals of national security and first amendment interests, but it concludes that Congress may proscribe the unauthorized disclosure and publication of classified information without unconstitutionally encroaching on first amendment rights. Finally, the note examines several problems that arise when drafting legislation to prohibit the unauthorized disclosure of classified information. The note concludes that a comprehensive legislative solution making the unauthorized disclosure and publication of classified information a crime is appropriate.

closure of intelligence agents' identities. Philip Agee, an ex-CIA agent, was primarily responsible for these disclosures. He collaborated with Louis Wolf, co-editor of the Covert Action Information Bulletin and the magazine Counterspy. In 1975, Counterspy identified Richard Welch as the CIA station chief in Athens, Greece; he was assassinated shortly after publication of his name. N.Y. Times, Dec. 24, 1975, at 1, col. 3 and at 10, col. 3. In 1980, the Covert Action Information Bulletin published the name of an agent in Jamaica; shortly thereafter, he was the victim of an unsuccessful attack on his home. New York Times, July 5, 1980, at 1, col. 5. The direct connection between publication and attack finally led Congress to pass the Intelligence Identities Protection Act of 1982. See infra notes 50-51 and accompanying text.


12 The term "leaking" is used throughout this note to refer to the unauthorized disclosure of government information by a government official. This note focuses on leaks that have as their ostensible purpose the furtherance of public debate, rather than disclosures that seek to harm the United States or to aid a foreign nation.
I. THE CASE FOR A COMPREHENSIVE STATUTE

Under current United States law, the federal government is largely unable to prevent or to punish the leaking and publishing of classified government information. The relevant criminal statutes are narrowly drafted and apply only in a few special situations. Moreover, the courts generally refuse to enjoin publishers from printing classified information. Because of the differing constitutional and statutory treatment of leakers and publishers of classified information, this section separately analyzes the law as applied to each.

A. The Leaker

No general criminal statute prohibits a government employee from disclosing classified information. Indeed, only the "espionage statutes" and a group of other, narrowly directed criminal provisions are relevant. An executive order presently classifies information "concerning the national defense and foreign relations" into three levels of classification:

1. "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.
2. "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.
3. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.


See infra notes 15-16, 50, 52, & 60.

The espionage statutes are codified at 18 U.S.C. §§ 793-794 (1982), but only § 793(d)-(e) is relevant to this note's discussion of persons who leak government secrets. Subsections 793(a) and (b) cover actions to obtain information by physical intrusion into military installations and also prohibit copying or otherwise obtaining tangible items with the intent to harm the United States or to advantage a foreign nation. Therefore, these provisions cover conduct preparatory to classic espionage. They do not, for the purposes of this note, relate to the traditional "leaker" who either already has authorized access to the information or cannot be said to have acted with a harmful intent. Section 793(c) makes criminal the receipt of tangible items obtained in violation of other espionage provisions. Section 793(f) covers the removal of tangible or intangible information through gross negligence and thus is not relevant to a discussion of purposeful leaks. Section 794(a) covers communications to a foreign agent made with intent to harm the United States or to advantage a foreign nation. Section 794(b) is applicable only in time of war and covers intentional transfers of information to foreigners about troop movements and military plans. Section 794(c) covers conspiracies to violate either § 794(a) or (b).

See infra notes 62-75 and accompanying text.

Fortunately, these statutes treat the problem of leaks in an incomplete and piecemeal fashion, leaving significant gaps in their coverage. The relevant provisions of the espionage statutes are drafted imprecisely and are more applicable to the problem of classic espionage than to leaks of classified information by government insiders. Moreover, application of the espionage statutes to a person who leaks classified information may present constitutional problems. Several other, more specific statutes, provide narrow coverage, but they fail to address many instances of disclosure that threaten the country’s security.18

1. The Espionage Statutes

Although certain provisions of the espionage statutes seem broadly to prohibit disclosure of government secrets, the statutes are ill-designed to deal with unauthorized disclosures that do not fit the mold of foreign espionage. Congress enacted the Espionage Act of 191719 shortly after the severance of diplomatic relations with Germany, as a direct response to a
wartime situation. Since that time, the statutes rarely have been applied to conduct that does not involve either outright spying or some connection with a foreign power.20 Other than a case of classic espionage, the last successful prosecutions under the statutes, known as the Red Menace cases, were in 1919.21 These cases, now in disfavor, did not involve leaks of classified information, but were instead convictions for obstructing military recruitment during World War I. The Supreme Court decided those cases in a climate of judicial hostility to the first amendment that has not endured.22 The only prosecution for a leak of classified information under the statutes was the aborted prosecution of Daniel Ellsberg and Anthony Russo23 for their role in the release of the Pentagon Papers.

Several reasons account for the statutes' ineffectiveness against persons who leak classified information. Often the executive branch is hesitant, for political reasons, to use a statute that was primarily designed to punish spying to prosecute persons who purposely release government secrets to promote public debate about controversial executive actions. Furthermore, the statutes' language is subject to several different interpretations,24 so their application to classified information leaks is uncertain.

The provisions of the espionage statutes most relevant to leaks of classified information are subsections 793(d) and (e) of title 18 of the United States Code, which address the dissemination of documents or information "relating to the national defense."25 The broad language of these pro-

---


21 Id. at 831. The Red Menace cases are Schenck v. United States, 249 U.S. 47 (1919), Frohwerk v. United States, 249 U.S. 204 (1919), and Debs v. United States, 249 U.S. 211 (1919). See also Abrams v. United States, 250 U.S. 616 (1919) (distribution of circulars intended to provoke resistance to the United States and calling for worker strikes in munitions factories during World War I held to violate the Espionage Act).


23 See supra note 11.

24 See Edgar & Schmidt, supra note 18, at 934 ("the legislation is in many respects incomprehensible").


(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or
visions criminalizes the willful disclosure by persons with either lawful or unauthorized possession of a document or information "relating to the national defense" to "any person not entitled to receive it." Absent some limiting constructions, this language apparently applies to all unauthorized disclosures of classified information.

Subsections 793(d) and (e) are flawed, however, because they reach both too much and too little. These provisions are underinclusive because they only apply to information that affects national defense. The provisions may be overinclusive and unconstitutionally overbroad because they appear to criminalize any revelation of documents "relating to the national defense" even if the defendant harbors no harmful purpose. Finally, the statute may be unconstitutionally vague because the language "entitled to receive it" is not defined in the statute itself or in any executive order.

Professors Edgar and Schmidt argue that Congress intended that other

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; . . .

(f) [s]hall be fined not more than $10,000 or imprisoned not more than ten years or both.

Id.

Subsections 793(d) and (e) also prohibit the retention of a document or other information relating to the national defense; these provisions may apply to persons who leak or publish such information. See infra notes 81-82 and accompanying text.

Edgar & Schmidt, supra note 18, at 1031-32, lists five serious questions of construction that arise when interpreting these provisions.

For a discussion of the overbreadth doctrine, see infra notes 200-02 and accompanying text.

The term "willfully" in subsections 793(d) and (e) does not solve the overbreadth problem because a conventional reading of "willfully" would render any deliberate transfer of defense-related documents criminal without requiring an additional harmful purpose. Edgar and Schmidt, however, argue that Congress intended to require purpose or knowledge that the "primary use" to which the information would be put was to injure the United States or advantage a foreign nation. Edgar & Schmidt, supra note 18, at 1038-1046, 1057-58; cf. United States v. Truong Dinh Hung, 629 F.2d 908, 919 (4th Cir. 1980) (approving jury instruction that "willfully" required a finding of bad faith, prompted by some personal or underhanded motive, which cured any overbreadth problem of § 793(e)), cert. denied, 454 U.S. 1144 (1982).

Edgar & Schmidt, supra note 18, at 1050-57.
statutes or executive orders define who is "not entitled" to receive classified information. Yet, the government's system of classifying information cannot be used to determine who is "entitled to receive" information because the executive order upon which the system is based does not indicate who is or is not entitled to receive the information. The order merely prohibits disclosure to "unauthorized" persons; therefore, the disclosure is criminal only if made to someone whom another statute or executive order has affirmatively declared not entitled to receive it; arguably, no one is liable under these provisions. Thus, the entitlement language of subsections 793(d) and (e) seems so vague as to be ineffective and, perhaps, unconstitutional.

Subsections 793(d) and (e) also present an underinclusiveness problem because they do not protect all types of secrets that affect national security. The statute concerns only information or documents that "relat[e] to the national defense," a phrase construed in the leading case of Gorin v. United States. Gorin involved prosecutions under other sections of the espionage statutes that, unlike subsections 793(d) and (e), contain scienter requirements. The United States Supreme Court rejected the contention that the phrase was unconstitutionally vague and defined "national defense" as a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness." The Court found that such a broad reading of "national defense" was not unconstitutionally vague because the statute

31 Id. at 1056.
32 See supra note 13.
33 See, e.g., Reagan Order, supra note 13, which provides in part: "Officers and employees of the United States Government . . . shall be subject to appropriate sanctions if they knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order." Id. § 5.4(b)(1).
34 For a discussion of the vagueness doctrine, see infra notes 201-08 and accompanying text.
36 312 U.S. 19 (1941).
37 Compare the intent requirements in 18 U.S.C. § 793(d)-(e) (1982) with those in § 793(a)-(b) and § 794(a). Section 793 provides, in part:
(a) Whoever, for the purpose of obtaining information respecting the national 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 . . . ; or
(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe
18 U.S.C. § 793 (1982). Section 794(a) provides in part:
(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation. . .
38 Gorin, 312 U.S. at 28.
also required that the act be done with "intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation." So limited, the Court said, the phrase suffered no problem of uncertainty.

Gorin's definition of "national defense" raises two problems with subsections 793(d) and (e). First, the Gorin definition of "national defense" does not include, for example, nonmilitary government secrets that nonetheless are vital to the country's foreign affairs. Subsequent case law has not corrected the deficiency. There are many situations, outside the military context, in which disclosure could harm the United States. For example, secrets regarding the gathering of intelligence, the protection of foreign confidences, and advances in technology may be unrelated to defense preparedness, but they are potentially important both politically and economically.

---

39 Id. at 27-28; see also United States v. Enger, 472 F. Supp. 490, 508 (D.N.J. 1978) ("[I]ntent or reason to believe that the information to be obtained is to be used to the injury of the United States or, to the advantage of any foreign nation, is an essential element under §§ 793 and 794.").

40 Evidence of classification is not dispositive of whether information relates to the national defense; Gorin made the issue of defense-relatedness a jury question. 312 U.S. at 31-32. Judge Learned Hand in United States v. Heine, 151 F.2d 813, 816-17 (2d Cir. 1945), cert. denied, 328 U.S. 833 (1946), however, added a gloss to Gorin by holding that information not kept secret by the government cannot be the subject of prosecution, even if the disclosure is made to foreigners. Heine thus complicates the "related to national defense" standard, and some courts have allowed evidence of classification to be admitted as probative of government intent to maintain secrecy. See, e.g., United States v. Soblen, 301 F.2d 236, 239 n.2 (2d Cir.), cert. denied, 370 U.S. 944 (1962). The concern with secrecy presents the danger that the jury will confuse the evidence concerning intent to maintain secrecy with the evidence of defense-relatedness. The practical effect of this confusion would be to collapse the standards of information "concerning national defense and foreign relations," embodied in the classification system, into the "relating to the national defense" standard set out in §§ 793-94. See, e.g., United States v. Truong Dinh Hung, 629 F.2d 908, 918 n.9 (4th Cir. 1980) (commenting on the lower court's jury instruction: "Certainly the classification of the documents was relevant to the question of whether they related to the 'national defense.' "), cert. denied, 454 U.S. 1144 (1982).

41 The case law, although endorsing a broad reading of the Gorin definition, is not very illuminating. See, e.g., United States v. Truong Dinh Hung, 629 F.2d 908, 918 (4th Cir. 1980) ("defendants' attempt to constrict the ambit of 'national defense' to strictly military matters cannot succeed"), cert. denied, 454 U.S. 1144 (1982); United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir.) (rejecting the contention that "'national defense is limited strictly to information concerning the 'military establishment' and military preparedness for defending the territory of the United States"), cert. denied, 444 U.S. 855 (1979).


43 The recent passage of statutes aimed at stopping the flow of technology to other coun-
The protection of secret advances in technology is especially important. The present statutory scheme is dated because it reflects a belief that war is the only significant threat to the nation's well-being. Today, however, economic necessity and economic strength increasingly determine the balance of power among nations. Japan is the premier example of a nation that is powerful despite its nominal defense structure. Consequently, technological achievements can be as important to the national security as weapon systems.

These nondefense concerns, however, were not as relevant in 1917 when subsections 793(d) and (e) were enacted. The subsections' coverage is incomplete and does not apply to all categories of information that affect national security. Disclosers of information not "relating to the national defense" are beyond the reach of the criminal law, even though the disclosure may be very damaging to the nation's security. 44

Gorin raises a second, more difficult, problem in applying subsections 793(d) and (e) to leakers. A construction that saves the statute against a vagueness attack prevents the statute from reaching persons who leak information without the specific intent to harm the United States or to advantage a foreign nation. In Gorin, the Court relied on the statute's specific intent requirement to limit the inherent vagueness of the phrase "relating to the national defense." The culpability provisions in subsections 793(d) and (e), however, require only "willfulness" rather than specific intent. 45 A "willfulness" standard is most likely insufficient to elimi-
nate the vagueness concerns, so the provisions are probably unconstitutional unless interpreted with the Gorin scienter requirement. Yet, requiring the government to prove specific intent to harm the United States or to advantage a foreign nation makes subsections 793(d) and (e) inapplicable to most persons who leak classified information. A leak typically involves a government official who disseminates classified information through the press. The leaker usually intends to provoke public debate over a controversial government policy and perhaps to initiate a movement for reform. Because the release of the secret to the media is strong evidence of a benign motive, the prosecution is unlikely to succeed in proving specific intent to harm the United States or to advantage a foreign nation.

Thus, subsections 793(d) and (e) do not provide an adequate basis for prosecuting persons who leak classified information. The statute does not reach the disclosure of classified information that is not directly related to the national defense, such as technological or diplomatic secrets. Moreover, even if the disclosure falls within the statute's scope, two problems arise. If a "willfulness" culpability standard applies, the statute is likely to be unconstitutionally vague. If, however, a court reads a higher stan-

only to "willful" culpability. 18 U.S.C. § 793(d) (1982). "Information" is subject to the additional requirement that the leaker "has reason to believe [that the information] could be used to the injury of the United States or to the advantage of any foreign nation." Id. § 793(e). See Nimmer, National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case, 26 Stan. L. Rev. 311, 324 (1974). Professors Edgar and Schmidt argue that to implement the legislative intent, the culpability requirement — "reason to believe could be used" — should be interpreted as referring to the actor's belief as to the "principal use" to which the information will be put. Accordingly, a person who discloses to further public debate believes that the primary use will be to inform the public. Edgar & Schmidt, supra note 18, at 996-998. But see National Security Decision Directive 84 (Mar. 11, 1983) at 5-6, reprinted in The President's National Security Decision Directive 84 and Department of Defense Directive on the Use of Polygraphs, 1983: Hearings Before the Legislation and National Security Subcomm. of the House Comm. on Government Operations, 98th Cong. 1st Sess. (1984) (Statement of Robert L. Keuch, Deputy Assistant Attorney General, Criminal Division, Department of Justice) (the Justice Department's "consistent" position has been that § 793 covers knowing disclosures of information without any additional requirements of culpability). Whether the additional requirement of "reason to believe" is enough to satisfy the Gorin rationale is unclear. If the construction of "reason to believe" given by Professor's Edgar and Schmidt is adopted, a leak to the press negates any intent to harm the United States or to advantage a foreign nation. In the end, however, the question is likely to reduce to a determination of what a document or information is for the purposes of § 793(d)-(e), a determination that Congress has not yet provided. See Edgar & Schmidt, supra note 18, at 1047-50.

This reading of "willfully" would also remedy potential overbreadth problems. But cf. United States v. Dedeyan, 584 F.2d 36, 39 (4th Cir. 1978) (overbreadth problems in the § 793(f)(2) requirement of "knowledge" are eliminated where "the Government must prove that 'disclosure ... would be potentially damaging to the national defense ... '").
standard of culpability into the statute, subsections 793(d) and (e) will not apply to persons who leak information to the press.

2. Other Statutes

In addition to subsections 793(d) and (e), several other narrow provisions prohibit the disclosure of specific types of information. Some of the provisions even apply to nonclassified information. Unlike the espionage statutes, these provisions clearly proscribe leaks without raising the interpretive and constitutional issues discussed above. Because they are narrowly drawn, however, they constitute a patchwork scheme of protection for government secrets and do not adequately fill the gaps left by the espionage statutes.

Section 798 of title 18 of the United States Code criminalizes the knowing and willful disclosure of classified information relating to cryptography. Section 798 does not require a purpose to harm the United States or to advantage a foreign nation; proof of knowing disclosure to unauthorized persons is the culpability standard. Interestingly, Congress did not believe that the broadly worded provisions of the espionage statutes already covered the disclosures addressed in section 798.

Subsections 421(a) and (b) of title 50 prohibit those with access to

---

47 Arguably, other criminal statutes, not discussed in this note, would apply to persons who leak documents or information. See, e.g., 18 U.S.C. § 641 (1982) (prohibiting the unauthorized conveyance, disposal, or theft of any property of the United States); 18 U.S.C. § 2071 (1982) (prohibiting the unauthorized willful removal or carrying away of records or reports filed with any United States court or public office).

48 This section provides in part:

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.


49 See Edgar & Schmidt, supra note 18, at 1066-69.

50 This section provides in part:
classified information from intentionally disclosing the identity of a covert agent to anyone not authorized to receive classified information. In fact, Congress enacted the law in response to the actions of individuals who sought to disrupt the Central Intelligence Agency's activities by exposing covert agents abroad. This provision applies to leaks, but only those involving an extremely narrow category of information.

Other statutes prohibit the disclosure of specific types of information without regard to its classified status. Perhaps the most important of these are the "restricted data" statutes that protect information concerning atomic weapons or energy. Section 2274 of title 42 prohibits the disclosure of restricted data with the intent to advantage a foreign nation where there is "reason to believe" that the data will be used to harm the

(a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent 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, shall be fined not more than $50,000 or imprisoned not more than ten years, or both.

(b) Whoever, as a result of having authorized access to classified information, learns the identify of a covert agent and intentionally discloses any information identifying such covert agent 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, shall be fined not more than $25,000 or imprisoned not more than five years, or both.


* See generally Note, The Constitutionality of the Intelligence Identities Protection Act, 83 Colum. L. Rev. 727 (1983) (arguing that the Intelligence Identities Act, as applied to information lawfully obtained from the public domain by persons without access to classified information, involved the first amendment). Moreover, the enactment of § 421 was an explicit recognition of the failure of existing statutes to cover the proscribed activity. See H.R. 4, The Intelligence Identities Protection Act: Hearings Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence, 97th Cong., 1st Sess. 28 (1981) (statement of Richard Willard, Counsel to the Assistant Attorney General for Intelligence Policy).

Other than the statutes discussed in the text, the only other provision expressly prohibiting the unauthorized disclosure of classified information is 50 U.S.C. § 783(b) (1982), which prohibits disclosure of classified information to agents of foreign governments or members of communist organizations. This provision does not apply to a typical leak of information to the press.


* 42 U.S.C. §§ 2271-2281 (1982). "Restricted Data" is defined in 42 U.S.C. § 2014(y) (1982) as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy . . . ."
United States or to advantage a foreign nation. Thus, unlike subsections 793(d) and (e) of the espionage statutes, recklessness with respect to harm to the United States is the culpability standard. Additionally, section 2277 imposes criminal liability on present and former government employees or contractors who knowingly disclose restricted data to any person not authorized by the Nuclear Regulatory Commission to receive it. These provisions apply to leaks as well as to cases of foreign espionage, and they apply regardless of the executive classification status of the data. Nevertheless, the narrow scope of these provisions also reflects the ad hoc nature of legislation prohibiting the disclosure of government secrets.

Section 952 of title 18 prohibits the disclosure of any matter that has been transmitted in the diplomatic code of a foreign country. Arguably,

---

54 This section provides:

Whoever, lawfully or unlawfully, having possession of, access to, control over, or being entrusted with any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data—

(a) communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with intent to injure the United States or with intent to secure an advantage to any foreign nation, upon conviction thereof, shall be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both;

(b) communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation, shall, upon conviction, be punished by a fine of not more than $10,000 or imprisonment for not more than ten years, or both.


55 For an analysis of the "reason to believe" standard in § 793(d)-(e), see supra note 45.

66 This section provides:

Whoever, being or having been an employee or member of the Commission, a member of the Armed Forces, an employee of any agency of the United States, or being or having been a contractor of the Commission or of an agency of the United States, or being or having been an employee of a contractor of the Commission or of an agency of the United States, or being or having been a licensee of the Commission, or being or having been an employee of a licensee of the Commission, knowingly communicates, or whoever conspires to communicate or to receive, any Restricted Data, knowing or having reason to believe that such data is Restricted Data, to any person not authorized to receive Restricted Data pursuant to the provisions of this chapter or under rule or regulation of the Commission issued pursuant thereto, knowing or having reason to believe such person is not so authorized to receive Restricted Data shall, upon conviction thereof, be punishable by a fine of not more than $2,500.


67 Executive order is the only means by which information may be classified within the scope of the Atomic Energy Act. See Reagan Order, supra note 13, at 179.

68 This section provides:

Whoever, by virtue of his employment by the United States, obtains from another or
Government Secrecy

1985] 815

this provision is the only prohibition on disclosures of nondefense matters. Section 952 expressly applies to employees of the government and thus reaches the leaker. It only applies to a very narrow category of sensitive information, however, because the statute is not integrated into the executive classification system.

The disjointed array of statutes show that Congress does not have a comprehensive scheme to deal with the problem of leaks. The existing statutes either prohibit those disclosures with a specific intent to harm the United States or to advantage a foreign nation, or they apply only to a few narrowly defined categories of disclosures. The specific intent statutes do not apply to information leaks because of their high culpability standard. These statutes are more appropriate to the problem of classic espionage. As a result, persons who leak information to further public debate may do so with impunity, as long as the information they disclose is not protected by one of the more narrowly directed statutes. A second infirmity of the specific intent statutes is that they only protect information relating to the national defense. These statutes do not cover diplomatic secrets, nonmilitary technology, and other nonmilitary secrets that affect the country's security. The more narrowly directed statutes, although protecting some of this information, nonetheless constitute an incomplete solution to the problem of leaks. Congress has ignored large categories of information that should not be disclosed with impunity. In summary, Congress has not constructed a principled and consistent scheme of criminal sanctions to punish the disclosure of vital government secrets. Moreover, persons who leak government secrets are but one side of the problem; the government must also pursue remedies against those who publish the secrets. Like the disclosure provisions, however, the statutes relevant to the publication of government secrets are vaguely drafted and incomplete.

B. The Publisher

The government may deal with the publication of its secrets in two ways. It can invoke prepublication controls to stop a publisher from distributing information before he publishes it, or it can use postpublication

has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

criminal sanctions that punish a publisher for distributing sensitive information. Prepublication control is useful because it prevents widespread dissemination of the information in the first instance. As a practical matter, however, it is effective only when the government is forewarned of an impending publication. Additionally, constitutional constraints limit the government’s use of prepublication control. Accordingly, postpublication sanctions are necessary to supplement any prepublication control that the government employs.

1. Prepublication Control

Prepublication control may take the form of an injunction or a temporary restraining order. The only relevant statutory provision is section 2280 of title 42 of the United States Code. Section 2280 allows the United States Attorney General to obtain a permanent or temporary injunction to prevent a violation of any of the several criminal provisions prohibiting disclosures of information related to atomic energy or weapons. The government has invoked this provision only once to enjoin a publisher for national security reasons. In United States v. Progressive, Snepp v. United States, 444 U.S. 507 (1980) (per curiam) represents a merger of prepublication control and civil sanctions that were imposed after publication. In Snepp the Court upheld the CIA’s practice of requiring employees to sign prepublication review agreements as a condition of employment. Id. at 509 n.3. Snepp violated his agreement, and the Court imposed a constructive trust on Snepp’s publication profits. Id. at 515-16. Although Snepp is pertinent to the scope of the government’s power to invoke prepublication control, a Snepp-type situation does not present the same problems that are encountered by a leak. Indeed, in Snepp no classified information was revealed. United States v. Snepp, 595 F.2d 926, 931 (4th Cir. 1979), rev’d in part, 444 U.S. 507 (1980) (per curiam); cf. United States v. Marchetti, 466 F.2d 1309 (4th Cir.) (upholding secrecy agreement not to disclose classified information and enjoining publication of that information), cert. denied, 409 U.S. 1063 (1972). Marchetti and Snepp are cases in which the government knew of the intention to violate a written agreement. This note addresses prepublication restrictions on persons outside the government who intend to publish classified information.

60 See supra notes 53-54, 56 and accompanying text for a discussion of the prohibited conduct. Section 2280 provides:

Whenever in the judgment of the [Nuclear Regulatory] Commission any person has engaged or is about to engage in any acts or practices which constitute or will constitute a violation of any provision of this chapter, or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with such provision, and upon a showing by the Commission that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary injunction, restraining order, or other order may be granted.


the defendant sought to publish an article containing detailed theoretical and design information for atomic weapons. The district court held that a preliminary injunction against publication under section 2280 was not unconstitutional because the situation fit the "extremely narrow recognized area, involving national security, in which a prior restraint on publication is appropriate." In dictum, the court concluded that "a preliminary injunction would be warranted even in the absence of statutory authorization because of the likelihood of direct, immediate and irreparable injury to our nation and its people."

As a method of prepublication control, a section 2280 injunction is severely limited in two ways. First, according to the Progressive court, section 2280 requires a showing of harm commensurate to that required by analogous prior restraint doctrines, even though a section 2280 injunction is based on a statute. Second, section 2280's scope is limited to potential violations of certain criminal provisions prohibiting disclosure of information related to atomic energy or weapons. Outside this narrow category of restricted information, the government does not have statutory authority to pursue an injunction against publication.

The government encountered its limited power to prevent publication

NEED CITE.] The Pentagon Papers case is the only other instance where the government obtained a prepublication injunction. The Pentagon Papers injunction was not a § 2280 injunction, however, and it lasted for less than two weeks. New York Times Co. v. United States, 403 U.S. 713, 724 (1971) (Douglas, J., concurring).

A peculiar aspect of the Progressive litigation was that the article in question contained only information already in the public domain. Nevertheless, the government argued that the "restricted data" statutes classify such information as soon as it comes into existence. Progressive, 467 F. Supp. at 991. The restricted data statutes, as well as the Export Administration Act of 1979, 50 U.S.C. app. §§ 2401-2420 (1982) and the Arms Export Control of 1976, 22 U.S.C. §§2751-2794 (1982) raise interesting questions about the legitimate reach of government control over privately generated and owned information. For discussion of these questions, see generally Cheh, The Progressive Case and the Atomic Energy Act: Waking to the Dangers of Government Information Controls, 48 Geo. Wash. L. Rev. 163 (1980) (The Atomic Energy Act, restricting the dissemination of classified information, was meant to apply to government owned or government generated information and not to privately generated information); Comment, National Security Controls on the Dissemination of Privately Generated Scientific Information, 30 UCLA L. Rev. 405 (1982) (efforts to restrict the flow of privately generated scientific information should focus on design and manufacturing information).

The district court judge held that the phrase "communicates, transmits, or discloses" in § 2274 included "publishing in a magazine," and distinguished the Pentagon Papers case in part because the government's request for an injunction in Progressive was based on a statute. Id. at 994. As a result, an injunction under § 2280 was appropriate to prevent a violation of § 2274. Id. at 1000.

Id. (citing New York Times Co. v. United States, 403 U.S. 713, 730 (1971) (per curiam) (Stewart, J., concurring)).
in the Pentagon Papers case, where it sought to enjoin the New York Times from printing a classified government study of United States decision-making in the Vietnam War.\textsuperscript{66} The government argued that despite the lack of statutory support, the executive branch could enjoin publication to prevent "grave and irreparable danger" to the public interest.\textsuperscript{67} The Supreme Court, in a per curiam opinion, reiterated that prior restraints are especially disfavored.\textsuperscript{68} As a result, the government had a "heavy burden of showing justification for the imposition of such a restraint."\textsuperscript{69} The Court held that the government did not carry its "heavy burden" and allowed the New York Times to publish the classified study.\textsuperscript{70}

The Court did not find that the documents' classified status alone justified an injunction. As a result, some classified documents will be protected from disclosure through prior restraints, but others will not. In effect, the Court held that although the government classified the documents because their disclosure would harm the United States, the Court will independently determine whether the disclosure will result in enough harm to justify an injunction. Because it is unclear what standards the courts will use to make this independent judgment, the deterrent value of the classification system is reduced.

The Pentagon Papers case leaves open alternative conclusions about the use of prepublication injunctions. First, prior restraint may be available on a lesser showing of harm if Congress has enacted explicit statutory authority for the injunction. The Pentagon Papers decision emphasized the lack of legislative authority for the requested injunction.\textsuperscript{71} Alternatively, the Court may require a showing of significant national security concerns before issuing an injunction, regardless of its statutory basis. In either case, the availability of prepublication controls is uncertain; accordingly, the government should not rely too heavily on this method of safeguarding its secrets. A second problem with relying on pre-

\textsuperscript{66} For an overview of the Pentagon Papers case, see generally P. Schrag, Test of Loyalty (1974); M. Shapiro, The Pentagon Papers and the Courts (1972) (presenting a wide range of materials bearing on the political and legal issues involved in the Pentagon Papers—the book's basic premise is that the "ultimate issue involved is democratic control over foreign policy").

\textsuperscript{67} New York Times, 403 U.S. at 732 (White, J. concurring).

\textsuperscript{68} "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." Id. at 714 (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963)).

\textsuperscript{69} Id. at 714 (quoting Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971)).

\textsuperscript{70} Id. at 714; see Edgar & Schmidt, supra note 18, at 931.

\textsuperscript{71} New York Times, 403 U.S. at 718 (Black, J., concurring), 720-22 (Douglas, J., concurring), 730 (Stewart, J., concurring), 731 (White, J., concurring), 742-47 (Marshal, J., concurring).
publication control is that it is useful only if the government knows beforehand of the unauthorized, impending publication.\textsuperscript{72} Consequently, postpublication sanctions are also necessary to effectively discourage publication of sensitive information.

2. Postpublication Criminal Sanctions

Like the criminal statutes that apply to persons who leak government secrets, two types of statutes potentially apply to persons who publish\textsuperscript{73} such information: the espionage statutes\textsuperscript{74} and other provisions that apply only to specific types of secret information.\textsuperscript{75} The relevant provisions of the espionage statutes are subsections 793(c), (d), and (e).\textsuperscript{76} These provi-
sions punish: (1) the receipt of documents with knowledge that they have been obtained in violation of other espionage provisions, (2) communication of defense-related documents or information, and (3) retention of that information. These provisions, however, may not include those who publish government secrets. The opinions issued in the Pentagon Papers litigation disagree as to whether the espionage acts reach publishing.

One source of dispute was whether the term “communication” as used in subsections 793(d) and (e) includes publishing. The espionage statutes do not define “communication.” The statute’s uncritical approach to the communication/publishing dichotomy is further confused by its prohibition against retaining the information. Professors Edgar and Schmidt point out that if subsection 793(e) criminalizes a publisher's retention of sensitive information, as Justice White argues in the Pentagon Papers case, but does not apply to publication itself, then a reporter may freely publish the information yet be criminally liable for its retention. This is an absurd result.

Accordingly, whether “communicating” includes “publishing” may not be the dispositive question with respect to leaks to the press. The key to reading the language of the statute consistently with legislative intent

---

77 The text of § 793(d)-(e) is quoted supra note 25.

78 In the District Court proceeding against the New York Times, the government argued that the espionage acts applied to the publication of the Pentagon Papers. Judge Gurfein interpreted § 793(e) as not encompassing “publishing.” United States v. New York Times Co., 328 F. Supp. 324, 328-30 (S.D.N.Y.), rev’d, 444 F.2d 544 (2d Cir.), rev’d, 403 U.S. 713 (1971) (per curiam). Although the government did not argue the point before the Supreme Court, several members of the Court commented on these provisions. Justice Douglas found the inclusion of the word “publishes” in other provisions dispositive and concluded that § 793(e) did not reach the press. New York Times, 403 U.S. at 721. Justice Stewart remarked that the espionage provisions were “of very colorable relevance to the apparent circumstances of these cases.” Id. at 730. Justice White, joined by Justice Stewart, wrote the most complete analysis of the issue. He argued that the government should not have relied on an injunction, but rather should have invoked the espionage provisions prohibiting retention of the information. He declined, however, to say whether a “publication” would trigger § 793(e). Id. at 739 n.9. Justice Marshall found Justice White’s discussion of § 793(e) “plausible.” Id. at 745. Chief Justice Burger, dissenting, added that he was “in general agreement” with Justice White. 403 U.S. at 752.

79 Id. at 737-39 & 739 n.9 (White, J., concurring).

80 Edgar & Schmidt, supra note 18, at 1036-37. In addition to the retention provisions in § 793(e), § 793(c) makes criminal the knowing receipt of tangible items obtained in violation of other provisions. If this provision applies to publishers then it too, is subject to the anomalous application discussed in the text.
Government Secrecy

seems to be the culpability requirements. If the requirement of a harmful intent embraces an understanding of the purpose for which the transfer or publication is "primarily to be used," then the anomalous interpretations of subsections 793(d) and (e) disappear.

Nevertheless, the confusion inherent in construing the espionage provisions, reflected by the diversity of opinion in the Pentagon Papers case, has several consequences. Foremost is the uncertainty as to the scope of the application of these statutes. Congress did not intend for the provisions to punish disclosures that further public debate, yet they plausibly could be so construed. Thus far, the courts have not had an opportunity to resolve questions concerning the provisions' expansive breadth because the government has been reluctant to prosecute difficult cases under these provisions for fear of adverse judicial pronouncements. As a result, although subsections 793(d) and (e) likely do not pertain to activities, including publishing, that relate to the furtherance of public debate, the question is far from settled.

Other criminal provisions explicitly apply to the publication of government secrets. Like the statutes that apply to persons who leak government secrets, however, these provisions have a narrow scope. Section 421 of title 50 prohibits the disclosure of any information identifying an individual as a covert agent to any person not authorized to receive such classified information. Unlike the espionage provisions, section 426(3) of this title explicitly defines "discloses" to include "publish." This statute illustrates Congress' willingness to regulate publications where the potential for serious harm exists.

Section 952 of title 18 expressly prohibits government employees from willfully publishing information contained in a foreign coded transmis-

---

81 See supra notes 29 and 45 and accompanying text for a discussion of the culpability requirements in § 793(d)-(e).
82 The "restricted data" provisions are very similar to the espionage statutes in this respect. See supra notes 53-54, 56 for the texts of 42 U.S.C. §§ 2274, 2277 (1982). Neither § 2274 nor § 2277 use the term "publication." Like § 793(d)-(e), they use the term "communications." Therefore, it is unclear to what extent the publishing of restricted data is subject to criminal sanctions, notwithstanding § 2280's authorization of injunctions against impending violations of either § 2274 or § 2277. In the Progressive case, however, the district court judge concluded that "[p]ublication or other disclosure or communication of the Restricted Data contained in [the magazine article] would likely constitute a violation of the Atomic Energy Act, 42 U.S.C. § 2274(b) [(1982)].' United States v. Progressive, Inc., 467 F. Supp. 990, 999 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir. 1979).
sion. Section 798 of title 18\textsuperscript{87} criminalizes the knowing and willful publication of classified cryptographical information concerning. Sections 795 and 797 of title 18\textsuperscript{88} together prohibit the publication of graphic representations of military installations and equipment. The enactment of sections 795 and 797 shows that Congress did not believe that subsections 793(d) and (e) of the espionage statutes adequately protected against disclosure of graphic representations of military installations and equipment because of the restrictive specific intent requirement of those subsections.\textsuperscript{89}

C. An Argument for Reform

As shown above, the relevant statutes do not provide a comprehensive treatment of the disclosure and publication of classified information. Instead, they represent ad hoc attempts to prevent the dissemination of specific categories of information. Moreover, the broadest and potentially most far-reaching provisions, the espionage statutes, do not address the problem of leaks of government secrets to promote public debate.\textsuperscript{90}

Furthermore, the unsettled state of the law adversely affects both the public and the government. The public can never be sure which activities are protected and which will result in criminal liability. Because of the uncertainty surrounding the scope of the espionage statutes, the government may hesitate to prosecute under them. Unfortunately, the infrequency of prosecutions limits the judiciary's opportunities to clarify the statutes' coverage. The lack of judicial construction perpetuates the uncertainty surrounding the current law.

The result has been an uneasy compromise during this century between the protection of government secrets and the citizens' rights of free expression. Although a flexible, if ineffective, deterrent against disclosure and publication is arguably superior to a hasty resolution of the conflict between free speech and government secrecy, the risk of a truly damaging disclosure outweighs the justifications for not eliminating the current gaps in the law.

Arguments that leaks are necessary to further public debate or to expose governmental misbehavior are unpersuasive. For example, disclosure of the details of Project Jennifer permanently prevented the salvage of a Soviet submarine. The disclosure did not further public debate, but in-

\textsuperscript{89} Edgar & Schmidt, supra note 18, at 1069.
\textsuperscript{90} Accord Espionage Laws and Leaks: Hearings Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence, 96th Cong., 1st Sess. 168 (1979) (written statement of Professor Thomas I. Emerson, Yale University).
Government Secrecy

stead, effectively foreclosed meaningful future debate. The issue was moot once the Soviets learned of the operation because they were able to force the CIA to abandon the project. This disclosure was, in essence, a policy decision of great importance made by one individual, who was neither elected to represent the people nor accountable to them. Furthermore, the decision was contrary to the considered judgment of the executive branch, the intelligence community, and several congressional committees. Elected officials of the government should make policy decisions of such importance, rather than individual citizens. Although persons who leak classified information to further public debate may not intend to harm the United States, such disclosures pose a significant danger to the country’s security. Congress should enact a comprehensive system of criminal sanctions to punish these leaks.  

II. NATIONAL SECURITY AND THE FIRST AMENDMENT

Current law inadequately protects the national security. A congressional solution, however, involves the regulation of speech and free expression, and therefore implicates first amendment concerns. This section analyzes the competing goals of national security and the first amendment and concludes that Congress may constitutionally proscribe the disclosure of classified information.

A. National Security—The Goals of Secrecy

Legislation that limits a government employee’s dissemination of information about the government imposes a barrier between an open government and the people, between the employee and the rest of society, and between the government and the press. In the context of national defense and diplomacy, however, compelling public policies may require such restrictions. Secrecy is vital to the national security. Secrecy might clash with American concepts of an open government, an educated and enlight-

---

91 As an institution, Congress is more capable of designing a comprehensive resolution to clashes between national security and first amendment rights than are the executive branch or the judiciary. The judiciary can only treat the problem in an ad hoc fashion. The executive branch cannot impose criminal sanctions; its powers are limited to administrative sanctions that do not reach persons outside the government. See United States v. Hudson & Goodwin, 11 U.S. (7 Cranch) 32, 34 (1812) (“The legislative authority of the Union must first make an act a crime . . .”).

92 “Congress shall make no law . . . abridging the freedom of speech, or of the press.” U.S. Const. amend. I.

93 “[T]he maintenance of an effective national defense require[s] both confidentiality and secrecy. . . . In the area of basic national defense the frequent need for absolute secrecy is, of course, self-evident.” New York Times Co. v. United States, 403 U.S. 713, 728 (1971) (per curiam) (Stewart, J., concurring).
ened people, and an unfettered press, but it is a necessary evil. The government can preserve secrecy only by imposing a system of sanctions against leaks of classified information.

The most important service any government can provide is the protection and perpetuation of the national existence. Thus, nations compete for power to advance their interests. Detailed knowledge of American defense capabilities, diplomatic objectives, or negotiating postures can secure to a competing nation a valuable advantage. After all, information is power in the realm of international relations, a fact proved by the enormous resources nations pour into intelligence-gathering organizations. Accordingly, protecting national security information is compelling justification for governmental secrecy.

Historically, the need to keep defense matters secret has received the greatest recognition during war. As Justice Holmes wrote, "[w]hen a nation is at war many things that might be said in time of peace are such a hindrance to its efforts that their utterance will not be endured so long as men fight . . . ." Citations. Congress enacted the Espionage Act in wartime, and other statutes apply only during war. During a war, plans of actual military operations, the disposition of forces, and the tactical and strategic ends of warring nations require secrecy lest an enemy learn of them. Disclosure of these details can result in the loss of lives and the failure of whatever objectives motivate the warring nation.

Today, however, the justifications for secrecy of military plans, tactics, and strategy have equal force during times of peace. Since World War II and the initiation of the "cold war," the two superpowers have clashed in indirect conflict through the use of proxy states. Thousands of lives were lost in the conflicts in Korea, Vietnam, Angola, and perhaps Central America. The need for secrecy during the current cold war is just as compelling as it would be during overt hostilities.

Other secrecy interests include defense contingency plans and the nature and characteristics of weapons systems and defense installations. This data merits protection during both peace and war. Disclosure of a nation's contingency plans, drawn up in the anticipation of hostilities, allows an enemy to prepare countermeasures in advance. Similarly, disclos-

---

95 See supra note 19 and accompanying text.
96 See supra note 20 and accompanying text.
97 Wartime secrecy among allies is essential to the appearance of a united front. Allies often have different wartime objectives and means of achieving them. An enemy with knowledge of these differences can exploit them and perhaps crack the coalition.
98 The Allies, in World War II, learned of most German plans and objectives through the code machine Ultra. In the long run Ultra likely saved a significant number of Allied lives. For the story behind Ultra, see F. Winterbotham, The Ultra Secret (1974).
ure of a weapon system’s performance limits or its wartime applications allows enemy states to respond to this information before hostilities ever begin. The disclosure of “stealth” technology in 1980 very likely encouraged the Soviets to develop methods that counter a stealth bomber’s ability to evade radar.99 Thus, the dissemination of secret research and development information could vitiate an otherwise effective military system.

A related secrecy interest concerns advances in nonmilitary technology. Economic advantage in world markets is becoming more central to a nation’s security. Advances in technology, especially during research and development, should be protected from disclosure. If the United States’ present economic power erodes, the protection of technological advances becomes as critical as the protection of weapon systems. Furthermore, some technologies, such as nuclear energy, have both military and nonmilitary applications. Thus, secret advances in technology should be closely guarded.

Another secrecy interest concerns intelligence operations, sources, and methods. An intelligence service attempts to secure information about foreign nations, including their military capabilities, political and cultural dynamics, and diplomatic options. Intelligence specialists also analyze foreign nations’ capabilities and intentions toward the United States and its allies. This analysis data has two objectives. The first is to maintain an effective national defense by observing the actions of hostile or potentially hostile nations. The second is to operate an effective foreign policy, by selecting the best diplomatic alternatives.

Secrecy of raw intelligence data, methods, and sources is of paramount importance to the furtherance of these goals. If a foreign nation knows the extent to which the United States has learned of its day-to-day government operations, its military dispositions and weapons capabilities, or its perceived vital or peripheral interests, it will take steps to block such a flow of information. Ongoing intelligence operations are particularly susceptible to failure if disclosed;100 where a covert operation is ongoing, it presents perhaps the most compelling case for secrecy.

Courts are sensitive to the need for secrecy surrounding intelligence activities. In United States v. Nixon,101 the Supreme Court stated that “[t]he President, both as Commander-in-Chief and as the nation’s organ for foreign affairs, has available intelligence services whose reports are

99 For a discussion of leaks involving “Stealth,” see supra note 10.
100 Project Jennifer, discussed supra notes 1-9 and accompanying text, shows the consequences of the disclosure of an ongoing intelligence operation.
not and ought not to be published to the world."\footnote{102} The Court has also stated that "[t]he Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service."\footnote{103}

In denying Freedom of Information Act (FOIA)\footnote{104} requests addressed to intelligence agencies, courts have been even more sensitive to the need for intelligence secrecy. For example, the United States Court of Appeals for the D.C. Circuit has referred to the "mosaic-like nature of intelligence gathering," and found that seemingly innocent information deserved protection in the context of intelligence operations.\footnote{105} In short, when protecting details of intelligence sources, methods, and operations from public disclosure, "courts . . . accord the utmost deference to executive assertion of state secrets."\footnote{106}

Secrecy is also important to the conduct of foreign affairs. As Justice Stewart asserted in his concurring opinion in the Pentagon Papers case, "it is elementary that the successful conduct of international diplomacy . . . require[s] both confidentiality and secrecy. Other nations can hardly deal with this Nation in an atmosphere of mutual trust unless they can be

\begin{footnotes}
\footnote{Id. at 719 (quoting Chicago & Southern Airlines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948)).}
\footnote{Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (per curiam).}
\footnote{Salisbury v. United States, 690 F.2d 966, 971 (D.C. Cir. 1982); accord CIA v. Sims, 53 U.S.L.W. 4453, 4458-59 (1985); Halperin v. CIA, 629 F.2d 144, 150 (D.C.Cir. 1980) ("each individual piece of intelligence information, much like a jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"); Hayden v. National Sec. Agency, 608 F.2d 1381, 1389 (finding that the trial court did not abuse its discretion in refusing to disclose any part of classified affidavit even though portions of the affidavit were already in the public domain), cert. denied, 446 U.S. 937 (1980); United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) ("[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad of the scene and may put the questioned item of information in its proper context"), cert. denied, 409 U.S. 1063 (1972).}
\footnote{In Sims, the Court had the following comments: Foreign intelligence services have both the capacity to gather and analyze any information that is in the public domain and the substantial expertise in deducing the identities of intelligence sources from seemingly unimportant details [T]he Director . . . has power to withhold superficially innocuous information on the ground that it might enable an observer to discover the identity of an intelligence source. . . . It is conceivable that the mere explanation of why information must be withheld can convey valuable information to a foreign intelligence agency. Sims, 105 S.Ct. at 1892-93 (citations omitted).}
\end{footnotes}
assured that their confidences will be kept."\textsuperscript{107} The premise that information on foreign affairs requires secrecy is based on somewhat different interests than those underlying a national defense. In the national defense context, the immediate protection of vital national security interests demands secrecy; in foreign affairs, the requirement of confidentiality flows from the need to freely communicate with other nations, both allied and enemy. Although the ultimate rationale for secrecy in diplomacy is still security, it is removed from the immediacy surrounding direct national security interests.

Nonetheless, when nations deal with each other, they often do so in secret. Allies frequently exchange national security information. Delicate negotiations are generally conducted in secret.\textsuperscript{108} When one state communicates a bargaining position to another, it may hope that the position will be accepted. If the proposal is not accepted, however, no state wishes to back down publicly. Similarly, a country, when dealing with the United States, may wish to have certain information kept confidential for fear that revelation would be an embarrassment domestically. Additionally, nations may wish to keep negotiations secret to present a \textit{fait accompli} to the world.\textsuperscript{109}

Although these are only a few of the possible reasons supporting secrecy in international relations, they reflect accepted practices. Secrecy in both national security and foreign affairs has been a historical as well as a

\begin{itemize}
\item \textsuperscript{107} New York Times Co. v. United States, 403 U.S. 713, 728 (1971) (Stewart, J., concurring).
\item \textsuperscript{108} In United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936), the Court quoted the words of President Washington when he was asked to divulge information concerning the Jay Treaty negotiations:

\begin{quote}
The nature of foreign negotiations requires caution, and their success must often depend on secrecy; and even when brought to a conclusion a full disclosure of all the measures, demands, or eventual concessions which may have been proposed or contemplated would be extremely impolitic; for this might have a pernicious influence on future negotiations, or produce immediate inconveniences, perhaps danger and mischief, in relation to other powers. The necessity of such caution and secrecy was one cogent reason for vesting the power of making treaties in the President, with the advice and consent of the Senate, the principle on which that body was formed confining it to a small number of members. To admit, then, a right in the House of Representatives to demand and to have as a matter of course all the papers respecting a negotiation with a foreign power would be to establish a dangerous precedent.
\end{quote}

Id. at 320-21. (quoting 1 Messages and Papers of the Presidents 1789-1897 194-95 (1913)).
\item \textsuperscript{109} Throughout the 1930s, the U.S.S.R., through Foreign Minister Maxim Litvinov, reacted strongly against the resurgence of Germany under Hitler. M. Litvinov, Against Aggression 18-21 (1939). Yet, in the summer preceding the Nazi invasion of Poland, Germany and the Soviet Union signed a Non-Aggression Pact after secret negotiations. In effect, this diplomatic feat protected the German Eastern front when it invaded Poland and enabled it to concentrate on potential Western intervention.
\end{itemize}
continuing fact. Generally, courts have refused to interfere with decisions on secrecy in the conduct of foreign affairs.110

Secrecy is necessary, in sum, to conduct an effective foreign policy and to provide for an effective national defense. Commentators generally agree that these goals require some degree of secrecy.111 They disagree, however, on the extent to which these goals demand the protection of all confidential information. Courts, however, frequently adopt a deferential standard when faced with a government request that secrecy interests be protected.112

Two reasons underlie the courts' deference. First, because the executive branch is primarily responsible for the country's defense113 and foreign affairs,114 judicial review of executive branch decisions on the need for

110 See, e.g., Chicago & Southern Airlines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) ("It would be intolerable that courts without the relevant information should review and perhaps nullify actions of the Executive taken on information properly held secret... But even if courts could require full disclosure, the very nature of executive decisions as to foreign policy is political, not judicial."); United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936) (discussing congressional limits over Executive action in the area of foreign policy: "It is quite apparent that in the maintenance of our international relations... congressional legislation, which is to be made effective through negotiation and inquiry within the international field, must often accord to the President a degree of discretion... "). Nonetheless, the executive must always act within constitutional constraints, even when formulating and implementing foreign policy. Id.

111 See, e.g., Katzenbach, Foreign Policy, Public Opinion and Secrecy, 52 Foreign Affairs 1, 17 (1973).

112 Judicial deference is most apparent when those outside the government seek access to government secrets, as in FOIA litigation, see supra note 105 and accompanying text. The judiciary, however, is less deferential when the government seeks to prevent the dissemination of secrets already in the possession of those outside the government. See, e.g., New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam) (requiring the government to carry a heavy burden of proof that protection of secrecy is required).

113 "The President shall be Commander in Chief of the Army and Navy of the United States." U.S. Const., art. II, § 2, cl. 1.

114 See United States v. Curtiss-Wright Export Co., 229 U.S. 304, 319 (1936), where the Court stated:

Not only, as we have shown, is the federal power over external affairs in origin and essential character different from that over internal affairs, but participation in the exercise of the power is significantly limited. In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation. He makes treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiation the Senate cannot intrude; and Congress itself is powerless to invoke it. As Marshall said in his great argument of March 7, 1800, in the House of Representatives, "The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations."

Id. See generally L. Henkin, Foreign Affairs and the Constitution (1972) (discussing the relationship between the Constitution and the conduct of foreign affairs).
Government Secrecy

secrecy in these areas may be inappropriate due to separation of powers concerns. Arguably, the judiciary is institutionally incompetent to interfere with an executive decision that certain matters require secrecy, unless another constitutional interest is at stake. Additionally, courts may be hesitant to interfere with an executive determination that national security would be harmed by disclosure because of the courts' lack of experience in this area and the serious repercussions of a mistake. Thus, the courts recognize that secrecy in certain situations is essential to national security. Maintaining secrecy, however, imposes certain costs on society. A balance must be struck between these costs and national security.

B. The First Amendment as a Constraint on Secrecy

Despite its compelling justifications, secrecy also conflicts fundamentally with many of the principles underlying a democratic government. In particular, it conflicts with the free flow and exchange of information about the operation of government, thus implicating first amendment issues. Any congressional solution to the problem of leaks must operate within the constraints of the first amendment. Because the first amendment offers different protections to the public, to government employees, and to the press, the following analysis separately discusses the rights of these three groups.

1. The Public's Right to Know

The term "right to know" refers to a variety of concepts: the public's general right to be informed about governmental activities and performance; the right to compel the government to produce specific information within its control; and the right of access to particular government proceedings. Regulating disclosures of classified information implicates


It is not, however, inappropriate for courts to review any secrecy or national security decision that the executive makes. Particularly where constitutional issues arise, it is uniquely the courts' province to apply the law, regardless of the executive's claims. United States v. Nixon, 418 U.S. 683, 703 (1974); Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803). Executive claims of national security have not prevented judicial review in the past. See, e.g., Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), cert. denied, 425 U.S. 944 (1976); United States v. United States Dist. Court, 407 U.S. 297 (1972).

119 For a discussion of different meanings of the right to know, see Emerson, Legal Foundations of the Right to Know, 1976 Wash. U.L.Q. 1, 5-20.
two aspects of the right to know: the public’s right to be informed and the right to compel the government to produce specific information. At present, the legal status of the right to know is unsettled, yet the right might constrain the government’s ability to withhold secrets.

117 Emerson, supra note 116, at 3-4.

118 Academic debate has arisen concerning the extent of a constitutional right to know. Some commentators argue that the first amendment right to know guarantees a right of access to governmental information and an affirmative governmental duty to disclose. See, e.g., Emerson, supra note 116, at 14. Emerson argues:

[T]he constitutional right to know embraces the right of the public to obtain information from the government . . . . The public, as sovereign, must have all information available in order to instruct its servants, the government. As a general proposition, if democracy is to work, there can be no holding back of information; otherwise ultimate decisionmaking by the people, to whom that function is committed, becomes impossible. Whether or not such a guarantee of the right to know is the sole purpose of the first amendment, it is surely a main element of that provision and should be recognized as such.

Id.; see also Note, The First Amendment Right to Gather State-Held Information, 89 Yale L.J. 923 (1980) (arguing that the right to gather information held by the government is specifically found in the first amendment and that government regulation of the right must be narrow and nondiscriminatory).

Other commentators assert that the Constitution does not impose a duty on the government to disclose information. See, e.g., BeVier, An Informed Public, an Informing Press: The Search for a Constitutional Principle, 68 Calif. L. Rev. 482, 482-83 (1980) (arguing that the Constitution’s prescription of a representative democracy, the lack of a “normative” principle by which to evaluate citizens’ claims for information, and the entrusting of whether to grant such claims to nonjudicial branches of government support the conclusion that a right to know is not a principle of constitutional significance.); Easterbrook, The Production of Information, 1981 Sup. Ct. Rev. 309, 350-51. Easterbrook argues:

The public’s “right to know” first appeared in the Court’s cases more than 170 years after the First Amendment was adopted, which may be taken as a sign that it is based on invention rather than interpretation . . . .

If there is a “right to know,” perhaps the repeal of the Freedom of Information Act would be unconstitutional . . . . Nonsense. The “right to know” is a mere by-product of the First Amendment right to speak. If one person has a right to speak, others learn. It is quite inappropriate to take a by-product and convert it into a right of independent standing.

Id.; see also Henkin, The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers, 120 U. Pa. L. Rev. 271 (1971) (arguing that a “right of the people to know” is not expressed in the Constitution and that the Constitution’s drafters would not have considered the government’s secrecy in certain areas a violation of the press).

The courts have not held that the right to know is a Constitutional right that places the government under a duty to disclose. Nonetheless, they have considered the first amendment to contain narrow aspects of the right to know.

The right to know is based on a theory of effective self-governance: “a major purpose of [the first amendment] was to protect the free discussion of governmental affairs.” Mills v. Alabama, 384 U.S. 214, 218 (1966). As one commentator expressed, “there is one principle which both commands widespread agreement and is derived from constitutional structure:
Arguably, under the first amendment the public has a right to compel the government to produce information. Effective operation of any form of self-government requires unrestricted communication between the people and the government and a public awareness of the government's activities. Based on such reasoning, the Supreme Court has recognized a right to know, under the first amendment, in cases concerning the public's and media's access to judicial proceedings in criminal prosecutions.\(^1\) The Court supported those decisions with sweeping language that underscores the essential link between information and effective self-governance. In particular, the Court discussed the importance of "furthering the First Amendment's mission of securing meaningful public control over the process of governance"\(^2\) and preventing "abridgement of [the public's] rights of access to information about the operation of their government."\(^3\)

The Court, however, has not achieved a consensus on the exact limits of the public's right to know.\(^4\) Its decisions in this area address only access to judicial proceedings in criminal prosecutions. The Court has

the core first amendment value is that of the democracy embodied in our constitutionally established processes of representative self-government." BeVier, supra note 118, at 502. Professor Alexander Meiklejohn relates first amendment freedoms to self-government. See, e.g., A. Meiklejohn, Political Freedom, Free Speech and Its Relation to Self Government (1960).

\(^1\) See Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980).


\(^3\) Id. at 828 (Stevens, J. concurring) (quoting Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 584 (1980) (Stevens, J., concurring)).

\(^4\) Compare Houchins v. KQED, 438 U.S. 1, 15-16 (1978) (plurality opinion) ("Neither the First Amendment nor the Fourteenth Amendment mandates a right of access to government information or sources of information within the government's control.") with Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 576 (1980) (plurality opinion) ("[T]he First Amendment guarantees of speech and press, standing alone, prohibit government from summarily closing courtroom doors which had long been open to the public at the time that Amendment was adopted.") and id. at 583 (Stevens, J., concurring) ("Today . . . for the first time, the Court unequivocally holds that an arbitrary interference with access to important information is an abridgment of the freedoms of speech and of the press protected by the First Amendment."). But see the analysis contained in First Amendment Coalition v. Judicial Inquiry & Review Bd., 579 F. Supp. 192 (E.D. Pa. 1984), where the district judge read the case law as establishing the following test:

[The sharp doctrinal division in Saxbe and Pell has given way to a substantial doctrinal consensus reflected in Richmond Newspapers: A governmental restriction on public and press access to information about matters of public concern presents a First Amendment question; a restriction on public and press access can be sustained, but only to the extent that it demonstrably advances significant governmental interests.

Id. at 211
never decided whether the Constitution requires the government to disclose a particular piece of classified information.\footnote{123 As Justice Stewart once lectured: There is no constitutional right to have access to particular government information, or to require openness from the bureaucracy (Citing Pell v. Procunier, 417 U.S. 817 (1974)). The public's interest in knowing about its government is protected by the guarantee of a Free Press, but the protection is indirect. The Constitution itself is neither a Freedom of Information Act nor an Official Secrets Act. The Constitution, in other words, establishes the contest, not its resolution. Congress may provide a resolution, at least in some instances, through carefully drawn legislation. For the rest, we must rely, as so often in our system we must, on the tug and pull of the political forces in American society. Stewart, Or of the Press, 26 Hastings L.J. 631, 636 (1975). Justice Stewart's words, spoken before Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980), still apply as to any constitutional duty on the government to disclose information. \footnote{124 Thus, in Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980), the Court drew support from the tradition, at the time of the Constitutional Convention, of open criminal proceedings. Id. at 569. Secret information classified pursuant to valid executive interests, and within constitutional constraints, presents a far different case.} The lack of any norm or criterion by which to apply such a right.\footnote{125 See BeVier, supra note 118, at 506-08 ("But how much is enough? And by what criteria is the scope of government's duty to disclose to be measured?"); Cheh, Judicial Supervision of Executive Secrecy: Rethinking Freedom of Expression for Government Employees and the Public Right of Access to Government Information, 69 Cornell L. Rev. 690, 724 (1984) ("The issue comes to this: By what standard can the courts decide how much information is sufficient to make democracy work?"); see also Houchins v. KQED, Inc., 438 U.S. 1, 12 (1977) (suggesting that it is the legislatures' duty to draw the necessary lines); Henkin, supra note 118, at 278 (Can courts meaningfully weigh the Government's 'need' to conceal, the Press's 'need' to publish, the People's 'need' to know?").} Nevertheless, it would be a mistake to read the first amendment as establishing a right to compel the government to reveal classified information. Historically, the first amendment embraced the right to know for criminal trials,\footnote{126 In Branzburg v. Hayes, 408 U.S. 665 (1972), the Court considered the extent of the press' right to gather news and said: "There are few restrictions on action which could not be clothed by ingenious argument in the garb of decreased data flow. For example, the prohibition of unauthorized entry into the White House diminishes the citizen's opportunities to gather information he might find relevant to his opinion of the way the country is being run, but that does not make entry into the White House a First Amendment right." Id. at 684 n.22 (quoting Zemel v. Rusk, 381 U.S. 1, 16-17 (1965)). Indeed, Professor Cheh considers this to be the principal reason for the Supreme Court's rejection of the argument that the public can obtain information within the government's control. Cheh, supra, at 724.} but not for disclosure of classified information. Moreover, the government has a valid, countervailing interest in preventing general access to classified secrets.

A host of practical difficulties would accompany a constitutional interpretation requiring the government to disclose information, particularly classified information. The courts could not in principle contain such a right.\footnote{127 As Justice Stewart once lectured: There is no constitutional right to have access to particular government information, or to require openness from the bureaucracy (Citing Pell v. Procunier, 417 U.S. 817 (1974)). The public's interest in knowing about its government is protected by the guarantee of a Free Press, but the protection is indirect. The Constitution itself is neither a Freedom of Information Act nor an Official Secrets Act. The Constitution, in other words, establishes the contest, not its resolution. Congress may provide a resolution, at least in some instances, through carefully drawn legislation. For the rest, we must rely, as so often in our system we must, on the tug and pull of the political forces in American society. Stewart, Or of the Press, 26 Hastings L.J. 631, 636 (1975). Justice Stewart's words, spoken before Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980), still apply as to any constitutional duty on the government to disclose information. \footnote{128 Thus, in Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980), the Court drew support from the tradition, at the time of the Constitutional Convention, of open criminal proceedings. Id. at 569. Secret information classified pursuant to valid executive interests, and within constitutional constraints, presents a far different case.} The lack of any norm or criterion by which to apply such a right.\footnote{129 See BeVier, supra note 118, at 506-08 ("But how much is enough? And by what criteria is the scope of government's duty to disclose to be measured?"); Cheh, Judicial Supervision of Executive Secrecy: Rethinking Freedom of Expression for Government Employees and the Public Right of Access to Government Information, 69 Cornell L. Rev. 690, 724 (1984) ("The issue comes to this: By what standard can the courts decide how much information is sufficient to make democracy work?"); see also Houchins v. KQED, Inc., 438 U.S. 1, 12 (1977) (suggesting that it is the legislatures' duty to draw the necessary lines); Henkin, supra note 118, at 278 (Can courts meaningfully weigh the Government's 'need' to conceal, the Press's 'need' to publish, the People's 'need' to know?").} The lack of any norm or criterion by which to apply such a right
suggests that Congress, rather than the courts, should resolve this issue. In fact, Congress has already enacted a comprehensive statute, the Freedom of Information Act (FOIA), defining the public's right to compel governmental disclosure.

Congress enacted the FOIA to promote public access to government information and to prevent excessive secrecy. The statute allows any citizen to obtain federal agency records that are not exempt under the statute, and it contains nine narrowly-drawn exemptions, two of which are relevant here. First, the FOIA does not require the disclosure of matters that are "specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and . . . are in fact properly classified pursuant to such Executive Order." Second, the FOIA exempts matters that are "specifically exempted from disclosure by statute."

126 Houchins v. KQED, Inc., 438 U.S. 12 (1977) (A right to access "invites the Court to involve itself in what is clearly a legislative task which the Constitution has left to the political processes."); BeVier, supra note 118, at 508-12 (arguing that the courts are not equipped to decide what information the government must reveal to its citizens); Henkin, supra note 118, at 278-79.


128 When an agency denies an FOIA request, and the applicant sues for release of the information in federal court, the agency must supply affidavits supporting the agency's decision. The court must then "determine the matter de novo," placing "the burden . . . on the agency to sustain its action." Id.; Military Audit Project v. Casey, 656 F.2d 724, 738 (D.C. Cir. 1981). In conducting this review, the district court should "accord substantial weight to an agency's affidavit concerning the details of the classified status of the disputed record." Id. (quoting S. Rep. No. 1200, 93d Cong., 2d Sess. 12 , reprinted in 1974 U.S. Code Cong. & Ad. News 6267, 6290). A court can then grant summary judgment on the basis of agency affidavits, provided that the affidavits show "the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith." Military Audit Project, 656 F.2d at 738. Where the agency decisions asserts to the national security, courts grant the same deference as provided to classification decisions. Goland v. CIA, 607 F.2d 339, 350 n.64 (D.C. Cir. 1978), cert. denied, 445 U.S. 927 (1980). In effect, the courts review the procedure by which the classification occurred, but not whether the sought-after material meets the classification category in which the agency placed it. Recently enacted legislation allows the CIA to prevent material it designates as "sensitive operational information" from search, review, or release under FOIA. Central Intelligence Agency Information Act, Pub. L. No. 98-477, 98 Stat. 2209 (1984). This act does, however, allow for judicial review of the CIA's designation of a file as sensitive. For an overview of the FOIA process, see M. Halperin, Litigation Under the Amended Freedom of Information Act (4th ed. 1978); Note, National Security and the Amended Freedom of Information Act, 85 Yale L.J. 401 (1976); Comment, National Security and the Public's Right to Know: A New Role for the Courts Under the Freedom of Information Act, 123 U. Pa. L. Rev. 1438 (1975).


130 Id. § 552(b)(3). As noted, supra, note 43, 10 U.S.C. § 140c (Supp. I 1983), authorizing
The FOIA, therefore, represents a legislative definition of the public's right to know. Congress' specific exemption of classified information from disclosure represents a legislative balancing of the competing political interests. Indeed, it is significant that only "properly" classified information is exempt. This evinces Congress' attitude that only a valid governmental interest in secrecy should block the free flow of information to the public. The principle of an open government requires that only potentially harmful classified information be withheld.

Arguably, Congress should enforce the balance it struck in the FOIA by imposing criminal penalties for all unauthorized disclosures of "properly" classified information. The level of harm that justifies classified status or exemption from compulsory disclosure, however, does not necessarily warrant criminal penalties. Any affirmative regulation of disclosures, particularly criminal penalties, should restrict only that information that presents a compelling reason for secrecy.

2. Government Employees

Government employees are subject to several different, and often conflicting, demands on their loyalty. They are under a duty to be loyal to the United States;131 additionally, they must be loyal to their superiors and perform in a manner consistent with administration policy.132 Occasionally these duties may conflict. For example, in the course of performing his job, the employee may discover that government officials have engaged in wrongful acts. In this situation, the employee may believe that his duty to the country requires that he disclose this information. The extent to which employee disclosures are protected is unclear. Various

---


132 This requirement is imposed by administrative personnel actions. See supra note 17. In addition, National Security Decision Directive 84, supra note 45, at 18, provides that "[a]ll persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." Violations of such agreements will result in no "further access to classified information" and "administrative sanctions as appropriate." Id. at 19. Thus, notwithstanding the lack of criminal remedies, a clear course of civil and administrative remedies may be invoked when employees leak information covered by nondisclosure agreements. See Snepp v. United States, 444 U.S. 507 (1980) (per curiam) (upholding validity of secrecy agreement and imposing constructive trust on profits made in violation of agreement); United States v. Marchetti, 466 F.2d 1309 (4th Cir.) (approving injunction granted to prevent disclosure of classified information in violation of secrecy agreement), cert. denied, 409 U.S. 1063 (1972).
statutes prohibit retaliatory personnel actions against an employee who discloses official wrongdoing. These statutes do not cover disclosures of classified information.

Any attempt by government to restrict employee expression, including the leaking of classified information, implicates the first amendment. The following analysis examines the protections of the first amendment where the government attempts to restrict its employees’ expression.

Although historically government employment was a privilege rather than a right, the Supreme Court has more recently noted that government employees do not give up all rights of free expression. Moreover, an employee’s rights to free expression may vary with the context of the expression. Where criticism of policy or expression on matters of public concern are at issue, the Court has generally applied a balancing test to determine whether to permit employee discipline. If, however, the employee’s speech affects national security interests, the balancing test is

---

133 See supra note 17.

134 A “national security” exception to first amendment protection may exist. Near v. Minnesota, 283 U.S. 697 (1931), was a landmark decision because of its formulation of the principle against prior restraints. In dictum, the Near Court excluded some subjects from the scope of the first amendment without reference to whether the mechanism used was a prior restraint or subsequent punishment:

No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops. On similar grounds, the primary requirements of decency may be enforced against obscene publications. The security of the community life may be protected against incitements to acts of violence and the overthrow by force of orderly government.

Id. at 716. Thus, the first amendment may not protect disclosures harmful to national security. Chief Justice Burger and Justice Blackmun, each dissenting in the Pentagon Papers case, noted this point. New York Times Co. v. United States, 403 U.S. 713, 749 (1971) (Burger, C.J., dissenting); Id. at 761 (Blackmun, J., dissenting). If the speech is within the scope of the first amendment, however, a government’s ability to prevent speech in the employer-employee context must be determined.

136 See, e.g., Justice Holmes’ opinion in McAuliffe v. Mayor of New Bedford, 155 Mass. 216, 220, 29 N.E. 517, 517 (1892) (“The petitioner may have a constitutional right to talk politics, but he has no constitutional right to be a policeman.”) This view of the employee’s right began to change in a series of Supreme Court cases that dealt with the freedom of association. See Keyishian v. Board of Regents, 385 U.S. 589 (1967) (invalidating New York statutes barring employment on the basis of membership in “subversive” organizations); Cafeteria Workers Local 473 v. McElroy, 367 U.S. 886, 898 (1961) (dictum) (government could not deny employment because of previous membership in a particular party); Wieman v. Updegraff, 344 U.S. 183 (1952) (state could not require employee’s oath denying past affiliation with Communists). See generally Van Alstyne, The Demise of the Right-Privilege Distinction in Constitutional Law, 81 Harv. L. Rev. 1439 (1968) (arguing that because of the size and power of the government today, courts should control the state through substantive due process).

weighted heavily in favor of deferring to the government’s compelling need for secrecy.

A balancing test was first set forth in *Pickering v. Board of Education*,137 where the Court upheld the right of a teacher to criticize the operations of the school system in which she worked.138 The *Pickering* approach considers the identity of the person as a government employee to be important. The Court’s use of a balancing test, rather than a stricter test, parallels the less severe scrutiny now used in challenges on overbreadth grounds.139

In *Broadrick v. Oklahoma*,140 the Court refused to find a state statute regulating the political activities of state employees constitutionally invalid because it was not “substantially overbroad.” *CSC v. Letter Carriers*,141 decided the same day as *Broadrick*, upheld the validity of the federal counterpart to the state statute involved in *Broadrick*. *Letter Carriers*, however, upheld the statute by invoking the *Pickering* balancing test; the Court concluded that the government’s interest in limiting partisan activities outweighed the first amendment rights of the employee.142

Recently, in *Connick v. Meyers* the Court intimated that *Pickering* and its progeny apply only if the employee speech in question relates to matters of “public concern.”143 If “public concern” encompasses all matters that are of interest to the public, then classified information is arguably within this category. If, however, the “right to know” does not include the right of access to government secrets, a better interpretation of “matters of public concern” would exclude matters involving government secrets. Even if classified information were of public concern, the *Pickering* balancing test would probably permit some government restrictions; where employee expression involves national security, the government’s interest in secrecy is significant. Indeed, in cases involving national security, the Supreme Court has been deferential towards governmental regulation.144

137 Id.
138 “The problem in any case is to arrive at a balance between the interests of the teacher, as a citizen, in commenting upon matters of public concern and the interest of the State, as an employer, in promoting the efficiency of the public services it performs through its employees.” Id. at 568.
139 For a discussion of the overbreadth doctrine see infra notes 193-200 and accompanying text.
142 Id. at 564.
144 See, e.g., *Haig v. Agee*, 453 U.S. 280 (1981), where the Court upheld the revocation of Philip Agee’s passport, despite his claim that this violated his first amendment right to criticize the government. Agee had been disclosing the identities of agents abroad in viola-
The *Pickering* line of cases seems to focus on the first amendment as a procedural protection. When discussing the regulation of speech in the context of national security, however, the better view is to regard the issue as substantive—the focus should be on the content of the speech. The few cases that explicitly address national security have arisen where the government has contracted explicitly with an employee to control his expression. Importantly, these cases emphasize the extent to which the government may regulate employee speech that contains secret information. The cases typically involve situations in which an employee of the Central Intelligence Agency signed a secrecy agreement promising not to disclose classified information.

In *Snepp v. United States*, the Supreme Court invoked the contractual remedy of constructive trust to confiscate the proceeds of a book a

44 The concerns reflected by *Pickering* and its progeny may be described as "procedural" because the underlying issue in these cases is usually whether dismissal from employment, an appropriate prerogative of the employer in most contexts, is unfair or arbitrary, especially where it follows criticism of the employer. In situations involving classified information, by contrast, there is not the same concern for arbitrariness; rather, the focus would be almost wholly on the ability to regulate such speech consistent with the first amendment. *Connick*'s emphasis on speech of "public concern" does not change the inquiry. A court would initially view the substance of the speech, but it would still use the *Pickering* balancing test.

At least one commentator has argued that *Pickering* is closely analogous to the leak situation: "[b]oth *Pickering* and unauthorized leaks involve publication of information by an employee particularly familiar with an issue and expression that is critical of the agency and that is intended to cause public interference with agency implementation of policy." Katz, Government Information Leaks and the First Amendment, 64 Calif. L. Rev. 108, 140 (1976). Leaks of classified information, however, present different concerns. The *Pickering* court and Katz's article focus on the purpose of disclosure and the regulation of employees in the workplace. The focus in cases involving leaks of classified information, by contrast, should be on the content of the information disclosed and on the government interest in protecting the secrecy of the information.

For a similar view, see Cheh, supra note 125, at 712.


former government employee had published without first obtaining clearance as set out in his employment agreement. Aside from the obligations imposed by the contractual agreement, Snepp's use of the information he derived from government employment did not enjoy the full protection of the first amendment. The Court, in dictum, stated that "this Court's cases make clear that—even in the absence of an express agreement—the CIA could have acted to protect substantial government interests by imposing reasonable restrictions on employee activities that in other contexts might be protected by the First Amendment." Snepp thus reflects the prevailing view that government employees' free speech rights are limited, particularly where national security is concerned.

Although Snepp could be read narrowly, as resting solely on the contract's secrecy agreement, a broader reading comports with the thrust of the opinion. The Snepp Court grappled primarily with the remedy sought—in this case a constructive trust. Concerning the government’s ability to regulate the dissemination of classified information, the Court clarified the interests at stake:

The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service. . . . The agreement that Snepp signed is a reasonable means for protecting this vital interest.

---

149 Id. at 509 n.3. The curious aspect of Snepp was that although the employee failed to fulfill his contractual obligations by obtaining preclearance review, the government stipulated that no classified material had been disclosed. Id. at 510. The Court thus rested its decision on the terms of the contract, finding that the violation of the contract "exposed the classified information with which he had been entrusted to the risk of disclosure." Id. at 511. Although the dissent disagreed with the Court's treatment of nonclassified information, it agreed that "even in the absence of a written employment agreement," Snepp had a "duty to protect confidential or 'classified' information." Id. at 518 (Stevens, J., dissenting).

150 United States v. Marchetti, 466 F.2d 1309, 1317 (4th Cir.), cert. denied, 409 U.S. 1063 (1972), explicitly makes this point: "We would decline enforcement of the secrecy oath . . . to the extent that it purports to prevent disclosure of unclassified information . . . ." See also Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362, 1370 (4th Cir.), cert. denied, 421 U.S. 992 (1975) (reaffirming the Marchetti holding and stating that an employee, "by his execution of the secrecy agreement and his entry into the confidential employment relationship, . . . [has] effectively relinquished his First Amendment rights").

151 The Snepp Court declined to comment on whether a constructive trust would have been available absent an agreement. 444 U.S. at 515 n.11. A more recent D.C. Circuit opinion expands Snepp beyond its facts: "It makes no difference to our analysis whether the government seeks to restrict the speech rights of its employees by individual contract or by a broad rule . . . . An explicit contract may, however, affect the remedies available to the government for breach of a constitutionally valid restriction." McGeehe v. Casey, 718 F.2d 1137, 1141 n.10 (D.C. Cir. 1983) (citing Snepp v. United States, 444 U.S. 507 (1980) (per curiam)).

152 444 U.S. at 509 n.3. Moreover, the Court stated that the CIA "is an agency thought by
Thus, Snepp stands for the proposition that in some circumstances the first amendment rights of employees must give way to vital national security concerns. Perhaps, the only limitation of Snepp is that it provides no substantive guidance for future resolutions of the conflict between employee expression and national security.

The United States Court of Appeals for the D.C. Circuit's recent decision in McGehee v. Casey, however, provides a test for the regulation of employee speech in the national security context: "First, restrictions on the speech of government employees must 'protect a substantial government interest unrelated to the suppression of free speech.' . . . Second, the restriction must be narrowly drawn to 'restrict speech no more than is necessary to protect the substantial government interest.'" The McGehee court, applying this balancing test, held that the CIA scheme for classification and censorship of "secret" information did not violate the first amendment.

The McGehee court found that censorship of "secret" information was a "substantial governmental interest" unrelated to the suppression of free expression because information classified as "secret" could cause serious damage to the national security. Second, the court held that "the classification criteria for 'secret' information reasonably confine the resulting censorship" because "they impede disclosure only when it poses a reasonable probability of 'serious' harm." McGehee and Snepp, together, show every President since Franklin D. Roosevelt to be essential to the security of the United States and—in a sense—the free world. It is impossible for a government wisely to make critical decisions about foreign policy and national defense without the benefit of dependable foreign intelligence." Id. at 512 n.7.

718 F.2d 1137 (D.C. Cir. 1983).

Id. at 1142-43 (quoting Brown v. Glines, 444 U.S. 348, 354-55 (1980)). Brown upheld an Air Force regulation that prohibited service members from circulating petitions without approval of the base commander. 444 U.S. at 353. The importance of McGehee is that it makes the Brown test applicable to government employment generally, without regard to the unique context of military necessity and discipline. But see Parker v. Levy, 417 U.S. 733, 758 (1974) ("the different character of the military community and of the military mission requires a different application" of the first amendment). Although McGehee concerned challenges involving the validity of secrecy agreements, at issue was "the CIA's substantive criteria and scheme for deciding how to classify, and thereby censor, writings of former agents." 718 F.2d at 1141.

McGehee involved only one level of classification—"secret"—defined by then Exec. Order No. 12,065, § 1-103, 3 C.F.R. 190, 191 (1979). See, supra, note 13 for other levels of classification in current Exec. Order No. 12,365.

718 F.2d at 1147.

Id. at 1143 (quoting Brown v. Glines, 444 U.S. 348, 354 (1980)).

Id.
that government employees are not protected by the first amendment when they disseminate classified information. Thus, the first amendment is not a bar to efforts by the government to proscribe the dissemination of classified information by its employees.

3. The Press

The Supreme Court has never considered the freedom of the press to be absolute. If the first amendment does not protect the speech, the press does not have a constitutional right to publish it. If, however, the speech is protected by the first amendment, the issue becomes whether the type of restriction placed on the press is constitutional. For the regulations imposing prior restraints, the level of scrutiny is very high and unlikely to be met by the necessary showing of harm. Where, however, the regulation is in the form of subsequent punishment, the required showing of harm is lower.

In 1931, the Supreme Court in *Near v. Minnesota* stated in dictum: "No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops." Because this language addresses the government’s powers in wartime, the viability of the *Near* dictum was unclear until recently. In 1981, however, the Su-

158 This conclusion is also implied by the frequent statements in decisions that the government has no compelling interest in regulating information that is unclassified or already in the public domain. See, e.g., Id. at 1141 (“The government has no legitimate interest in censoring unclassified materials.”); United States v. Marchetti, 466 F.2d 1309, 1313 (1972) (The first amendment precludes “restraints with respect to information which is unclassified or officially disclosed, but we are here concerned with secret information . . . .”).


160 But see New York Times Co. v. United States, 403 U.S. 713, 717 (1971) (per curiam) (Black, J., concurring) (“Both the history and language of the First Amendment support the view that the press must be left free to publish news, whatever the source, without censorship . . . .”).


162 283 U.S. 697 (1931).

163 Id. at 716.

164 Id.

165 Until the Pentagon Papers case, no court had occasion to test the contemporary significance of the *Near* exceptions. But, as Justice Linde of the Oregon Supreme Court has argued, the Pentagon Papers case could not properly test the validity of the *Near* dictum. Linde, Courts and Censorship, 66 Minn. L. Rev. 171, 193-95 (1981). First, the government in
Government Secrecy

preme Court in *Haig v. Agee* \(^{166}\) reaffirmed Near’s dictum that publication of some categories of national security speech, in certain contexts, is unprotected by the first amendment. Citing Near, the *Agee* Court stated that where “disclosures, among other things, have the declared purpose of

the Pentagon Papers case was seeking to enjoin the New York Times without clearly basing its claim on federal law. Indeed, no law applied to the facts posed by the Pentagon Papers case. Thus, the scope of the first amendment may not have been the proper issue. See New York Times Co. v. United States, 403 U.S. 713, 741 (1971) (per curiam) (Marshall, J., concurring) (“The issue is whether this Court or the Congress has the power to make law.”). Second, because of the lack of a statutory basis, the Court avoided the substantive issue of the scope of the first amendment and instead relied on the prior restraint doctrine. Linde, supra, at 185; see also Jeffries, Rethinking Prior Restraint, 92 Yale L.J. 409, 409 (1983) (“the significance of focusing on prior restraint was not all that clear”).

The preference for focusing on the procedural aspects of prior restraint and the lack of any applicable statute are well represented by an exchange between Alexander Bickel, arguing for the New York Times, and Justice Stewart:

**THE COURT** [Stewart, J.]: But let me give you a hypothetical case. Let us assume that when the members of the Court go back and open up this sealed record, we find something there that absolutely convinces us that its disclosure would result in the sentencing to death of 100 young men whose only offense had been that they were 19 years old, and had low draft numbers. What should we do?

**MR. BICKEL:** Mr. Justice, I wish there were a statute that covered it.

**THE COURT:** Well there isn’t, we agree—or you submit—so I’m asking in this case, what should we do?

**MR. BICKEL:** I’m addressing a case which I am as confident as I can be of anything, Your Honor will not find that when you get back to your chambers. It’s a hard case. I think it would make bad separation of powers law, but it’s almost impossible to resist the inclination not to let that information be published, of course.

**THE COURT:** . . . I’m posing a case where the disclosure of something in these files would result in the death of people who were guilty of nothing.

**MR. BICKEL:** You’re posing me a case, of course, Mr. Justice, . . . in which the chain of causation between the act of publication and the feared event—the death of these 100 young men—is obvious, direct, immediate—

**THE COURT:** That’s what I’m assuming in my hypothetical case.

**MR. BICKEL:** I would only say, as to that, that it is a case in which, in the absence of the statute, I suppose most of us would say—

**THE COURT:** You would say the Constitution requires that it be published, and that these men die? Is that it?

**MR. BICKEL:** No. No, I’m afraid I’d have—I’m afraid my inclinations of humanity overcome the somewhat more abstract devotion to the First Amendment, in a case of that sort.


\(^{166}\) 453 U.S. 280 (1981). In *Agee*, the Court held that the revocation of Philip Agee’s passport on the ground that his prior and continuing disclosures of the identities of intelligence agents posed a threat to national security was not a violation of his first amendment rights. Id. at 308-09. Agee had written two books that disclosed the identities of covert agents abroad. Dirty Work: The CIA in Western Europe (P. Agee & L. Wolf eds. 1978); Dirty Work 2: The CIA in Africa (E. Ray, W. Schaap, K. Van Meter, & L. Wolf eds. 1979).
obstructing intelligence operations and the recruiting of intelligence personnel . . . [t]hey are clearly not protected by the Constitution."

Moreover, the *Agee* Court expanded the applicability of *Near*'s dictum beyond the context of wartime and examined several factors in order to determine whether the speech in question was outside the scope of the first amendment.

*Agee*’s conduct, a campaign to fight the CIA by exposing covert agents abroad, was distinguished from prior cases where the Court had refused to uphold passport revocations on national security grounds based solely on speech, beliefs, or association. *Agee*’s publications had “the declared purpose” of obstructing the CIA’s activities and were thought to have caused “serious damage to the national security.” The Court concluded that “when there is a ‘substantial likelihood’ of ‘serious damage’ to national security . . . the Government may take action to ensure that the holder may not exploit the sponsorship of his travels by the United States.”

*Agee* reflects the Court’s recognition that some speech is unprotected by the first amendment. *Agee*, however, should not be construed too broadly for several reasons. First, *Agee*’s purpose to obstruct intelligence activities was important to the Court. Because few leaks will be accompanied by such express intentions, *Agee*’s significance is perhaps restricted to its facts. Second, the Court clearly required a showing of “serious damage to national security” to justify a ruling that the speech is unprotected. In *Agee* this showing was conceded by all parties, something unlikely to recur in future litigation. The Court has not articulated a standard of substantive first amendment protection, in cases not factually analogous to *Agee*, for speech implicating national security interests. Instead, where the press is concerned, the Court has focused on the form of the government regulation without deciding whether the first amend-

167 453 U.S. at 308-09.
168 The disclosures at issue in *Agee* did not occur during a war, and the Court recognized this fact: “[h]istory eloquently attests that grave problems of national security and foreign policy are by no means limited to times of formally declared war.” Id. at 303.
169 See *Aptheker v. Secretary of State*, 378 U.S. 500 (1964), and *Kent v. Dulles*, 357 U.S. 116 (1958), where the Court reversed decisions denying passports based only on political beliefs. The *Agee* Court stated that *Kent* did not consider the case of “an individual whose conduct is damaging the national security and foreign policy of the United States.” *Agee*, 453 U.S. at 304.
171 Id. at 309.
172 *Agee* called a press conference to announce a “campaign to fight the United States CIA wherever it is operating” and his intent “to expose CIA officers and agents . . . .” Id. at 283.
173 Id. at 287 nn.10 - 11.
ment protects the substance of the expression.

The Pentagon Papers case reflects the continuing significance of the doctrine of prior restraint. The doctrine prohibits the government from enjoining speech in advance of publication whether or not the speech is subject to subsequent criminal prosecution.\textsuperscript{174} The doctrine addresses the form of the regulation of speech rather than the underlying substance of the expression. The Court first recognized the constitutional distinction between prior restraint and the content of the speech in \textit{Near v. Minnesota},\textsuperscript{175} a decision relied on by at least two members of the majority in the Pentagon Papers case.\textsuperscript{176} Although the use of the doctrine of prior restraint has been recently criticized,\textsuperscript{177} most likely the distinction be-

\begin{itemize}
\item \textsuperscript{174} Emerson, The Doctrine of Prior Restraint, 20 Law & Contemp. Probs. 648, 648 (1955).
\item \textsuperscript{175} 283 U.S. 697, 720 (1931) ("The fact that the liberty of the press may be abused by miscreant purveyors of scandal does not make any the less necessary the immunity of the press from previous restraint in dealing with official misconduct. Subsequent punishment . . . is the appropriate remedy . . . .")
\item \textsuperscript{176} New York Times Co. v. United States, 403 U.S. 713, 733 (1971) (per curiam) (White, J., with whom Stewart, J., joined, concurring) ("Prior restraints require an unusually heavy justification under the First Amendment; but failure by the Government to justify prior restraints does not measure its constitutional entitlement to a conviction for criminal publication.")
\item \textsuperscript{177} See, e.g., Jeffries, supra note 165; Redish, The Proper Role of the Prior Restraint Doctrine in First Amendment Theory, 70 Va. L. Rev. 53 (1984).
\end{itemize}

Professor Redish argues that the doctrine of prior restraint is properly invoked only "when that restraint limits expression prior to a full and fair hearing in an independent judicial forum to determine whether the challenged expression is constitutionally protected." Redish, supra, at 72. Thus, the doctrine would impose a heavy presumption against validity on any form of administrative abridgment. Id. at 83. Moreover, interim judicial restraints, those granted prior to a full and fair hearing, should be granted only when a compelling interest, such as harm to the national security, can be demonstrated. Id. at 83, 85-86. Redish concludes that if the "full and fair hearing" rationale is accepted then "judicially issued prior restraints on expression are no more harmful to first amendment interests than are subsequent punishment systems . . . ." Id. at 90.

Professor Jeffries argues that the doctrine of prior restraint is one of "contemporary irrelevance" because it represents an approach which seeks to expand first amendment protection without addressing the underlying substantive content of the expression. Jeffries, supra note 165, at 420. The early and "doubtful pedigree of First Amendment protection against subsequent punishment created a powerful incentive for advocates of expanded constitutional protection . . . to describe the restriction at hand as a prior restraint." Id. at 413. But with recent limitations on the government's ability to penalize speech "there is no need to invoke that categorization in order to protect First Amendment freedoms." Id. at 420.

Professor Jeffries also takes issue with the distinction between prior restraint and subsequent punishment, at least as it relates to an injunction. Id. at 426-34. Jeffries argues that "[i]n not only are injunctions unlike administrative preclearance, they are also far more like subsequent punishments than the conventional rhetoric would suggest. In both cases the threat of punishment comes before publication; in both cases the fact of punishment comes after." Id. at 427. The chief difference is that an "adjudication of illegality precedes publication" in an injunction. Id. at 428. Jeffries regards the narrowly confined injunction order as
tween prior restraint and subsequent punishment is still important.\textsuperscript{178} Accordingly, the significance of this distinction to the publication of national security secrets is considered below.

The special disfavor accorded prior restraints is reflected in the requirement that the government establish that significant harm will occur without the restraint. According to the per curiam decision in the Pentagon Papers case, "[t]he Government ‘thus carries a heavy burden of showing justification for the imposition of such a restraint.’"\textsuperscript{179} Clearly, however, the independent significance of the prior restraint doctrine does not place an absolute bar against the use of these restraints. Nevertheless, no test can easily be found that defines when such a restraint is appropriate. The Pentagon Papers per curiam decision provided little guidance; although it seemed to implicitly require proof of direct, immediate, and

\textsuperscript{178} See, e.g., Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546 (1975). According to the Court:

\textsuperscript{179} 403 U.S. at 714 (quoting Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971)).
irreparable damage.\(^{180}\)

Thus, even in the national security context, a very heavy burden is placed on the government to justify imposing a prior restraint. Proof of direct, immediate, and irreparable damage is an extremely difficult burden because it requires an abstract assessment of the potential damage. As a result, the doctrine of prior restraint, as a practical matter, may place an absolute bar against prior restraints even where national security interests are at issue.

The Supreme Court has never decided a case where the government sought to punish the publication of national security secrets. In other contexts, however, the Court's stance is similar to the severe scrutiny used in cases involving prior restraints. In *Landmark Communications v. Virginia*,\(^{181}\) the Court reversed the criminal conviction, under a state statute, of a newspaper that disclosed information regarding confidential judicial proceedings. The Court employed a very strict standard of review: ""the substantive evil must be extremely serious and the degree of imminence extremely high before utterances can be punished"";\(^{182}\) a ""solidity of evidence\(^{183}\) is necessary to make the requisite showing of imminence. 'The danger must not be remote or even probable; it must immediately imperil.'""\(^{184}\) Virginia's failure to supply the necessary proof of imminent danger rendered the criminal statute invalid on first amendment grounds.\(^{185}\)

*Landmark*'s relevance to the disclosure of national security secrets may be questioned for several reasons. First, the Court noted that it was not ""concerned with the possible applicability of the statute to one who secures the information by illegal means and thereafter divulges it.""\(^{186}\)

---

\(^{180}\) The per curiam opinion did not reflect the absolutist position Justices Black and Douglas adopted in their concurrence. See 403 U.S. at 719 (Black, J., with whom Douglas, J., joined, concurring). But the other members of the majority provided similar tests, with Justice Brennan's opinion perhaps the most narrow: ""[O]nly governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea can support even the issuance of an interim restraining order."" Id. at 726-27 (Brennan, J., concurring). Justice Stewart would have required proof that ""disclosure . . . will surely result in direct, immediate, and irreparable damage to our Nation or its people."" Id. at 730 (Stewart, J., with whom White, J., joined, concurring). For a similar postscript reading of the Pentagon Papers decision, see Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 591-93 (1976) (Brennan, J., concurring).


\(^{182}\) Id. at 845 (quoting *Bridges v. California*, 314 U.S. 252, 263 (1941)).

\(^{183}\) Id. (quoting *Pennekamp v. Florida*, 328 U.S. 331, 347 (1946)).

\(^{184}\) Id. (quoting *Craig v. Harney*, 331 U.S. 367, 376 (1947)).

\(^{185}\) Id.

\(^{186}\) Id. at 837. Accord *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97, 105-06 (1979) (holding that a state may not criminally punish publication of an alleged juvenile delinquent's name when ""lawfully obtained by a newspaper").
Second, the peculiar nature of confidential proceedings inquiring into a judge’s conduct, present in Landmark, did not forewarn a third party that disclosure would be a criminal misdemeanor. Thus, a newspaper could not reasonably know that publication was proscribed.

The Landmark holding implicitly acknowledged this second limitation because the Court not only refrained from balancing any harm against a governmental interest, but also affirmatively embraced the publication of this type of information: “The operation of the [inquiry into judicial conduct], no less than the operation of the judicial system itself, is a matter of public interest. . . . The article . . . clearly served those interests in public scrutiny and discussion of governmental affairs which the First Amendment was adopted to protect.” The facts in Landmark do not present the type of forewarning of unlawful behavior inherent in a leak of classified information. Knowledge that information was classified would, in every case, warn of some unlawful action. Moreover, retention of information, knowing that it is classified, could itself be criminal. In short, Landmark does not analyze the problems posed by the publication of “illegally obtained” classified information.

Moreover, the heavy burden of proof in Landmark is inconsistent with the Court’s treatment of national security in Snepp and Agee. Admittedly, those cases evidenced a concern for harm to the national security that would equate disclosure of national security secrets with Landmark’s requirement that “the substantive evil must be extremely serious.” Landmark’s requirement of “imminence,” however, seems out of place when national security is compromised. Many disclosures could render grave damage to the national security without presenting a danger that “immediately imperils,” and yet, the “substantive evil” would be very great. Because the Landmark test does not cover such situations, it is

---

187 Similarly, the information disclosed in Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979), was obtained by interviewing witnesses at the scene of the crime. Id. at 99. The Court in Smith, moreover, characterized Landmark as one of a series of cases that “involved situations where the government itself provided or made possible press access to the information.” Id. at 102-03.

188 435 U.S. at 839.

189 The Landmark Court limited its analysis to the question of “publishing truthful information regarding confidential proceedings of the Judicial Inquiry and Review Commission.” Id. at 837.

190 435 U.S. at 845.

191 Such harm could occur, for instance, with the disclosure of secret research and development data concerning a “Star Wars” anti-ballistic missile defense. Certainly the nation’s safety is not “immediately imperiled,” since it would still require considerable time to convert the research and development data into a working weapons system. Moreover, the capability to launch this weapon assumes a certain level of industrial development. Theoretically, by the time such a weapon is launched, it could be obsolete. Alternatively, and just as
not appropriate for cases involving national security interests.

Nevertheless, a claim of harm to the national security should not automatically justify a prior restraint; rather, Agee and Snepp suggest that the government can legitimately regulate speech that would harm the national security, and the burden of proof should focus on whether that harm is likely to occur. Indeed, where national security is concerned the proper test should require a showing that serious harm to the national security has or will probably occur as a result of the publication.

Thus, the first amendment does not per se bar the legitimate governmental regulation of the publication of national security information. The distinction to which the Court has consistently clung involves the nature of the regulation. Where a prior restraint of disclosure of national security information is sought, the Pentagon Papers decision imposes on the government a burden of proof of harm that is unlikely to be met. Yet, the Court has consistently implied that it would more favorably treat a regime of subsequent punishment. Nevertheless, the reasoning of Snepp and Agee should be extended to allow the subsequent punishment of publications of national security secrets only upon a showing that serious harm to the national security is likely.

In summary, the protection of national security presents the most compelling justification for secrecy in government. Leaks of classified information that breach that secrecy should be proscribed. Where the disclosure of information would bring great harm to the national security, the first amendment does not prevent legislative regulation. The government is not under a constitutional obligation to disclose government secrets. Moreover, government employees do not have a constitutional right to disseminate classified national security information. Finally, the first amendment does not protect the press from subsequent punishment where publication poses a likelihood of serious harm to the national security.

The regulation of leaks, however, should not unduly interfere with the public's legitimate right to be informed about the government's activities. Where the regulation of leaks is concerned, the presumption should first

likely, it could render vulnerable missiles that previously were not vulnerable. But a decade or more might pass before the "substantive evil" actually transpired.

Justice Stewart, concurring in Landmark, perceived the limitations of the holding:

Though government may deny access to information and punish its theft, government may not prohibit or punish the publication of that information once it falls into the hands of the press, unless the need for secrecy is manifestly overwhelming. . . . National defense is the most obvious justification for government restrictions on publication. Even then, distinctions must be drawn between prior restraints and subsequent penalties.

Id. at 849 & n. (Stewart, J., concurring).
be in favor of open government, subject only to overriding concerns that the national security may be greatly harmed. Guided by this principle, Congress should proscribe unauthorized disclosures of classified information.

III. A PROPOSAL FOR A COMPREHENSIVE LEGISLATIVE SOLUTION

The previous section argued that the first amendment does not prevent Congress from proscribing the unauthorized disclosure of classified information. In drafting legislation to prevent the disclosure of government secrets, however, Congress must resolve other problems to regulate this disclosure effectively and constitutionally. The first two concerns are constitutional: a statute cannot be either unconstitutionally overbroad or vague. These concerns necessitate an examination of the role that the present executive classification system should play in efforts to prevent leaks. If the present classification system is to be the basis for criminal penalties, then Congress must confront problems of overclassification. Similarly, reliance on the present system raises questions about the scope of judicial review and the proper use of classified information at trial.

Both the substance and procedure of the executive classification system pose problems that dictate a more comprehensive solution than merely appending criminal penalties to the disclosure of information that is classified pursuant to executive order. As one possible solution, Congress could create an independent agency to determine whether information should be subject to protection. This agency should employ procedural mechanisms that reduce the tendency to classify documents or information that are not harmful to the national security. Congress should also enact a statute that criminalizes the knowing and unauthorized disclosure of information that this agency has independently determined requires protection by the criminal sanction.

\[192\] This note does not extensively analyze the overbreadth and vagueness doctrines. Instead, it provides a brief overview of the impact of these doctrines on the drafting of legislation to regulate the unauthorized disclosure of classified information. For extensive analyses, see generally L. Tribe, American Constitutional Law 710-736 (1978); Redish, The Warren Court, The Burger Court and the First Amendment Overbreadth Doctrine, 78 Nw. U.L. Rev. 1031 (1983); Note, The First Amendment Overbreadth Doctrine, 83 Harv. L. Rev. 844 (1970).
A. Drafting Concerns

1. The Overbreadth and Vagueness Doctrines

Given the clash between first amendment interests and national security interests, the most important concern in drafting a statute that regulates leaks is to confine its reach to those areas that necessitate regulation. Historically, courts have monitored regulation restricting first amendment rights by the use of the "overbreadth" doctrine. The practical and procedural significance of the overbreadth doctrine is that it presents an exception to traditional rules of standing. If a litigant can show that legislation impairs protected speech to a greater extent than is necessary to further a concededly legitimate governmental goal, he is allowed to challenge the validity of the statute on its face.

The United States Supreme Court in Broadrick v. Oklahoma recognized that application of the overbreadth doctrine is "strong medicine" and imposed new limitations on the reach of the doctrine. Most impor-

---

193 Thus, the substantive goal of the "overbreadth" doctrine is to protect "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials." New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

194 "Litigants . . . are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from constitutionally protected speech or expression." Broadrick v. Oklahoma, 413 U.S. 601, 612 (1973). But see Monaghan, Overbreadth, 1981 Sup. Ct. Rev. 1, 3 (arguing that the overbreadth doctrine does not "possess a distinctive standing component; it is, rather, the application of conventional standing concepts . . . .").

This doctrine has another important implication. As Professor Jeffries, supra note 165, has noted, the legality of an injunction traditionally "may not be challenged by disobeying its terms." Id. at 431. But subsequent criminal sanctions may be ignored and later challenged on grounds of overbreadth. If a statute is facially invalid, there is no supplementary punishment for disobeying its terms. By contrast, the challenge of an injunction on similar grounds "would be no defense in a contempt proceeding based on violation of that order." Id.


196 The Court stated:

[It]s function . . . attenuates as the otherwise unprotected behavior that it forbids the State to sanction moves from "pure speech" toward conduct and that conduct—even if expressive—falls within the scope of otherwise valid criminal laws . . . . Although such laws, if too broadly worded, may deter protected speech to some unknown extent, there comes a point where that effect—at best a prediction—cannot, with confidence, justify invalidating a statute on its face . . . . To put the matter another way, particularly where conduct and not merely speech is involved, we believe that the overbreadth of a statute must not only be real, but substantial as well, judged in relation to the statute's plainly legitimate sweep.
tantly, the Court held that only a statute "substantially overbroad" would be invalidated on its face. Courts have applied the Broadrick test to statutes concerning first amendment expression generally.

The requirement of "substantiality" in Broadrick is to be "judged in relation to the statute's plainly legitimate sweep." In regulating national security secrets, the governmental interest is plainly legitimate. Thus, any proposed legislation must be narrowly drawn to not sweep substantially beyond the rightful concerns posed by the unauthorized disclosure of classified information.

As noted previously, the government does not have an obligation to disclose secrets. Moreover, the government can proscribe the unauthorized disclosure of classified information without violating the first amendment. A subtle, yet pervasive, problem of overbreadth exists, however, in the standards of classification. If the classification scheme is not limited to information whose disclosure truly harms the national security, a statute based on this classification scheme may be overbroad. For example, a statute permitting the executive to classify merely embarrassing mat-

Id. at 615 (citation omitted).

197 Id. at 615.

198 See, e.g., New York v. Ferber, 458 U.S. 747 (1982). In Ferber, the Court did not find "substantially overbroad" a statute that prohibited persons from knowingly promoting a sexual performance by a child under the age of 16 by distributing material depicting such a performance. Id. at 774. The Court explicitly extended Broadrick to reach "traditional forms of expression such as books and films" involving "conduct plus speech." Id. at 771; see also Redish, supra note 192, at 1064 ("All overbreadth challenges will now be tested by the special 'substantiality' requirement").

Although the Court has not considered the overbreadth doctrine in the context of national security, it has similarly restricted that doctrine's reach in the military context. In Parker v. Levy, 417 U.S. 733 (1974), the Court upheld the court-martial of an officer for remarks "unbecoming an officer" and "to the prejudice of good order and discipline in the armed forces." Id. at 738. The Court noted that "the 'weighty countervailing policies' . . . which permit the extension of standing in First Amendment cases involving civilian society, must be accorded a good deal less weight in the military context." Id. at 760 (quoting Broadrick, 413 U.S. at 611); see also Winters v. New York, 333 U.S. 507, 524 (1948) (Frankfurter, J., dissenting) ("The requirement is fair notice that conduct may entail punishment. But whether notice is or is not 'fair' depends upon the subject matter to which it relates.").

199 Id. at 615. Professor Redish concludes that this test "probably should be construed to dictate that if the majority of cases reached by the statute does not involve protected conduct, the statute's overbreadth will not be deemed 'substantial,' even though it might be 'real.' " Redish, supra, note 192 at 1064.

200 One court, however, has rejected the contention that the "secret" level of classification was overbroad. McGehee v. Casey, 718 F.2d 1137, 1143 (D.C. Cir. 1983). The McGehee court stated that the criteria for "secret" information "reasonably confine the resulting censorship to cases in which a substantial government interest is served. The criteria do not sweep too broadly because they impede disclosure only when it imposes a reasonable probability of 'serious' harm." Id. (quoting Lanzetta v. New Jersey, 306 U.S. 451, 453 (1939); Connally v. General Constr. Co., 269 U.S. 385, 391 (1926)).
ters might be overbroad. Accordingly, the government should regulate only classified information that may legitimately be kept secret.

Whereas the overbreadth doctrine focuses on the substantive areas of expression impinged upon by government regulation, the 'vagueness" doctrine is concerned with the indefiniteness of penal statutes: "Due process requires that all 'be informed as to what the State commands or forbids,' . . . and that 'men of common intelligence' not be forced to guess at the meaning of the criminal law." Strictly speaking, vagueness is not a first amendment concern; rather, it is a due process concern. The vagueness doctrine requires fair notice of the prohibited conduct and the prevention of arbitrary and discriminatory enforcement.

Unlike overbreadth, the vagueness doctrine does not give litigants standing to challenge a statute on its face. Moreover, its reach is limited by the rule that a statute is not unconstitutionally vague when court decisions have clarified its meaning. A statute proscribing the knowing disclosure of classified information should not face vagueness problems for lack of fair notice because when a document is stamped "classified," the reader is on notice that disclosure is illegal.

The classification system, because of its necessary generalities, may implicate vagueness concerns. In addition to fair notice, the vagueness

202 But, "[w]here a statute's literal scope . . . is capable of reaching expression sheltered by the First Amendment, the [vagueness] doctrine demands a greater degree of specificity than in other contexts." Id. at 573.
203 The Court has focused primarily on three values offended by vague laws: fair notice of what is proscribed; the prevention of arbitrary and discriminatory enforcement; and the prevention of "chilling effects" that lead citizens to curtail their rightful first amendment freedoms. See, e.g., Grayned v. City of Rockford, 408 U.S. 104, 108-109 (1972).
204 Parker v. Levy, 417 U.S. 733, 756 (1974) ("One to whose conduct a statute clearly applies may not successfully challenge it for vagueness.").
205 See, e.g., id. at 752-54 (narrowing statutes' broad scope by adopting constructions of the United States Court of Military Appeals and other military authorities).
206 Vagueness would not be an issue where, for example, a statute criminalized the knowing disclosure of information that was, in fact, classified. It would, however, be relevant where the criminal statute incorporated the classification standards themselves as the basis for liability. One advantage of incorporating the classification system into a penal statute is that the standards are more precise than those found in, for example, the espionage statutes or the vague term "national security." Thus, the problem of curing vagueness by requiring a scienter is unnecessary. See, e.g., the discussion of Gorin v. United States, 312 U.S. 19 (1940), supra notes 36-39 and accompanying text, where the Court cured the vagueness of the term "relating to the national defense" by incorporating a "bad faith" requirement. Gorin, 312 U.S. at 26-28. In contrast, an individual who discloses classified information would be apprised that his action was proscribed. He would not need to guess whether his conduct violated the law. Thus, the only scienter required in this context would be "knowledge" of classification, and because such information is clearly marked as classified, this
doctrine "requires legislatures to set reasonably clear guidelines for law enforcement officials and triers of fact in order to prevent 'arbitrary and discriminatory enforcement.' " Accordingly, the classification system itself could be challenged on vagueness grounds unless the government has adopted specific standards for classification decisions. Without such standards, decisions to classify may be arbitrary and thus unconstitutionally vague.

The present Executive Order regulating the classification scheme provides both for "levels" of classification—confidential, secret, or top secret—and "categories" of classification—e.g., military plans and intelligence activities. Each classification level refers to the "national security" as a standard by which to determine the degree of secrecy protection desired. Although "national security" is "inherently vague," Execu-

requirement is more relevant to a third party receiving the information than to the leaker. Consequently, vagueness would only be a concern when the standards for classification, and for liability, were themselves indefinite.


But see McGehee v. Casey, 718 F.2d 1137, 1145-46 (D.C. Cir. 1983) (rejecting a vagueness challenge to the "secret" classification). The McGehee court declined to pass on the "confidential" classification. Id. at 1147.


Id. § 1.1; see supra note 13.

Id. § 1.3, which provides:

Classification Categories.
(a) Information shall be considered for classification if it concerns:
(1) military plans, weapons, or operations;
(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
(3) foreign government information;
(4) intelligence activities (including special activities), or intelligence sources or methods;
(5) foreign relations or foreign activities of the United States;
(6) scientific, technological, or economic matters relating to the national security;
(7) United States Government programs for safeguarding nuclear materials or facilities;
(8) cryptology;
(9) a confidential source; or
(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President.


See supra note 13 for the text of the classification level criteria.

Government Secrecy

1985]

Government Secrecy

853

tive Order 12,356 specifies the types of information that may be classified. Such added specificity will likely save the classification scheme from vagueness challenges.

In *McGehee v. Casey*, the United States Court of Appeals for the D.C. Circuit relied on the executive order's added specificity to uphold the "secrecy" level of classification against a vagueness challenge. In doing so, the court noted that the classification categories provided added degrees of particularity. Although it found some additional vagueness in the classification categories, the court concluded that the CIA's own administrative standards of classification narrowed these terms. Finally, the court noted that judicial review of an agency's classification decision was always available and judicial construction may narrow the broad language.

Although the *McGehee* court identified terms such as "national security," "foreign affairs," or "foreign relations" as potentially vague by themselves, it did not consider those words and their function in the classification process. A classification category is unable to address every conceivable event because varied situations inevitably arise. As a result, it may be impossible to use more specific words to establish classification standards. The classification system may need broad language to cover unusual circumstances. For the reasons articulated in *McGehee*, as well as the nature of the classification process in the national security context, the classification scheme is probably not unconstitutionally vague.

Thus, a narrowly drawn statute will solve vagueness problems, although it may not allay all concerns of overbreadth. Overbreadth may be prevented, in part, by narrow and precise standards of proscribed conduct, but it is still a problem in the classification system employing those standards. Accordingly, if Congress is to prevent leaks by reference to the classification system, it must confront the special problems posed by that system.

2. The Executive Classification System

Use of the executive classification system by Congress to prevent leaks presents several problems. First, and most importantly, Congress must

214 See supra note 211.
215 718 F.2d 1137, 1147 (D.C. Cir. 1983).
216 Id. at 1143-44.
217 Id. at 1144-45. The CIA, to guide employees in classifying information, used the Agency Information Security Program Handbook: Classifying, Declassifying, Marking and Safeguarding National Security Information. Id. at 1145 n.15.
218 Id. at 1145. Judicial review was available because *McGehee* presented a challenge to the CIA's censorship pursuant to a prepublication review agreement.
try to reduce overclassification so that the statute is not overbroad. A related problem is the proper role of judicial review in prosecutions involving classified information. Finally, contested decisions to classify pose special problems at trial about the release of classified information to either party.

A major criticism of the classification system is that it is inherently subject to overclassification. Overclassification can take several forms: the classification of nonsecret information included in documents that are otherwise properly classified; the classification of information that no longer presents any harm to the national security; or the classification of information whose disclosure would not damage the national security.

The underlying fear of overclassification is that the executive branch, through either inadvertence or purposeful conduct, will withhold information that should legitimately be public. For example, the present executive order expressly prohibits the classification of information that is not legitimately kept secret, but it also requires a presumption in favor of classification where any doubt exists. This example probably typifies the most frequent, yet subtle, form of overclassification: when in doubt, classify.

Overclassification has several adverse consequences. The public is deprived of information that it needs to keep abreast of the government's actions or policies. More directly, any scheme that affirmatively regulates the disclosure of classified information impinges on some protected speech. If Congress were to criminalize the unauthorized disclosure of information that is merely classified pursuant to an executive order, that scheme would likely be overbroad. Overclassification, moreover, de-

220 As Professor Emerson has stated, "[t]he function of the censor is to censor. He has a professional interest in finding things to suppress." Emerson, supra note 174, at 659. An extreme view of present overclassification abuses is reflected in the oft-quoted testimony before Congress by William G. Florence, a former Pentagon security officer, who stated that of the twenty million classified documents, "less than one-half of 1 percent . . . actually contain information qualifying even for the lowest defense classification. . . ." A. Schlesinger, The Imperial Presidency 329 (1974).

221 See Reagan Order, supra note 13, at 170 Section 1.6(a) states that "information [cannot] be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security."

222 Id. at 167. Section 1.1(c) states that "[i]f there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination . . . ."

223 As Professor Jeffries explains:

[t]here would be the bureaucrat's usual incentive to exaggerate the significance of his own responsibilities by assigning high security classifications to what he reviews; the expert's predictable bias toward overemphasizing the considerations that flow from
tracts from the legitimate purposes of classifying information to prevent harm to the national security.\(^{224}\)

In short, the present administrative scheme does not provide the appropriate mechanism on which to base criminal liability. Congress should be guided by the principle that liability should extend only to conduct that is likely to harm the national security. A showing that information is classified, without more, does not erase all doubts about the propriety of classification; yet, when someone is subject to a criminal sanction, there should be no reasonable doubt as to the harmful consequences of his act.

Doubts concerning the propriety of a particular classification decision at issue in a criminal prosecution are not eliminated by the prospect of judicial review. Requests for disclosure of classified information under the FOIA and prepublication review agreements invoke some degree of judicial review.\(^{225}\) By contrast, statutes that make the knowing disclosure of classified information a crime do not render classification decisions open to examination.\(^{226}\)

The 1962 decision in *Scarbeck v. United States* held that where the use of classified information is an element of an offense no inquiry into the decision to classify is proper.\(^{227}\) As a matter of policy, this decision is cor-

---

Jeffries, supra note 165, at 435.

\(^{224}\) "For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained." New York Times Co. v. United States, 403 U.S. 713, 729 (1971) (per curiam) (Stewart, J., concurring).

\(^{225}\) Requests under the FOIA for information that is classified pursuant to Executive Order place the burden of proof on the executive agency to justify its claim of exemption from disclosure under 5 U.S.C. § 552(b)(1). See 5 U.S.C. § 552(a)(4)(B) (1977). In addition, FOIA calls for de novo judicial review of an agency decision. Id. This review is to determine whether the information is "properly classified." Id.

Similarly, the *McGehee* court held that a challenge to the CIA's determination that a manuscript submitted for prepublication review contained classified information required in camera judicial review of the CIA's justification. McGehee v. Casey, 718 F.2d 1137, 1148-49 (D.C. Cir. 1983).

\(^{226}\) See, e.g., United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir.) ("Under section 798 [of the Espionage Acts], the propriety of the classification is irrelevant. The fact of classification of a document or documents is enough to satisfy the classification element of the offense.") ("Under section 798 [of the Espionage Acts], the propriety of the classification is irrelevant. The fact of classification of a document or documents is enough to satisfy the classification element of the offense."). cert. denied, 444 U.S. 855 (1980). For the text of § 798, see supra note 48.

\(^{227}\) 317 F.2d 546, 558-60 (1963). The prosecution was brought under § 783(b) of the Espio-
rect with respect to government employees. A superior's classification decision should bind an employee that knows of the decision. The Scarbeck court noted, moreover, that to hold otherwise would nullify the legitimate goals of the statute:

[The trial of the employee would be converted into a trial of the superior. The Government might well be compelled either to withdraw the prosecution or to reveal policies and information going far beyond the scope of the classified documents transferred by the employee. The embarrassments and hazards of such a proceeding could soon render [the statute] entirely useless . . . .]

Several factors, however, caution against applying the Scarbeck rule to a statute that criminalizes unauthorized disclosures and publication of classified information. First, the Scarbeck court relied heavily on congressional intent "to make the superior's classification binding on the employee." Although this rule is sensible when applied to government employees, it does not address the concerns that arise where nongovernment persons, such as members of the press, are protected. Although Congress may punish the press where the disclosures are likely to damage the national security, the absence of an employer-employee relationship calls for institutional procedures that eliminate any doubt about the propriety of classification. Nor does it follow that the same quantum of harm posed by a disclosure that is sufficient to punish the employee would suffice to punish a member of the press due the special protection the first amendment gives to the press.

Second, Scarbeck was a prosecution involving aid to a foreign government. The Scarbeck rule thus is most appropriate when it is invoked in circumstances akin to espionage. When the actor's conduct evidences an intent to harm the United States, whether the documents were properly classified may be relevant. By contrast, leaks are not, as a rule, intended to harm the United States or to assist a foreign power. Thus, the inquiry should be whether disclosure is likely to harm the national security, not whether the leaker intended this harm. The present classification system, however, may call for the classification of documents even when their disclosure may not harm national security.

There are compelling reasons for not reexamining at trial the propriety of a decision to classify information. For example, the judiciary is ill-


nage Statutes, see supra note 51, which makes the unauthorized disclosure of classified information to an agent of a foreign government a crime.

228 317 F.2d at 560.
229 Id.
230 Scarbeck was charged with communicating classified information to representatives of the Polish government. Id. at 548-49.
equipped to second-guess executive branch classification decisions.\footnote{In the Pentagon Papers case, Justice Harlan stated that "in my judgment the judiciary may not . . . redetermine for itself the probable impact of disclosure on the national security." New York Times Co. v. United States, 403 U.S. 713, 757 (1971) (per curiam) (Harlan, J., dissenting). Cf. Chicago & Southern Airlines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) (these are "decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility").} Most importantly, such a reexamination at trial may result in the disclosure of more classified information. If the defendant is permitted to question the validity of a classification decision, the defense will make discovery requests for other secrets in an attempt to show that a particular document was not validly classified, or that it posed no harm to the national security. In such cases, the government may refuse to continue the prosecution for fear of disclosing additional secrets.

Although the Classified Information Procedures Act (CIPA)\footnote{18 U.S.C. app. §§ 1-16 at 549 (1982).} was enacted to address problems posed by the use of classified information during a prosecution, it does not prevent further disclosures of classified information at trial. CIPA was enacted to remedy the "grey mail" problem where a defendant makes vague or implicit threats that prosecution will result in the further disclosure of classified information.\footnote{See S. Rep. No. 823, 96th Cong., 2d Sess. (1980), reprinted in 1980 U.S. Code Cong. & Ad. News 4294.} CIPA applies in any case where the defendant attempts to admit classified information into evidence as reasonably necessary to all or part of his defense.

CIPA remedies the "grey mail" threat by imposing a duty on the defendant to specify, before trial, the classified information that he would disclose at trial.\footnote{One court summarized CIPA as follows: 

It is to provide procedures under which the government may be made aware, prior to trial, of the classified information, if any, which will be compromised by the prosecution. To that end, the defendant who reasonably expects that his or her defense will result in the disclosure of classified information is required, to assure admissibility of such information at trial, to give the court and the government prior notice of the classified information deemed involved. . . . [The government] may seek a ruling that some or all of the proffered classified information is not material. 18 U.S.C. app. § 6(a) (1976 & Supp. V 1981). It may move that a non-sensitive summary of the classified information be substituted for it, or it may admit a fact or facts sought to be proved by classified information, thus obviating the need for it. 18 U.S.C. app. § 6(c). Part or all of these pretrial proceedings are held in camera at the government's request. When the real cost to national security has been ascertained (or eliminated) by the CIPA procedure, the government can realistically weigh the nation's interest in prosecuting against that cost and make an informed decision. . . .

To insure fairness in the prior determination of the issues, the government is required to reveal details of its case to the defendant, 18 U.S.C. app. § 6(b)(2), including the evidence the government will use to rebut the defendant's revealed classified}
all, or part, of this evidence is inadmissible, but in doing so the court may effectively bar the government from continuing the prosecution.\textsuperscript{235} CIPA's importance is that the government may determine that the costs of disclosure outweigh the benefits of prosecution before trial rather than be surprised by evidence admitted at trial.

CIPA's resolution of the problem of disclosures, however, is limited. If classified information is material to the defense, nothing in CIPA suggests that it cannot be admitted into evidence.\textsuperscript{236} If evidence on the propriety of classification calls for further disclosures of classified information, the government may not prosecute. Thus, Congress should legislate a criminal sanction that forecloses the need for this type of reexamination, not by providing a defense of improper classification but by instituting changes in the present administrative system to eliminate most of the risks of improper classification.

The risks presented by the disclosure of classified information at trial are not present when the defendant claims that the information disclosed was already available to the public. When the "leaked" information is already in the public domain, there has merely been an attempted leak. The guiding principle in regulating leaks should be the prevention of harm to the national security. The corollary to this principle is that prevention of harm to the national security can be accomplished by maintaining secrecy. Any information already available to the public is, of course, not secret\textsuperscript{237} although it may still be regarded as classified.\textsuperscript{238}

Nevertheless, a significant controversy surrounds the propriety of regulating classified information that has escaped into the public domain. Although attempts to commit crimes are often punished in other contexts, the justification for punishing unauthorized leaks in spite of first amendment interests is harm to the national security. Of course, a mere attempt to leak does no tangible harm to the nation. Thus, first amendment inter-
ests can be accommodated by eliminating attempts to leak, or leaks of already public information, from the scope of a criminal statute. The statute should place on the defendant the burden to prove that the matters disclosed were already in the public domain.239

Thus, a statutory solution to the problem of unauthorized leaks must be narrowly drawn to avoid violating vagueness principles and restricted in scope so as not to implicate overbreadth concerns. Additionally, a solution must address the difficulties presented by the executive classification system. The next section proposes a legislative solution to these concerns.

B. A Proposal for a Comprehensive Legislative Solution

Only those government secrets necessary to national security should be protected from unauthorized disclosure by criminal penalties.240 Moreover, before the imposition of criminal liability, the likelihood of serious harm to the national security should be shown. Congress should therefore establish both the categories of information to be protected and the particular level of harm that must flow from disclosure before criminal penalties obtain. Additionally, Congress may want to separate and insulate this process from the vagaries of the executive classification system by establishing an independent administrative agency. This agency would be solely responsible for deciding what information will be protected with criminal sanctions. This section proposes a legislative scheme that satisfies these concerns.

Congress should consider creating a separate and independent administrative body,241 the Classification Screening Agency (CSA), to decide which government secrets merit added protection by the criminal sanc-

239 FOIA cases have acknowledged that publicly known information cannot be withheld under exemptions 1 and 3. See, e.g., Founding Church of Scientology v. National Sec. Agency, 610 F.2d 824, 831-32 (D.C. Cir. 1979); Lamont v. Department of Justice, 475 F. Supp. 761, 772 (S.D.N.Y. 1979). Nonetheless, FOIA cases also protect the specific context within which information is located, even if certain parts of the information are already known. Afshar v. Department of State, 702 F.2d 1125, 1130-32 (D.C. Cir. 1983); Phillippi v. CIA, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981); Military Audit Project v. Casey, 656 F.2d 724, 741-45 (D.C. Cir. 1981). Thus, any defendant accused of leaking classified information should, in order to prevail on this point, show that the disclosed knowledge itself did not reveal any additional secrets.

240 See infra note 253 and accompanying text.

241 A separate administrative agency will limit the abuses of overclassification inherent in the executive classification system. Whereas members of the executive branch are inclined to protect all information, an independent agency has no such inclination. As noted previously, supra note 223 and accompanying text, merely attaching the criminal sanction to classification decisions made by officials in the executive branch would implicate the overbreadth doctrine. An independent agency is necessary to eliminate any conflict of interest in classifying information to significantly curtail the potential for overbreadth.
tion. The CSA should consist of the Classification Screening Board (CSB) and screening officers to be nominated by the executive branch subject to the consent of the Senate. The CSB will be the operative body within the CSA to decide, by majority vote, whether information or documents are appropriately protected against unauthorized disclosure by criminal penalties.

The CSB will only examine information that is already classified by the executive branch. When the government wants greater protection for its secrets, it will transfer the classified information to the CSA. A screening officer will review either the information itself or a detailed affidavit prepared by the original classifying body that states the justifications for greater protection. If the officer cannot make a reasonable decision based on the affidavit, he can request the documents themselves. This affidavit shall also state, or the screening officer should ascertain, the extent of the expected harm from disclosure and the information's secrecy category. The screening officer may oppose the government's application in a proceeding before the CSB if he feels that it does not merit protection because the request falls outside of congressionally enacted standards or that disclosure will not result in sufficient harm. If an outside party opposes the government's application, the screening officer should represent this party's interest against the government.

---

242 Ideally, to insulate the CSA totally from the control of the executive branch, Congress should appoint the members of the CSB and each screening officer. This procedure would, however, violate the appointment powers granted to the executive. See Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam). Congress, however, retains considerable control over the CSA through its ability to reject the executive's nominees.

243 This limitation is one of convenience. Because of the executive's interest in protecting the national security, the executive classification system serves as the most far-reaching effort to define what disclosures would be harmful. If information is not important enough to classify pursuant to executive order, there is no need to duplicate that determination. Thus, as a matter of administrative convenience the initial screening of information is best left to the executive. Moreover, this scheme sets up a two-step process that helps to insure against overclassification. First, the executive must determine that the disclosure would be harmful. Second, the CSA must determine that disclosure would also be harmful according to congressional guidelines.

244 This two-step process necessarily imposes additional costs to the executive branch. This scheme ensures that the executive will calculate whether the benefits of protection outweigh the administrative costs.

245 Thus, this scheme places the burden of proof on the executive branch to justify protection by criminal penalties. By contrast, the present executive classification system imposes no such obligation on anyone, although it provides several categories of classified information.

246 The primary justification for this adversarial procedure is to institutionally eliminate any proclivity to overclassify or to classify without consideration of the public's right to be informed about government action. Thus, the screening officer's duty is to oppose the government's applications unless they clearly merit additional protection.
screening officer is vested with an institutional responsibility to oppose the government's application unless he determines that the information is clearly within the statute.

When the CSB receives the government's request, whether or not opposed by the screening officer, it will decide in a closed hearing whether the information should be protected according to congressionally enacted standards. If the screening officer opposes the government's request, the government may send a representative to argue for its position or, if it chooses, rest on its affidavit. The hearing will be confidential, and the CSB's decision will be the final administrative action in the matter.247

Once the CSB determines that the information should be protected with criminal sanctions, it shall "stamp" the documents or, in the event of computer-stored information, shall program a warning to be displayed upon viewing or printing the information.248 This stamp shall state that the CSA has determined that unauthorized disclosure of the information, by any person, will result in criminal prosecution. Once the material or documents are stamped, they will have the status of Protected Information.

An "unauthorized" disclosure is any disclosure of Protected Information that has not been declassified pursuant to procedures embodied in

---

247 If the CSB denies the government's request there is no reason in policy or precedent to provide judicial review of the CSB's decision. The government may still rely on administrative or civil remedies to protect classified information. Judicial review, moreover, should not be provided if the CSB determines that the information warrants additional protection. The judiciary has neither the aptitude nor the means with which to challenge the CSB's decision. As noted previously, supra note 226, courts have not inquired whether information classified pursuant to executive order was properly classified in prosecutions of intentional disclosure of classified information. Where the information is subject to an additional determination by an independent agency, with the safeguards outlined above, there is even more reason to defer to the judgment of the CSB.

The theory underlying the creation of an independent agency is separation of powers. This proposal is thus markedly dissimilar from the "Official Secrets" regime that presently exists in several western democracies, most notably Great Britain. See the Official Secrets Act, 1911, 1 & 2 Geo. 5, ch. 28, as amended, 10 & 11 Geo. 5, ch. 75 (1920) and 2 & 3 Geo. 6, ch. 121 (1939). The British Official Secrets Act creates a presumption that all government-owned or controlled information is "official" and proscribes the unauthorized dissemination or publication of official "secrets."

While the Official Secrets Act has provoked a great deal of criticism over the years, it has proved remarkably durable. Nonetheless, its days may be numbered, since the movement for a freedom of information act in Great Britain has grown much stronger. See J. Michael, The Politics of Secrecy: The Case for a Freedom of Information Law (1979). For a comparison of executive secrecy in the Western democracies, see T. Franck & E. Weisband, Secrecy and Foreign Policy (1974).

248 This requirement is necessitated by the accompanying criminal penalties that make only "knowing" disclosure of this information criminal. Thus, a "stamp" would ensure that those handling the documents know of their status.
an executive order and is made to any person not authorized pursuant to executive order to receive the information.\textsuperscript{249} The executive branch can, of course, declassify any classified material by following procedures set out in an executive order. If, however, the executive wishes to declassify "Protected Information" it must notify the CSA before the information may be disclosed without invoking criminal penalties.

The CSA should maintain an index of all government applications, including those requests granted and denied.\textsuperscript{250} A document's status as Protected Information shall last no longer than three years; then the government must submit a new application explaining why the information requires continued protection.\textsuperscript{251} The stamp placed on the document should, if possible, contain an expiration date.\textsuperscript{252} For information requiring protection for less than three years, the CSA may specify an amount of time that the status as Protected Information will last.

In conducting the screening process, the CSB shall review the government's request using three criteria. First, the executive branch must have already classified the information pursuant to executive order. Second, the CSB must determine that the information falls within congressionally created categories of information that require secrecy. Third, the CSB must determine that disclosure of the information would likely result in serious damage to the national security.

\textsuperscript{249} This definition of "unauthorized" serves two purposes. First, the requirement that information not be declassified resolves the potential conflict when a document is stamped "Protected Information" but has been declassified by the executive. If the executive wishes to declassify Protected Information it must notify the CSA. This ensures that the executive will not manipulate secrets to its advantage by relying on threats of criminal prosecution while "officially leaking" information for political purposes. Information that is Protected Information has been determined to require protection, and should not lose its character solely by executive disclosure. Second, the requirement that "authorization" be made by reference to the executive order achieves an integration of the two systems that protects the executive's legitimate and necessary determinations as to who is authorized to receive information.

\textsuperscript{250} An index of those requests granted provides proof of what information was actually stamped "Protected Information." An index of rejected requests ensures that the executive branch cannot resubmit the same material for another determination, although it may do so if new justifications or circumstances arise.

\textsuperscript{251} Limiting "Protected Information" to three years serves two related purposes. First, this requirement precludes the potential inherent within the executive classification system to keep information classified indefinitely even though its disclosure poses no harm to the national security. A related purpose is to provide the CSB some flexibility in determining the proper length of time for protection. The agency may refer to specific conditions—e.g. for the duration of an intelligence operation or negotiation process—or by reference to a specific term of months or years. Although some information will require protection beyond three years, the executive may easily resubmit an application for further protection.

\textsuperscript{252} This ensures that those handling the documents know when looking at a document whether it is still Protected Information.
Congress should limit the extension of Protected Information to the following categories:

1. details of future military operations, military plans, defense contingency plans, and national strategy during wartime;
2. characteristics of weapons systems, installations, and projects;
3. secret technology during its research and development stage;
4. intelligence activities, sources, methods, and cryptology or code information; and
5. details concerning on-going diplomatic negotiations and foreign relations.

The disclosure of information or documents outside these categories should not be subject to criminal sanctions. The executive branch should also establish that disclosure of such information would likely result in serious damage to the national security before the CSA should impose a penalty for unauthorized disclosure.

The CSA should also attempt to spot government efforts to protect information that is not legitimately secret. The executive may, for example, attempt to conceal embarrassing facts or details of official wrongdoing. Other types of "invalid" secrecy interests include attempts to hide incompetence, inefficiency, wrongdoing, and administrative error, or to restrain competition and independent initiative.

If the CSA finds such information in an executive agency's application,

---

253 Thus, information that was merely embarrassing or related to illegal activities would clearly not qualify under these five categories. In the event that embarrassing information is intermingled with information that requires protection, the embarrassing information should be segregated. If this is not possible, the CSB should deny the executive's request for criminal penalties. As with other provisions, this in effect coerces the executive to seek criminal penalties where the information clearly deserves protection.

These categories are narrower than, for example, the present classification system because there is no provision for information that falls outside the five categories, even if the disclosure would damage the national security. See Reagan Order, supra note 13, at 169, § 1.3(a)(10). Note that under the first category of information protected by Congress, the Pentagon Papers would not qualify for protection by criminal penalties because they did not contain details of future military operations or national strategy.

254 This criterion is considerably narrower than the standard of harm required for invocation of the "confidential" level of classification found in the present executive order. See id. § 1.1(a)(3), for the definition of "confidential" information. The standard is narrower to maintain the credibility and legitimacy of a system that deters unauthorized disclosures with criminal sanctions.

255 Like the categories of information that qualify as Protected Information, the categories of "invalid" secrecy interests are contained in the present scheme. See Reagan Order, supra note 13, § 1.6. Both the categories of qualifying and invalid secrecy interests, however, should be affirmatively enacted by statute because the executive may at any time enlarge or restrict the scope of the executive classification system.
it should attempt to separate this invalid information from any legitimate secrets. If there are no legitimate secrets, or if the attempted separation proves impossible, the CSA should deny the executive's application. The government may still impose administrative sanctions for unauthorized disclosure. Congress, however, should require that the CSA disclose any embarrassing or illegal information to the appropriate congressional committee. Congress should also penalize the disclosure by a member of the CSA of any classified information if the disclosure is made to anyone other than a member of Congress.

In addition to the creation of the CSA, Congress should criminalize the unauthorized disclosure of Protected Information. This statute would be rather simple. By creating the CSA, Congress has already dealt with the troublesome problem of defining what information falls within the statute's ambit. The statute, then, will provide for criminal penalties for the knowing and unauthorized disclosure of Protected Information by any person.

A "disclosure" should include any communication such as the delivery of documents or their publication. A "knowing" disclosure requires knowledge that the information is Protected Information, that the disclosure is unauthorized, and that the actor's conduct resulted in a disclosure. Finally, "any person" should include not only a government employee but also a publisher of the information.

256 This obligation will discourage baseless claims for additional criminal penalties. It is also a recognition that the public, through its elected representatives, should be notified of such government activity. In order to prevent the CSA from becoming an additional source of leaks, however, the agency can disclose only to the appropriate congressional committee.

257 This statute avoids any problem of vagueness because it clearly delineates the proscribed conduct, and the defined standard of classification eliminates arbitrariness concerns. Moreover, the required scienter is "knowledge," which is the highest culpability standard short of requiring an intent to harm the United States. There is no effort to proscribe reckless or negligent conduct because the justifications for invoking criminal penalties are arguably not as compelling.

258 Proof that the information is Protected Information is established by certification from the CSA that it is recorded in an index compiled by the CSA and that the expiration date has not expired. Because of the elaborate safeguards provided by creating the CSA, there is no need to inquire into whether the information was properly deemed to be Protected Information. This statute therefore avoids the problems posed by the use of classified information at trial that would exist if more than proof of its status as "Protected Information" was required.

259 One of the more dramatic aspects of this statute is its express coverage of the publication of "Protected Information." As argued previously, see supra notes 188-91 and accompanying text, the first amendment does not bar the subsequent punishment of publication where national security is concerned. There are compelling reasons for proscribing such publications. Unlike the difficulty entailed in identifying leakers, determining who published Protected Information is presumably easy. In every instance of publication, the actor could quickly be ascertained. Thus, to forgo prosecution of the publisher is to accept the
Congress should also provide two affirmative defenses. The first is that the disclosure, although not authorized, was made only to a member of Congress. The second defense is that the disclosure was of information already in the public domain. Public domain should be read narrowly so that a defendant must show that the information in its total context, rather than in separate bits and pieces, was already available to the public.\textsuperscript{260}

C. Some Justifications for the Proposed Scheme

This section examines the underlying policies and the expected effects of the proposed statutory scheme. The proposed scheme seeks to surmount the difficulties of the present statutory framework while adequately protecting first amendment interests. This legislative scheme's primary goal is to close the significant gaps that now exist in the law. Most notably, the present legal framework does not punish the ordinary leak of information by a government employee to a member of the press.

Additionally, the proposed scheme is simple and clear, and much of the uncertainty in the law of government secrets will be eliminated. Potential offenders need not guess whether the statute applies to them. Nor would prosecutors hesitate to initiate leak prosecutions for fear of falling outside of an unclear or inaptly named statutory scheme such as the Espionage Act.

Moreover, no new classification system is needed. This system gives the executive branch flexibility in administering the executive classification system. The executive can choose not to send documents to the CSA if it is unlikely that they will pass the CSA's standards. Although the CSA adds a degree of protection for secrets, an executive agency may still counter unauthorized disclosures with administrative sanctions and civil remedies.

The proposed statute also addresses overbreadth and vagueness concerns. The statute is not vague because it provides clear notice of the proscribed conduct: all unauthorized disclosures of Protected Information are prohibited. Additionally, the proposed statute is not overbroad because it only applies to information whose disclosure would harm the national security, a narrow and restricted class of information. Moreover,

\textsuperscript{260} The concern here is that one should not be prosecuted for disclosing information that was already available to the public because the central goal of this statute is to protect secrecy. But if the information is available to the public only in parts, it may be that disclosure of the total document confirms information that was previously unknown.
the creation of an independent agency also helps to eliminate overbreadth concerns. The proposed scheme will encourage greater respect for information that is deemed Protected Information than the present executive classification receives; the new system addresses both overclassification and official leaks, two abuses in the present system.

The procedural steps that the executive must take to have information declared Protected better protects first amendment rights. While the proposed scheme would not result in the classification of any additional material, it does impose criminal sanctions on disclosure of some classified information. Criminal penalties, however, do not obtain until the CSA has decided that the information merits protected status after a screening officer has had an opportunity to contest the executive’s request. Injecting this element of adversariness into the classification process provides an institutional mechanism for focusing on the public interests involved. Most importantly, it counters any institutional tendency to overclassify documents with an institutional bias against classification. This sensitivity to classification, coupled with the independent status of the Screening Board, protects both legitimate national security concerns and the public’s need to be informed about the operation of the government.

This proposed scheme also imposes subsequent punishment upon those who knowingly publish or communicate Protected Information to another. Several policy reasons support including the media within the scope of the statute. The first, of course, is to ensure that the statute reaches all the actors in the chain of disclosure. The media is capable of disseminating sensitive information on the widest possible scale. To deter the actor most capable of causing a great deal of harm, the statute should reach those who knowingly publish leaked Protected Information. Additionally, not including the publisher within the proposed statute would render the statute much less effective: if one is unable to ascertain the identity of the leaker, any deterrent value in such a statute would be minimal. To obtain a credible deterrent, therefore, those who publish leaked information must be within the ambit of the proposed legislation.

Although proponents of an absolutist reading of the first amendment would argue that such a scheme violates the first amendment guarantees, this is not the case. The government can subject the press to criminal punishment, provided it meets proper standards.261 Because national security information is quite different from that ordinarily regulated and because the statute is narrowly drawn and requires a showing of significant harm from unauthorized disclosure, it likely passes constitutional muster.

The statute’s culpability standards require that a publisher know of the

261 See supra notes 180-91 and accompanying text.
protected status of the information before he can be convicted. Such a standard ensures that the statute reaches only those publishers on notice of the harm which disclosure could produce. Thus, the proposed legislation is narrowly drawn to reach only the publisher who knowingly disseminates Protected Information.

This scheme will place a greater administrative burden on the government if it wishes to protect secrets with criminal penalties. Sending material to the CSA for screening will potentially cause delays in the operation of agencies, added expense in the protection of secrets, and possibly even a wider exposure of confidential material. The added deterrence gained from criminal penalties, however, would most likely make the additional burdens well worth the cost.

First, important government secrets receive an additional level of protection—one that provides more deterrence than already existing administrative and civil sanctions. The deterrence gained from criminal penalties should make vital secrets far more secure from unauthorized disclosure. Second, only a limited class of information will be protected—information falling into specified categories and whose disclosure will seriously harm national security. The administrative burden placed on executive agencies to comply with this limited system will therefore be minimal. An agency need not send material to the CSA for protected status if it perceives that the added burden will outweigh any incremental protection.

The proposed system, then, not only solves problems generated by the unauthorized disclosure of classified information but does so within a framework that adequately protects first amendment interests. Stripped to its essence, a congressionally established screening agency, prescribing those secrets for which leaking is a crime, best mediates the conflicting goals of secrecy in national security and first amendment or open government values. Although the government obtains greater protection of certain secrets, it does so at an administrative price. This price means that the public’s interest in open government does not suffer from the availability of criminal punishment for unauthorized leaks of legitimate secrets.

IV. CONCLUSION

Unauthorized disclosures of classified information have occurred with increasing frequency. These disclosures are very often harmful to the national security of the United States. Yet, the government does not have a principled or comprehensive system for preventing either leaks or publication of classified information. The first amendment does not bar the postpublication punishment of those who leak or those who publish government secrets that result in serious damage to the national security. The executive classification system, however, is an inadequate basis for
invoking criminal penalties.

Thus, Congress should provide a comprehensive solution to the problem. Congress should create an independent agency that determines what information merits protection by criminal penalties. Finally, Congress should also penalize both those who leak and those who publish such information without authorization. Only in this manner may the conflicting goals of national security and the first amendment be adequately resolved.

E.E.B.
K.E.M.