The Constitutionality of the Intelligence Identities Protection Act

On June 23, 1982, President Reagan signed into law[1] the Intelligence Identities Protection Act of 1982 (the Act),[2] making criminal the disclosure of the identities of United States foreign intelligence operatives. Enactment of this legislation reflects heightened concern within the United States intelligence community over the exposure of foreign agents, which can threaten agents' personal safety and the effectiveness of intelligence activities. Despite this compelling interest in safeguarding the vitality of American intelligence efforts, the Act raises critical first amendment issues regarding the government's power to punish the divulgence of national security information.

This Note evaluates the constitutionality of the Act in light of first amendment principles. After describing the Act's criminal provisions, the Note analyzes recent Supreme Court decisions in the area of disclosure of confidential government information and national security information. Observing that the Court has delineated narrow yet significant areas of virtually unprotected disclosure, but has set extremely high standards of review in the areas outside the unprotected sphere, the Note applies these principles to the Act. The Note concludes that two sections of the Act, if narrowly construed, avoid constitutional difficulties. The third section, however, cannot be narrowly construed to avoid application to disclosure of properly classified information, lawfully obtained from the public domain by persons without autho-

---

1. Remarks on Signing H.R. 4 Into Law, 18 Weekly Comp. Pres. Doc. 829 (June 23, 1982).
2. Pub. L. No. 97-200, 1982 U.S. Code Cong. & Ad. News (96 Stat.) 122, amending the National Security Act of 1947 (to be codified at 50 U.S.C. §§ 421-26).

The Act's substantive provisions are as follows:

> Sec. 601. (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 identity 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.
>
> (c) Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classi-

rized access to classified information, and consequently violates the first amendment.

I. Protection of Intelligence Identities

A. *Background*

In recent years, disclosures of the classified identities of those intelligence officers, agents, and sources located abroad[3] have created mounting concern within the United States intelligence community. This concern is particularly directed at the editors of certain books (*Dirty Work* "1" and "2")[4] and periodicals (*Counterspy* and *Covertaction Information Bulletin*).[5] In these publications, the editors have purported to identify foreign intelligence operatives in order to expose and nullify covert political intervention in the affairs of other countries.[6] On at least two occasions, violent attacks on United States agents have followed public reports of their identities.[7] Moreover, the Central Intelligence Agency (CIA) attributes a continuing decrease in the effectiveness of United States intelligence activities to agent identity disclosures.[8]

---

fied intelligence relationship to the United States, shall be fined not more than $15,000 or imprisoned not more than three years, or both.

3. See generally 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. 13–56 (1981) (statements of W. Casey, R. Willard, J. Warner et al.) [hereinafter cited as House Hearings]; Intelligence Identities Protection Act of 1981—S.391: Hearing before the Subcomm. on Security and Terrorism of the Senate Comm. on the Judiciary, 97th Cong., 1st Sess. 26–70 (1981) (statements of W. Casey, J. Stein, F. Hits, and R. Willard) [hereinafter cited as Senate Hearings].

4. 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). See S. Rep. No. 201, 97th Cong., 1st Sess. 7–8 (1981) [hereinafter cited as Senate Report].

5. See House Hearings, supra note 3, at 1 (statement of Rep. Mazzoli).

6. See Agee, Introduction: Where Myths Lead to Murder, *in* Dirty Work, supra note 4, at 17–20; Proposals to Criminalize Unauthorized Disclosures, Hearings before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence, 96th Cong., 2d Sess. 112 (1980) (statement of W. Schaap, editor, CovertAction Information Bulletin) [hereinafter cited as Proposals]. In response to the passage of the Act, then pending in Congress, the editors of *CovertAction Information Bulletin* announced in March 1982 that the periodical would discontinue its practice of disclosing identities until the Act's constitutionality was tested in court. N.Y. Times, Mar. 13, 1982, at 11, col. 1.

7. In 1975 Richard Welch was identified as CIA Station Chief in Athens by the editors of *Counterspy* magazine and was murdered a month later. See Senate Report, supra note 4, at 8. The editors denied responsibility for his (or any other) murder. See Proposals, supra note 6, at 113. In 1980 an American Embassy official in Jamaica was the target of an assassination attempt two days after the editors of *CovertAction Information Bulletin* alleged he was one of a number of CIA officers stationed at the Embassy and, at a news conference, revealed the names, addresses, telephone numbers, and automobile information of these officers. Senate Report, supra note 4, at 8; see also H.R. Rep. No. 221, 97th Cong., 1st Sess. 4–5 (1981) [hereinafter cited as House Report].

8. House Hearings, supra note 3, at 13–14 (statement of W. Casey, Director of the Central Intelligence Agency). The assertion has been disputed by intelligence observers. See Franck & Eisen, Balancing National Security and Free Speech, 14 N.Y.U. J. Int'l L. & Pol. 339, 353–54 (1982).

Existing legal sanctions cannot deter these disclosures.[9] Relevant provisions of the espionage statutes,[10] which prohibit the communication of information relating to the national defense, apparently do not apply to the publication of such information;[11] nor has any court specifically upheld the validity of a prosecution under the theft-of-government-property statute[12] where the "property" is national security information.[13] Thus, no prosecutions have been attempted. The government has not sought a prior restraint against these disclosures, probably because such a restraint would be difficult to justify in the absence of a statute specifically prohibiting the disclosures.[14]

B. *The Intelligence Identities Protection Act of 1982*

The Intelligence Identities Protection Act was enacted by the 97th Congress in response to the perceived threat to national security posed by intelligence revelations.[15] The Act prohibits disclosures by three classes of individ-

---

9. The present Department of Justice takes the position that disclosures may be prosecuted under existing statutes but that certain problems with the scope of the statutes, see infra text accompanying note 11, and difficulties of proof preclude their effectiveness. House Hearings, supra note 3, at 28 (statement of R. Willard, Counsel to the Attorney General for Intelligence Policy).

10. 18 U.S.C. § 793(d), (e) (1976). The espionage statutes are codified at 18 U.S.C. §§ 793–798 (1976).

11. See Edgar & Schmidt, The Espionage Statutes and Publication of Defense Information, 73 Colum. L. Rev. 929 (1973).

12. 18 U.S.C. § 641 (1976).

13. In the two reported national security cases in which this statute was the basis of a prosecution, the defendant was convicted under the espionage statutes, see supra note 10, as well, and the courts of appeal declined to review the validity of the § 641 conviction because of the concurrent-sentence doctrine. United States v. Truong Dinh Hung, 629 F.2d 908, 922 (4th Cir. 1980), cert. denied, 454 U.S. 1144 (1982); United States v. Boyce, 594 F.2d 1246, 1252 (9th Cir.), cert. denied, 444 U.S. 855 (1979). The Fourth Circuit suggested, in dictum, that national defense information is not "government property" within the meaning of § 641. *Truong Dinh Hung*, 629 F.2d at 924–29. See generally Nimmer, National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case, 26 Stan. L. Rev. 311, 315–24 (1974).

14. See New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam) (vacating prior restraint not based on statute prohibiting disclosure). In concurring opinions, two Justices suggested that they might uphold a prior restraint if there were a statute specifically authorizing such a proceeding. Id. at 732–34, 740 (White, J., concurring); id. at 746–47 (Marshall, J., concurring). Two other Justices, also concurring, suggested a willingness to uphold a prior restraint if there were at least a statute barring the publication. Id. at 720–22 (Douglas, J., concurring); id. at 718–19 (Black, J., concurring).

15. Pub. L. No. 97-200, 1982 U.S. Code Cong. & Ad. News (96 Stat.) 122, amending the National Security Act of 1947 (to be codified at 50 U.S.C. §§ 421–26).

The Act is a direct descendant of several bills that were introduced in the 96th Congress to criminalize disclosures of intelligence identities. H.R. 5615, 96th Cong., 1st Sess. (1979); S. 2216, 96th Cong., 1st Sess. (1979); S. 2284, 96th Cong., 2d Sess. (1980). The bills died in the crush of pre-adjournment legislation. N.Y. Times, April 8, 1981, at A14, col. 1. For a history and a critique of these bills, as to both constitutionality and functionality, see Note, "Naming Names": Unauthorized Disclosure of Intelligence Agents' Identities, 33 Stan. L. Rev. 693 (1981). The Stanford Note, in a brief discussion of the first amendment interests at stake, comes to the general conclusion that a statute prohibiting intelligence identity disclosures could be constitutional, but argues that prior restraints may be preferable less restrictive means. Id. at 706–09. In contrast, this Note undertakes an extensive first amendment analysis

uals, mandating fines and imprisonment penalties[16] for the violation of its provisions.[17] There is no provision for the use of injunctions or other restraining orders[18] to suppress disclosures.[19]

1. *Disclosure by Government "Insiders."* The Act distinguishes between persons who have had authorized access[20] to classified information (insiders) and those who have not had such access (outsiders).[21] Sections 601(a) and (b) define the offense as committed by insiders, with a further distinction between a person who has had access to classified information "that identifies a covert agent"[22] and one who learns a covert identity "as a result of having had access to classified information" in general.[23] Persons subject to these sections are

---

Because of the line of descent of the Act, see House Report, supra note 7, at 10–11; Senate Report, supra note 4, at 1–5, this Note occasionally cites the legislative history of the 96th Congress legislation.

16. Section 601(a) imposes a fine of not more than $50,000 or imprisonment for not more than ten years, or both; § 601(b), $25,000 and/or five years' imprisonment; § 601(c), $15,000 and/or three years. The reason for the declining penalties is the relatively lesser degree of trust required of defendants in succeeding categories, and the concomitantly lesser breach of the trust. House Report, supra note 7, at 12; Senate Report, supra note 4, at 18.

17. The other provisions of the Act delineate defenses (§ 602), create extraterritorial jurisdiction (§ 604), prohibit the implication of authority to withhold information from Congress (§ 605), and define various terms (§ 606).

18. The House rejected an amendment to the Act providing for injunctive relief. 127 Cong. Rec. H6534 (daily ed. Sept. 23, 1981). Opponents of the amendment cited their fear of such relief being held unlawful because of the extra constitutional scrutiny applied to prior restraints. Id. at H6533-34 (statement of Rep. Mazzoli); id. at H6534 (statement of Rep. McClory).

19. The Act may well provide a basis for the imposition of a prior restraint. See supra note 14 and accompanying text. A discussion of the possible basis and limitations of a prior restraint based on the Act is beyond the scope of this Note.

20. "Authorized" is defined in § 606(2) to mean:

> having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

21. The terms "insider" and "outsider" are borrowed from Comment, First Amendment Standards for Subsequent Punishment of Dissemination of Confidential Government Information, 68 Calif. L. Rev. 83, 84 n.6 (1980).

22. Section 601(a). "Covert agent" is defined in § 606(4):

> (A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency—(i) whose identity as such an officer, employee, or member is classified information, and (ii) who is serving outside the United States or has within the last five years served outside the United States; or (B) a United States citizen whose intelligence relationship to the United States is classified information, and—(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or (ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or (C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

Identification must be accurate. See House Report, supra note 7, at 13; Senate Report, supra note 4, at 18.

23. This distinction is not material in the context of this Note. See infra text accompanying note 117.

primarily government employees, who, as a rule, have agreed with the government not to reveal classified information.[24]

Both sections prohibit the intentional disclosure[25] of "any information identifying such covert agent" when the disclosure is made "to any individual not authorized to receive classified information," if the discloser "know[s] 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." The identity of an agent must be classified information, but the information disclosed need not be, as long as it identifies an agent.

2. *Disclosure by "Outsiders."* Section 601(c) defines the offense with respect to persons who do not fall within sections 601(a) and (b), i.e., anyone who has not had "authorized access to classified information." Like sections 601(a) and (b), section 601(c) requires that the discloser intentionally reveal identifying information, knowing that he is identifying an agent whose identity the United States is trying to conceal. Unlike sections 601(a) and (b), however, the section requires that the revelation be made "in the course of a pattern of activities intended to identify and expose covert agents . . . with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States." While it remains unsaid, section 601(c) implicitly covers two means of access: (i) lawful access, whether gained by obtaining access to such information as is in the public domain or by receiving information from an "insider,"[26] and (ii) unlawful access, gained by breaking some law in the process.[27]

II. Constitutional Standards for Punishing Disclosure of National Security Information

The constitutionality of the Intelligence Identities Protection Act under the first amendment will depend on the protection that that amendment affords national security speech—the communication of information classified for national security purposes.[28] Applicable Supreme Court precedent

---

24. House Report, supra note 7, at 6–7. Although many such agreements are formal, in United States v. Snepp, 444 U.S. 507, 510 (1980), the Supreme Court said that such agreements may be implied from the position of trust such persons occupy in the government. See infra notes 109–10 and accompanying text.

25. Section 606(3) defines "disclose" to mean "communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available." It thus specifically deals with one problem of using the espionage statutes in this area, the uncertainty whether they cover publication. See supra note 11 and accompanying text.

26. A further distinction exists between information that exists as an identification (e.g., "Deputy Ambassador X is really the CIA Station Chief") and that which exists as an identification only after one deduces it (e.g., in source A, "In Togo, only CIA employees are permitted to wear brown suits"; in source B, "Deputy Ambassador X is the only U.S. government employee in Togo who wears a brown suit").

27. The law violated must be one that otherwise would have prevented access. See infra note 81 and accompanying text.

28. Sections 601(a) & (b) of the Act contain the element of access to "classified information," and §§ 601(a)–(c) contain the element of disclosing the identity of a "covert agent," which

suggests that some national security speech is beyond the scope of the first amendment while other national security speech does benefit from first amendment protection. Speech in the former category may be regulated in any manner that the government finds appropriate. Speech in the latter category is also regulable, but only in limited circumstances.

A. *Unprotected Communication of National Security Information*

Certain forms of communication of national security information receive no first amendment protection. Such communication falls into two categories: speech by certain government insiders and speech whose content and context except it from the doctrine of prior restraint. Communication falling within these categories may be prohibited and punished by statute.

1. *Speech by Insiders—The* Snepp *Principle.* The first amendment does not protect classified information divulged by government employees whose positions involve such a high degree of trust that a fiduciary duty exists. In *Snepp v. United States*,[29] the Supreme Court upheld a standard prepublication review requirement imposed by agreement on a former CIA employee. That agreement required the employee to submit for review all material to be published relating to the CIA, regardless of whether the material was classified.[30] Another part of the agreement, not challenged in the case, prohibited

---

is defined by § 606(4) to mean a person whose identity as an agent is "classified information." Section 606(1) defines classified information as that designated as such "pursuant to the provisions of a statute or Executive order."

It is not obvious on the face of the Act that what is being punished is the disclosure of classified information, since it in terms refers only to information that "identifies" a covert agent. This Note assumes that the proper construction of the statute is narrow, so that it does regulate "national security speech" as here defined. See infra text accompanying notes 121–23 & 131.

Information is classified pursuant to the National Security Act, 50 U.S.C. §§ 401–406 (1976), by Executive order. The current order requires that "Top Secret" classification, the highest grade, be based on a decision by authorized officials that "unauthorized disclosure . . . reasonably could be expected to cause exceptionally grave damage to the national security," Exec. Order No. 12,356, § 1.1(a)(1), 47 Fed. Reg. 14,874 (1982). Information may be classified as "secret" if unauthorized disclosure reasonably could be expected to cause "serious" damage, id. § 1.1(a)(2); or "confidential," if unauthorized disclosure reasonably could be expected to cause "damage," id. § 1.1(a)(3). Doubts are resolved in favor of classification and in favor of the higher level, pending final determination. Id. § 1.1(c). The effect of classification is to restrict unauthorized access to such material. Id. § 4.1.

29. 444 U.S. 507 (1980) (per curiam).

30. All persons with access to "sensitive compartmented [classified] information" must sign similar secrecy agreements; all persons with access to classified information must sign nondisclosure agreements (without prepublication review). Presidential Directive on Safeguarding National Security Information, Dep't of Justice release, Mar. 11, 1983. The agreements are worded to comply with *Snepp*. See N.Y. Times, Mar. 12, 1983, at A1, col. 3. Besides the CIA, several other federal agencies specifically require employees to sign similar secrecy agreements. See 22 C.F.R. § 10.735-303(b) (1982) (Department of State); 28 C.F.R. § 45.735-12(c) (1982) (Department of Justice); see also statement of Lloyd E. Dean, Federal Bureau of Investigation, April 16, 1980, statement of Daniel C. Schwartz, National Security Agency, April 16, 1980, and statement of George A. Zacharias, Defense Intelligence Agency, March 16, 1980, before the Oversight Committee of the House Permanent Select Committee on Intelligence. See generally the survey of policies of government agencies in Prepublication Review and Secrecy Requirements Imposed upon Federal Employees, Hearing before the Subcomm. on Civil and Constitutional Rights of the House Judiciary Comm., 96th Cong., 2d Sess. 59–73 (1980).

him from disclosing classified information without authorization.[31] The Court acknowledged the government's "compelling interest" in protecting both the secrecy of information important to national security and the appearance of confidentiality essential to effective intelligence activities.[32] Without inquiring at length into the scope of first amendment protection,[33] the Court found that the agreement signed by the defendant created a "trust relationship," which included an "obligation not to publish *any* information relating to the Agency without submitting the information for clearance."[34] Such an obligation was found to be a reasonable means of serving the government's interest.[35] The majority, moreover, did not rely on the contractual relationship alone. Speaking more broadly, they indicated that the defendant's status as an employee and his access to confidential materials might also establish such a "trust relationship" and concomitant fiduciary duty.[36] Thus, while in other circumstances an employee's speech "might be protected by the First Amendment," his fiduciary status precludes such protection.[37]

This holding is narrower than might appear on first impression. While the employee may be restrained from and punished for publishing any material relating to intelligence activities unless he complies with the review imposed by agreement, when he does comply with this review the government may only prohibit the employee's unauthorized disclosure of properly classified information. The prohibition must be limited to properly classified information because in the case of unclassified or improperly classified information the government's interest in suppression is not compelling. Authority to classify is broad, encompassing information whose unauthorized disclosure "could" be expected to cause damage to the national security;[38] thus there is no tenable argument for suppression of unclassified or improperly classified information on the ground of potential harm to national security. In *Snepp*, the government apparently recognized the force of this argument, since it did not argue for so broad a standard.[39] Indeed, the Court noted that neither the govern-

---

31. The CIA reviews submitted material in order to determine whether publication would compromise classified information or sources. *Snepp*, 444 U.S. at 511.

32. Id. at 509 n.3.

33. The Court did not advance a particular rationale, but merely stated in a footnote that the CIA could protect certain government interests by imposing reasonable restrictions on speech "that in other contexts might be protected by the First Amendment." Id. Thus the Court essentially assumed a stance of extreme deference: as long as a restriction is a "reasonable means" of advancing the compelling interest in national security, it is permissible.

34. Id. at 510–11.

35. Id. at 509 n.3. See supra note 33.

36. Id. at 509 n.3, 511 n.6.

37. Id. at 509 n.3.

38. See supra note 28.

39. See Medow, The First Amendment and the Secrecy State: *Snepp v. United States*, 130 U. Pa. L. Rev. 775 (1982); Comment, *Snepp v. United States:* The CIA Secrecy Agreement and the First Amendment, 81 Colum. L. Rev. 662 (1981).

The only circuit court to consider this issue adopted substantially these arguments. Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir.), cert. denied, 421 U.S. 992 (1975).

ment nor foreign agencies would be concerned with unclassified or public domain information: since that information is available elsewhere, the government has no interest in ensuring that it not be published.[40] The Court drew from its finding that Snepp "violated his obligation to submit *all* material for prepublication review," the conclusion that Snepp "exposed the classified information with which he had been entrusted to the risk of disclosure."[41] Thus the insider's fiduciary obligation is only to protect classified information.

In addition, although *Snepp* does not so hold, "properly classified" must be limited to the classification of information relating to activities that are not themselves illegal. There is a strong first amendment interest in encouraging insiders who know of such illegal activities to make these activities public. Insiders may be the only persons who are able to obtain or interpret information on these activities, and the government cannot be said to have a legitimate interest in keeping them secret.[42]

2. *Speech Unprotected Because of Content and Context.* Communication with certain content also may be deemed unprotected. Prior restraints against expression are ordinarily disfavored; they carry a "heavy presumption against [their] constitutional validity,"[43] a presumption to which subsequent punishment schemes are not subject. The 1931 case of *Near v. Minnesota*[44] established this doctrine within first amendment law. But at the same time, in dictum, the *Near* Court stated that prior restraints are not disfavored in "exceptional cases."[45] Among these are the prevention in wartime of "actual obstruction to [the government's] recruiting service or the publication of the sailing dates of transports or the number and location of troops."[46]

Though the *Near* "troopship" exception applies by its terms only to prior restraints, the exception logically applies to subsequent punishment schemes as well. In the hierarchy of speech-regulation methods, prior restraints occupy the lowest position.[47] Thus, if a prior restraint would be allowed in a particu-

40. 444 U.S. at 513 n.8.

41. Id. at 511 (emphasis added).

42. At the very least, such a limitation would be consistent with the first amendment interest in preventing, through free discussion, official breaches of the public trust. See New York Times Co. v. Sullivan, 376 U.S. 254, 274–75 (1964); see also Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 838–39 (1978); Mills v. Alabama, 384 U.S. 214, 219 (1966). See generally Blasi, The Checking Value in First Amendment Theory, 1977 Am. B. Fnd. Rsch. J. 521. The current classification order prohibits information from being classified to conceal violations of law. Exec. order No. 2, 356, § 1.6(a), 47 Fed. Reg. 14,874 (1982).

For a discussion of the legal limits on activity of intelligence agencies, see infra note 99.

43. Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963).

44. 283 U.S. 697 (1931).

45. Id. at 716.

46. Id. (footnote omitted). Also included are obscenity, incitement to violence or overthrow of the government, and fighting words (see also the discussion of fighting words infra note 57 and accompanying text).

47. The hierarchy is expressed through the technique of burdening prior restraints with a presumption against validity, see supra text accompanying note 45, which subsequent punishments do not share even though subsequent punishment schemes may themselves be subjected to rigorous tests of first amendment validity. See Smith v. Daily Mail Publishing Co., 443 U.S. 97, 102 (1979). This distinction is drawn because prior restraints are thought to be more restrictive in their impact on protected speech than are subsequent punishments. E.g., A. Bickel, The Morality of Consent 61 (1975) ("A criminal statute chills, prior restraint freezes."); Emerson, The Doc-

lar situation, a subsequent punishment would, a fortiori, be permissible.[48] Indeed, the Supreme Court has implicitly adopted this position: in a recent case it cited the *Near* exception in passing on a subsequent punishment in the form of a passport revocation statute.[49]

The *Near* "troopship" exceptions define expression that, because of both its content (i.e., obstruction of recruiting, or disclosure of sailing dates) and its context (i.e., wartime) may be restrained. The original formulation was expressed in terms of a category of speech that "no one would question" could be restrained in advance.[50]

The more recent case of *Haig v. Agee*[51] affirms the viability of the *Near* exception,[52] and, moreover, expands the range of content and context factors

---

trine of Prior Restraint, 20 L. & Contemp. Prob. 648, 655–60 (1955). This differential impact may not always bear out in practice, see *Smith*, 443 U.S. at 101 ("respondents acknowledge that the statutory provision for court approval of disclosure actually may have a less oppressive effect on freedom of the press than a total ban on the publication"); nor is the theory without its critics, e.g., Litwack, The Doctrine of Prior Restraint, 12 Harv. C.R.-C.L. L. Rev. 519 (1977); Mayton, Toward a Theory of First Amendment Process: Injunctions of Speech, Subsequent Punishment, and the Costs of the Prior Restraint Doctrine, 67 Corn. L. Rev. 245 (1982); Murphy, The Prior Restraint Doctrine in the Supreme Court: A Reevaluation, 51 Notre Dame Law. 898 (1976). See also infra note 48.

48. The only reason a subsequent punishment might not be permissible would be that the reasons permitting a particular prior restraint were inapplicable to a subsequent punishment statute. In general, all restraints on expression have the broad goal of preventing particular communication; prior restraints and subsequent punishment both aim to accomplish this goal through deterrence of the expression. Prior restraints accomplish deterrence by judicial or administrative restraint imposed prior to expression; subsequent punishment schemes, like all penal statutes, deter by the in terrorem nature of the punishment embodied in the statute. While no method relying on deterrence can ever be fully effective, prior restraints are deemed more likely to be effective. Because the greater likelihood of effective enforcement carries a greater threat to the exercise of first amendment rights, prior restraints are normally more difficult to sustain than are subsequent punishments. See supra note 47. If a prior restraint is upheld, it is because the court considers the expression sufficiently dangerous to warrant the risk of deterring protected speech, such as speech involving risk to national security. United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir. 1979). Even in *Progressive*, though, the government rested its claim of an overriding interest on its statutory authority under the Atomic Energy Act, 42 U.S.C. § 2274 (1976), to punish disclosure of the relevant information. 467 F. Supp. at 991.

If deterrence is the goal, and the risks are high enough to warrant a prior restraint, the government should be required to provide some notice to potential speakers that their speech is disfavored; such notice should be embodied in a statute punishing disclosure. See supra note 14 and accompanying text. Furthermore, since subsequent punishment statutes are more efficient, cf. Mayton, supra note 47, at 253–54 (lower transaction costs than prior restraints), and more likely to survive, given the disfavor of prior restraints, deterrence could more easily be accomplished by such statutes. There is, then, no reason to reverse or erase the traditional hierarchy in the national security situation.

49. Haig v. Agee, 453 U.S. 280, 308 (1981). See infra text accompanying notes 51–54.

50. 283 U.S. at 716.

51. 453 U.S. 280 (1981).

52. *Agee* does alter the character of the *Near* exception in one important manner. Although the *Near* exception was framed in terms of wartime considerations, the *Near* "troopship" exceptions are, according to *Agee*, not limited to wartime. In *Agee* the Supreme Court stated that "[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. Indeed, in *Agee* the Court cited the "troopship" exceptions in upholding a speech restraint imposed in peacetime, without commenting on this expansive application. Id.

that define it. Under *Agee*, the speaker's purpose, knowledge, and conduct are indicators of what may be termed per se unprotected speech.

In *Agee*, the United States revoked the passport of former CIA agent Phillip Agee on the ground that his prior and continuing disclosures of the identities of intelligence agents posed a threat to national security. The Supreme Court held that revocation of the passport was not an unconstitutional abridgment of Agee's first amendment rights. First, the Court stated that revocation "rests in part on the content of [Agee's] speech: specifically, his repeated disclosures of intelligence operations and names of intelligence personnel"; it then quoted the *Near* troopship exception language, and concluded, using language that closely echoed that of the *Near* Court,[53] that the disclosures were "not protected."[54] Implicit in the Court's reliance on *Near* is the notion that when speech falls within the literal terms of *Near*, or very close to them, there is no need to balance competing interests[55] in order to determine whether it is protected. *Agee*, then, defines a core of expression that is categorically unprotected, and leaves open the possibility that other analogous speech may be deemed to fall within this core category.

Because *Agee* places the disclosure of intelligence identities within the core of the *Near* exception, it is important for the purposes of this Note to define the limits of the *Agee* holding. The mere fact that speech discloses[56] intelligence identities does not mean that the speech is unprotected. Unlike the old "fighting words" category, the content of the speech is not determinative of the issue.[57]

First, the purpose of the speech in question is also relevant in determining whether or not the speech falls within the core. In declaring Agee's disclosures "clearly not protected," the Court said, "among other things, [the disclosures] have the *declared purpose* of obstructing intelligence operations and the recruiting of intelligence personnel."[58] The relevance of the purpose factor is not immediately apparent, but may be read as an indicator of the likelihood of the occurrence of the feared effect—in this case the obstruction of intelligence activities.[59]

---

53. "Agee's disclosures, among other things, have the declared purpose of obstructing intelligence operations and the recruiting of intelligence personnel." Id. at 308–09.

54. Id. Note that the speech restraint in *Agee* was the functional equivalent of a subsequent punishment scheme. For the implications of this, see supra text accompanying notes 47–49.

55. To determine the efficacy of a prior restraint on expression not subject to the *Near* exceptions (and otherwise not unprotected), the court must "determine whether . . . 'the gravity of the "evil," discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger.'" Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 562 (1976) (quoting United States v. Dennis, 183 F.2d 201, 212 (2d Cir. 1950) (L. Hand, J.)).

56. Note that the Court referred to Agee's *repeated* disclosures. 453 U.S. at 284.

57. The "fighting words" category was brought into first amendment law in Chaplinsky v. New Hampshire, 315 U.S. 568 (1942), and focused solely on the content of the expression. That narrow approach, however, is obsolescent; the Court's approach now has some contextual elements. L. Tribe, American Constitutional Law 617–23 (1978); see Cohen v. California, 403 U.S. 15 (1971).

58. 453 U.S. at 308–09 (emphasis added).

59. In this context, purpose does not serve the usual function of a mens rea, which is to provide a moral component of the punished activity, compare, e.g., J. Hall, General Principles of

In addition, the breadth of the *Agee* holding is limited by Agee's status as an intelligence "insider." In cases involving the disclosure of confidential information, the Court generally distinguishes between persons with authorized access to the confidential information (insiders)[60] and persons without such access (outsiders).[61] In *Agee* this distinction makes sense because the "insider" element, like the purpose factor, increases the likelihood that the obstruction will occur. Insiders are more likely to possess the requisite intention to obstruct; their knowledge of the intelligence area decreases the chance that they would disclose harmful information recklessly or negligently. Also, insiders are more likely to know what information would be most harmful.[62] Agee's insider status, however, was not in itself crucial. His status was important because it provided him with knowledge regarding the significance of the disclosed information. Thus, an outsider's possession of the same knowledge would be an equally good correlative of the likelihood that obstruction would occur. This use of Agee's insider status distinguishes *Haig v. Agee* from *Snepp*, where the insider status was itself crucial.[63]

Finally, one must examine the relevance of Agee's conduct to the decision. In earlier cases,[64] the Court refused to uphold passport revocations predicated on the holders' purported danger to the national security, when the only manifestations of this danger were speech, beliefs, or association. By

---

Criminal Law 133–41 (2d ed. 1960). This is clear from the way in which the court considered purpose in deciding the first amendment issue: in its inquiry the focus was on the effect of the expression the government sought to suppress rather than on the moral culpability of the actor. Agee conceded that his activities "were causing or were likely to cause serious damage to the national security" for the purpose of challenging the facial validity of the revocation regulation. 453 U.S. at 287 & nn.10 & 11. The Secretary of State had made the determination of "serious damage." Since the Court held that "the Government's interpretation of the terms 'serious damage' and 'national security' shows proper regard for constitutional rights and is precisely in accord with our holdings on the subject," id. at 309 n.61, the Court must have assumed that "serious damage" is here equivalent to the "actual obstruction" referred to in *Near*. See supra note 46 and accompanying text. It therefore held that "when there is a '*substantial likelihood*' of 'serious damage' to national security," as there was here, the government may act against a passport holder. Id. at 309 (emphasis added).

Of course, purpose alone is insufficient to cause the obstruction; it must be coupled with speech capable of causing obstruction in order to be the object of sanctions.

60. See supra text accompanying notes 29–42.

61. See infra text accompanying notes 71–90.

62. But this knowledge may not be as great as the employer's: the agency may have a broader understanding of what could cause harm, because it has access to more information. See Snepp v. United States, 444 U.S. 507, 512 (1980).

63. The Court did not rely on the *Snepp* principle in deciding *Agee*, even though Agee acknowledged that the disclosures violated his secrecy agreement; it noted instead that measures to enforce the agreement would be useless outside the United States. *Agee*, 453 U.S. at 308 n.60. Generally speaking, enforcement of an insider's fiduciary obligation would be limited to an injunction for specific performance of his contract obligations, if any contract exists, or the imposition of a constructive trust to remedy breach of his fiduciary obligations. See Medow, supra note 39, at 788 (summary of possible enforcement procedures). (Tort remedies may also be available. See Note, Breach of Confidence: An Emerging Tort, 82 Colum. L. Rev. 1426 (1982).) Furthermore, punishing an insider would require a statute authorizing punishment. Thus, the Court cited Agee's purpose and conduct in addition to his insider status. Moreover, the passport revocation order did not refer explicitly to his status. 453 U.S. at 286.

64. Aptheker v. Secretary of State, 378 U.S. 500 (1964); Kent v. Dulles, 357 U.S. 116 (1958).

contrast, the revocation of Agee's passport was predicated on his entire campaign to fight the CIA, of which "[b]eliefs and speech [were] only part."[65] The balance of the campaign consisted of conduct. Thus, the government alleged, and Agee conceded for the purposes of the litigation, that the campaign as a whole was causing or was likely to cause serious damage to national security.[66] Furthermore, the government never alleged that Agee's speech alone was damaging, nor did it base the passport revocation on this speech alone. Rather, the government referred to Agee's activities in foreign countries carried out with the intention to disrupt intelligence operations and his intention to continue these activities. The Court recognized the significance of Agee's conduct by holding that the passport revocation was a permissible burden on Agee's freedom to travel, and stating that restricting his travel, "although perhaps not certain to prevent all of Agee's harmful activities, is the only avenue open to the Government to limit these activities."[67] Restricting his travel could have virtually no effect on Agee's ability to disclose intelligence identities.

The Court's focus on Agee's conduct may be explained in one of two ways. Conduct may be necessary to show the likelihood of obstruction of intelligence operations. Or conduct could be evidence of an intention to obstruct (which, as is shown above, is itself a correlative of the likelihood of obstruction). At any rate, conduct is, according to *Agee*, an indicator of per se unprotected speech.

Assuming that conduct is a relevant consideration, the question becomes what conduct is relevant. *Agee* is not clear on this issue; the Court did not identify which of the activities comprising Agee's "campaign" were endangering the national security. The Court's description of the "campaign" consisted solely of the facts conceded for litigation.[68] These facts include the recruitment and training of collaborators; repeated and public disclosures of the identities of CIA agents, employees, and sources; Agee's violation of his secrecy agreement with the CIA; prejudice to the United States; and violence following disclosures.[69] From this it is unclear whether the conduct consists of all these factors, some of them, or some of them only in conjunction with each other. The Court is clear only on the point that the campaign must pose a serious danger to national security.

In sum, *Agee* outlines a set of indicators of per se unprotected national security speech: purpose, insider knowledge, and conduct. When some combination of these indicators is present there is no need to balance interests. *Agee* does not, however, make clear what combination of these indicators is neces-

---

65. *Agee*, 453 U.S. at 305.
66. See supra note 59.
67. 453 U.S. at 308.
68. Id at 306 & n.58.
69. Id. at 283-86 & nn.1-8.

sary. *Agee* clearly holds only that the combination of all three factors is sufficient to find disclosures per se unprotected.[70]

B. *Punishing Protected Disclosures of Confidential Information*

National security speech is a specific type of disclosure of confidential information.[71] When this type of disclosure is made by an insider or when the content and context of the disclosure except it from the doctrine of prior restraint, the disclosure receives no first amendment protection. When a disclosure does not fall into these unprotected categories, some test must be employed to evaluate the permissible scope of regulation of the disclosure. The test logically applicable to this problem is the constitutional analysis that has been developed to deal with the general problem of punishing disclosures of confidential information. The Supreme Court has articulated a balancing approach to the review of statutes punishing such disclosures by persons who either do not have authorized access to the disclosed information or who are not immediately privy to it.[72]

1. *Lawful Access by Third Parties to Confidential Information.* The Supreme Court held in *Landmark Communications v. Virginia*[73] that a statute

---

70. *Agee* must be reconciled with the analysis in New York Times Co. v. United States, 403 U.S. 713 (1971), the only Supreme Court case to pass on the constitutionality of a prior restraint sought on national security grounds. The Court held unconstitutional a restraint on the publication of a classified document (the "Pentagon Papers"). The test used to review the restraint was a definitional one, reflecting the principles implicit in the *Near* exception: "[O]nly governmental allegation and proof that publication will 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). "[D]isclosure . . . [must] surely result in direct, immediate, and irreparable damage to our Nation or its people." Id. at 730 (Stewart, J., concurring). The opinions of Justices Brennan and Stewart, being the narrowest of the five concurrences to the per curiam holding, must be considered the holding of the case.

The *Agee* Court did not mention *New York Times* when it applied *Near* to Agee's disclosures. It might be argued that the Court should have explicitly tested the disclosures under the definitional test instead of focusing on whether factors were present that indicated the likelihood that speech would cause obstruction of intelligence activities. The implication of such an argument is that, because *New York Times* requires actual proof of the likelihood of significant harm, *Agee* cuts back on the scope of the applicability of *New York Times*. See *Agee*, 453 U.S. at 321 n.10 (Brennan, J., dissenting).

The analysis outlined in this Note, however, renders this argument unnecessary. The doctrinal significance of *Agee*'s applying *Near* while failing to attach significance to *New York Times* lies in its explicit recognition that speech falling within the *Near* exception is unprotected for all purposes. These factors, showing likelihood of harm, obviate the need to *prove* harm. This per se rule can coexist with *New York Times*: if *Agee* factors are not present, the speech is not per se unprotected, but that is not the end of the analysis. The nature of the speech regulation determines the course of analysis. In the prior restraint area, the *New York Times* test would then be applied, requiring proof of harm. *Agee* neither expressly nor implicitly obviates the necessity for such proof when per se factors are absent. See also infra text accompanying notes 92-94 for a discussion of the relevance of *New York Times* to the subsequent punishment of national security speech.

71. For a definition of national security speech, see supra text accompanying note 28.

72. As outlined above, see supra notes 29–42 and accompanying text, when national security disclosures are made by insiders the speech is unprotected.

73. 435 U.S. 829 (1978).

that imposes criminal sanctions on disclosure of information regarding confidential judicial proceedings unconstitutionally abridges first amendment rights. In *Landmark*, the Court overturned a newspaper's conviction for divulging accurate information. Although the state had a legitimate interest in the confidentiality of these proceedings such that it might lawfully inhibit access to them, once a speaker had lawfully obtained information pertaining to these proceedings the state's interest was outweighed by the encroachment on freedom of expression.

The Court reached this result by balancing the interests of the state and the speaker. It held that in this context a court cannot defer to a legislative judgment, but must "make its own inquiry into the imminence and magnitude of the danger said to flow from the particular utterance and then . . . balance the character of the evil, as well as its likelihood, against the need for free and unfettered expression."[74] In this balancing process, rights of expression are given great weight: the standard used to balance is that " 'the substantive evil must be extremely serious and the degree of imminence extremely high before utterances can be punished.' . . . 'The danger must . . . immediately imperil.' "[75]

In addition, the Court stated that "[t]he possibility that other measures will serve the State's interests should also be weighed."[76] That is, the government must employ a less restrictive means of controlling dissemination.[77] Thus, it must, if feasible, control access to information by making it confidential, and must punish the breach of confidentiality by persons with authorized access; furthermore, it must control unauthorized access by "internal procedures."[78] The less-restrictive-means requirement permits the government to restrict initial access to confidential information to those immediately authorized to receive it, but prohibits the government from punishing disclosure by a third party who obtains the information.[79]

The information disclosed must, however, be lawfully acquired.[80] This limitation serves to ensure that the government, by its laws, controls access,

---

74. Id. at 843.

75. Id. at 845. Justice Stewart's concurrence included the formulation, "government may not prohibit or punish the publication of . . . information once it falls into the hands of the press, unless the need for secrecy is mainfestly overwhelming." Id. at 849 (footnote omitted).

76. Id. at 843.

77. See also Smith v. Daily Mail Publishing Co., 443 U.S. 97, 105 (1979).

78. *Landmark Communications*, 435 U.S. at 845 & n.13. Although this "internal procedures" requirement could be read to authorize the use of prior restraints on those insiders with authorized access, see Comment, supra note 21, at 88; cf. Snepp v. United States, 444 U.S. 507 (1980) (prepublication review procedure pursuant to valid secrecy agreement), the heavy disfavor of prior restraints, see supra notes 43–48 and accompanying text, means that a system of internally imposed controls on leakage would be much preferred. Cf. Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 563–65 (1976) (invalidating judicially imposed prior restraint on publication of certain information pertaining to trial: judge can control dissemination of information by measures short of prior restraint); id. at 601 n.27 (Brennan, J., concurring) (court has power to control release of information by court personnel).

79. For a critique of this distinction, see Comment, supra note 21.

80. Cf. Smith v. Daily Mail Publishing Co., 443 U.S. 97, 103 (1979) ("[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials

and relinquishes control where the reach of its law ends. Moreover, while a significant connection must exist between the law violated and the prevention of access to confidential information in order to punish disclosure of unlawfully acquired information,[81] the law need not be directed specifically at access. The government's less restrictive means of preventing disclosure should include all its lawful powers. For example, if confidential documents were kept on file in a locked room, and a person broke into the room unlawfully, looked at the information, and disclosed it, punishment would be warranted. The less restrictive means chosen by the government in this case is to lock a room, so if breaking open a locked door is unlawful, access is unlawful, even if the law is not directed specifically at preventing access to confidential information.[82]

2. *Information in the Public Domain.* Once information escapes into the public domain, the government effectively loses control over its dissemination. Regulation of the information can logically only be based on an interest other than preventing the public from gaining access to the information. Thus the state should not be able to restrain or penalize the dissemination of

---

may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."). This limitation seems to qualify a very broad statement made in the Court's opinion in Houchins v. KQED, Inc., 438 U.S. 1, 10 (1978): "The government cannot restrain communication of whatever information the media acquire—and which they elect to reveal."

81. For example, if a person drove through a red light on the way to gather information from a public library, it could hardly be said that access was unlawful.

82. Another definitional problem is whether initial unlawful access colors subsequent distribution of the information, so that a person could not disclose information obtained lawfully from a third person who had obtained it unlawfully. A variation of this question is whether unlawful disclosure by *A* to *B* is at the same time unlawful *access* by *B* from *A*. The problem could be solved by treating the information as akin to stolen property, so that its receipt would be unlawful in certain circumstances, such as where *B* knew *A* had had unlawful access. For a discussion of the problems such a concept raises, see generally Dennis, Leaked Information as Property: Vulnerability of the Press to Criminal Prosecution, 20 St. Louis U.L.J. 610 (1976). Cf. Nimmer, supra note 13, at 315–24 (use of 18 U.S.C. § 641 (1976), the theft-of-government-property statute, to punish removal of classified information by persons with authorized access, is unconstitutional). More generally, it could be argued that since disclosure of lawfully obtained information is allowed partially because it reflects a failure of the government adequately to restrict access, see supra text accompanying note 80, and since access to unlawfully obtained information does not reflect such a failure, the subsequent access is not "lawful" or at least not accorded the same treatment as lawfully acquired information.

Where initial disclosure by *A* is a violation of an insider's fiduciary obligation, *B*'s liability might be predicated on the theory that *B* participated in *A*'s breach. It would have to be determined whether *B*'s action completed the breach (since *A*'s breach makes confidentiality nonexistent, it is unlikely that one could find *B* to have completed any such breach), and whether *B* knew his action was a breach of trust. See G. G. Bogert & G. T. Bogert, The Law of Trusts and Trustees § 901 (rev. 2d ed. 1982).

Section 602(b) of the Act limits the reach of a prosecution for aiding and abetting, misprision of felony, or conspiracy. It requires that the "pattern" and "reason to believe" elements be satisfied as to a person prosecuted for these offenses. The legislative intent was to protect persons who receive disclosures made in violation of the Act. House Report, supra note 7, at 18; Senate Report, supra note 4, at 23. This provision does not fully answer the question, since conceivably a person could unlawfully obtain information and disclose it to a second person without violating the Act, and the second person could then disclose in arguable violation of the Act.

information obtained from sources available to the public, whether the information was affirmatively placed in the public domain[83] or not,[84] where the only asserted state interest is in maintaining the confidentiality of information.

But while the Supreme Court has never upheld a restriction on "disclosure" of public domain information, its language has been more circumspect when considering information that has come into the public domain despite or without the government's intervention than when the initial disclosure has come about by affirmative government action. In *Cox Broadcasting Corp. v. Cohn*,[85] for example, the Court held unconstitutional a statute punishing the disclosure of a rape victim's name where the name had been obtained from official court records. The state asserted an interest in protecting the victim's privacy. The Court did not engage in an explicit balancing process; rather it appeared to advance an estoppel argument. It stated that "the interests in privacy fade when the information involved already appears on the public record," and went on to say that "[b]y placing the information in the public domain . . . the State must be presumed to have concluded that the public interest was thereby being served. . . . If there are privacy interests to be protected . . . , the States must respond by means which avoid public documentation or other exposure of private information."[86] By comparison, in *Smith v. Daily Mail Publishing Co.*,[87] the Court employed a typical balancing-of-interests approach to strike down a statute prohibiting the publication of the identity of a juvenile participant in a court proceeding. In *Smith*, a newspaper obtained the identity of an accused juvenile offender by monitoring the police band frequency (a lawful activity) and questioning witnesses and a prosecutor. At least some of the information (the witness-provided portion) thus could be said to have reached the public domain without affirmative state action. The Court in fact stated that the way in which the information escaped "is not controlling" because "[a] free press cannot be made to rely solely

---

83. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975) (statute prohibiting publication or other disclosure of rape victim's name held invalid as applied to name obtained by reporter from indictments open to public scrutiny; information was obtained lawfully). Cf. Oklahoma Publishing Co. v. District Court, 430 U.S. 308 (1977) (invalidating pretrial order that prohibited publication of name of juvenile offender obtained at hearing that by law had to be closed but at which press was present and neither parties nor judge objected; information was obtained lawfully).

84. Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979) (statute prohibiting publication of name of offender held invalid; newspaper reporter obtained name by monitoring police radio and questioning witnesses).

85. 420 U.S. 469 (1975).

86. Id. at 494-95, 496. The Court further stated:

> Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business.

Id. at 495. Compare the implied consent rationale in United States v. Heine, 151 F.2d 813 (2d Cir. 1945) (L. Hand, J.), cert. denied, 328 U.S. 833 (1946), referred to infra notes 102-04 and accompanying text.

87. 443 U.S. 97 (1979).

upon the sufferance of government to supply it with information."[88] Nevertheless, the Court balanced the state's interest in protecting juvenile anonymity against the first amendment interest, rather than applying the estoppel argument of *Cox Broadcasting*. The Court decided that the state's interest was insufficient, noting that to be valid the statute must be "necessary"[89] to further the "highest form of state interest."[90]

The differing approaches of *Cox Broadcasting* and *Smith* may be read as an indication that in extraordinary circumstances the state may prevent the dissemination of public domain information. Considering the rationale underlying the cases, one can assume that if the state does not willingly make the information public, if the dissemination did not occur because the state failed to employ properly its less restrictive means, and if the initial disclosure was both minimal and containable, the interests of the state arguably outweigh those of the speaker.

C. *Is the Analysis of National Security Speech Different?*

Thus, although the Supreme Court has never directly addressed the question of the constitutionality of a statute punishing the disclosure of national security information,[91] there is an existing body of law that can be applied to statutes generally punishing disclosure of confidential information. Statutes punishing disclosure of national security information are a fortiori subject to this analysis, unless some reason compels a different treatment of national security speech. The relevant cases support a unified approach.

1. *The* New York Times *Standard.* While there is no body of case law dealing with the punishment of national security speech, the Supreme Court has set forth a standard for prior restraints in this area. In *New York Times Co. v. United States*,[92] the Court held that the first amendment prohibits a restriction on publication of classified national security information unless direct, immediate, and irreparable damage to the nation will inevitably follow.[93] The fact of classification, without more, is insufficient to prove such damage.

Although *New York Times* is a prior restraint case, the standard it sets forth logically should inform the selection of a standard applicable to the punishment of disclosure of national security information by outsiders. When the government controls access to information by classification, it sets up a mechanism whose effect is to prevent information from reaching the public—the same effect that a prior restraint has. With respect to those members of the

---

88. Id. at 103–04.
89. Id. at 104.
90. Id. at 102.
91. This is assuming that espionage statutes, which the Court has reviewed, see, e.g., Gorin v. United States, 312 U.S. 19 (1941) (vagueness challenge defeated), do not cover the disclosures, see supra text accompanying notes 10–16.
92. 403 U.S. 713 (1971).
93. See supra note 70.

public who obtain information despite the control, punishment for the disclosure of the information is analogous to punishment for ignoring a prior restraint.

This is not to say that the classification system is vulnerable to attack as a classic prior restraint. The system does not operate of its own force to prevent disclosure by outsiders. Rather, it operates by regulating disclosure to outsiders by agencies entrusted with sensitive information. Such disclosure is itself subject to the *Snepp* test, which validates the restraint. Thus the government may employ the system as a less restrictive means of keeping the information secret. There is a fundamental distinction, however, between regulating the national security speech of insiders through this less restrictive means, and regulating the speech of outsiders by the same means. Restricting public access clearly affects the *speech* interests of insiders, but not the *speech* interest of outsiders. It is thus not a classic prior restraint. Yet it partakes of the essential attributes of a prior restraint, i.e., the prevention in advance of the dissemination of information. If one acknowledges that the system has this effect without impinging on a *speaker's* interests, the logical implication is that the prior restraint analysis—The *New York Times* test—should apply to the punishment of a *speaker* when punishment is predicated on the application of that system to the speaker. The speaker cannot, however, challenge the operation of the system before it operates on his speech interests.

The substantive level of stringency embodied in the *New York Times* standard is substantially the same as that embodied in the *Landmark* standard for the punishment of the disclosure of confidential information. Both standards require a high degree of potential for immediate and extraordinary harm resulting from the disclosure.[94] Thus, the *Landmark* standard for the punishment of the disclosure of confidential information should also be applied to the punishment of the disclosure of national security information.

a. *Application to Lawfully Obtained National Security Information.* The *Landmark* balancing test requires a judge to speculate on the likelihood that significant harm will result from disclosure. In the case of the disclosure of national security information, requiring a court to speculate in this manner seems both an inordinate burden on the judge and an inaccurate method with which to test a statute's legitimacy. The validity of claims of harm to national security is inherently difficult to assess. A judge is unlikely to have experience in weighing the specialized factors involved in the decision.[95] Moreover, information necessary to make an accurate decision will likely be classified and

---

94. See supra text accompanying notes 74 & 75.

95. For example, the judge in United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir.1979), was asked to examine an article containing information on the operation of the hydrogen bomb and compare it with extremely technical information in the public domain in order to decide whether publication would "increase thermonuclear proliferation" and harm the national security. The court, while acknowledging that to write the article one needed sufficient expertise, considered itself up to the task of comparing the information.

thus unavailable to a judge.[96] In subsequent punishment cases, however, this problem can be effectively remedied by requiring proof that significant harm was actually caused by disclosure.[97] Mere proof of classification is not sufficient proof of significant harm, as *New York Times* held.[98]

The significant harm demonstrated must, however, affect a legitimate government interest. Absent such a requirement the government would be able to punish individuals for disclosures that revealed illegal government activity.[99]

b. *Application to Unlawfully Obtained National Security Information.* Where a statute punishes the disclosure of unlawfully obtained classified information, the government's interest should prevail and the statute be held constitutional. The less restrictive means of preventing disclosure of confidential information is through internal procedures designed to prevent information from escaping.[100] To allow disclosure after unlawful access nullifies the

---

96. Cf. the Classified Information Procedures Act, 18 U.S.C. App. (Supp. V 1981), which was enacted to deal with the problems that arise when criminal prosecutions require the government or defendant to disclose classified information in order to present a satisfactory case ("graymail" tactics). The Act provides for hearings to determine whether and how such information shall be disclosed.

97. One commentator has stated:

> Taken together, [*Cox Broadcasting v. Cohn*, *Smith v. Daily Mail Publishing Co.*, *Landmark Communications v. Virginia*, *Nebraska Press Ass'n v. Stuart*, and *New York Times Co. v. United States*] leave little doubt that, except in cases involving imminent national military catastrophe, the Court will not permit previous restraints upon, or subsequent punishment for, publication in a mass medium of accurate information that the publisher has lawfully acquired.

Cox, The Supreme Court, 1979 Term—Foreword: Freedom of Expression in the Burger Court, 94 Harv. L. Rev. 1, 17 (1980). Cox's limitation to "mass medium" seems unnecessarily cautious: the public interest can be served just as adequately by disclosure to individuals in a position to exert political influence as by dissemination to the public in general.

98. Since information may be classified by agents of the Executive, and may be classified upon a decision that "damage" may result, see supra note 28, the classification standard itself is insufficient proof of harm under the *New York Times* standard. See Comment, supra note 39, at 690 n.185.

99. The activities of the government in the intelligence area are limited by Executive order pursuant to 50 U.S.C. § 401 (1976) (congressional declaration of purpose to provide comprehensive national security program). Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981). In addition to circumscribing the authority of the various agencies affected, the order provides that the conduct of intelligence activities is to be carried out "consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded." Id. § 2.1; see also id. § 2.8 ("Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.").

Instances of reporting on the abuses of authority by the agencies with authority to classify are well known. See generally T. Powers, The Man Who Kept the Secrets 271-308 (1979). These reports clearly advance the first amendment checking interest, see supra note 42.

100. See supra notes 77-79 and accompanying text. A variety of such means are open to the government and are now being employed: These include physical barriers such as locked doors and windows; punishment of employees for failing to lock up documents; and compartmentalization of knowledge. T. Powers, supra note 99, at 66. Employees who have access to classified information may be subject to polygraph examinations. Presidential Directive on Safeguarding National Security Information, supra note 30. Some agencies construct elaborate systems to guard against disclosure and impose administrative sanctions on employees who violate the rules. See, e.g., 32 C.F.R. § 159.141 (1982) (Department of Defense) (sanctions for knowing, willful, unauthorized disclosure range from "warning notice" to "removal or discharge").

government's less restrictive means of controlling information availability. Thus, in contrast with the lawful-access situation, conditioning the right to disclose information gained unlawfully upon subsequent proof of significant harm would inadequately serve the government's interest in preventing such harm by restricting initial public access. Therefore, the public's interest in free expression extends only to the boundaries imposed by an otherwise valid law; if there is a sufficient connection between the law violated and the government's right to control access to classified information, disclosure may be punished.

2. *Public Domain National Security Information.* As indicated above, the state is generally not able to punish the dissemination of confidential information already in the public domain.[101] Once information escapes into the public domain, the government effectively loses control over it and can no longer assert an interest in preventing public access.

Courts have divided over the question of the scope of first amendment protection for public domain national security information. The Second Circuit held in *United States v. Heine*[102] that the espionage statutes cannot be construed to permit punishment of the dissemination of information gathered from "sources that were lawfully accessible to anyone who was willing to take the pains to find, sift and collate it."[103] The decision was not expressly based on the first amendment, but constitutional considerations entered into it: "so drastic a repression of the free exchange of information it is wise carefully to scrutinize, lest extravagant and absurd consequences result."[104] In *Alfred A. Knopf, Inc. v. Colby*,[105] where the court focused specifically on first amendment concerns, the Fourth Circuit indicated in dictum that it was in agreement with this position. The court stated that while insiders may not republish classified information in the public domain,[106] outsiders may.[107]

A district court reached a contrary conclusion in *United States v. Progressive, Inc.*[108] and imposed a preliminary injunction based on the Atomic

---

101. See supra notes 83–89 and accompanying text.

102. 151 F.2d 813 (2d Cir. 1945) (L. Hand, J.), cert. denied, 328 U.S. 833 (1946).

103. Id. at 815. *Heine*'s rationale was a theory of implied consent by the military services: "The services must be trusted to determine what information may be broadcast without prejudice to the 'national defense,' and their consent to its dissemination is as much evidenced by what they do not seek to suppress, as by what they utter." Id. at 816. Compare the rationale used by the Supreme Court in Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975), discussed supra note 86 and accompanying text.

104. 151 F.2d at 815.

105. 509 F.2d 1362 (4th Cir.), cert. denied, 421 U.S. 992 (1975).

106. Id. at 1370.

107. Id. (dictum).

108. 467 F. Supp. 990 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir. 1979). Cf. also Gros v. United States, 138 F.2d 261 (9th Cir. 1943) (upholding espionage conviction, challenged on other grounds, for dissemination of defense information apparently gleaned from newspaper clippings); United States v. Enger, 472 F. Supp. 490 (D.N.J. 1978) (not an essential element of an offense, such that it must be alleged in indictment under espionage statutes, 18 U.S.C. §§ 793 & 794 (1976), that information be of a secret, nonpublic nature).

Energy Act[109] against publication of classified information on the hydrogen bomb that had been gathered by a magazine reporter from both inadvertently declassified data and information in public sources. The court reasoned that a prior restraint was valid, by analogy to the *Near* exceptions, because even though some information was in the public domain, it took a certain amount of expertise to draw correct conclusions. Thus publication would, on the one hand, allow other nations more quickly to develop the bomb, while, on the other, would not significantly advance the public interest.[110]

The position set forth in *Heine* and *Knopf* is the more persuasive. The concerns that underlie the prohibition on the punishment of outsiders for the dissemination of confidential information in the public domain apply with even more force in the case of public domain national security information. *Smith* and *Cox Broadcasting* were based on the argument that once information is in the public domain the government no longer has a legitimate interest in regulating dissemination. This reasoning is particularly applicable to national security information. Intelligence agencies have become so numerous and so sophisticated that any disclosure of confidential information is likely to be detected and exploited immediately.[111] Moreover, the first persons to obtain disclosed information are likely to be precisely those from whom the government is most interested in keeping the information. Thus, after even minimal initial disclosure, the government's legitimate interest[112] in regulating dissemination declines precipitously. From the government's point of view, little can be gained from inhibiting additional dissemination.

Furthermore, in cases where the government affirmatively or negligently places the information in the public domain,[113] it may be argued that the government has failed to employ its less restrictive means of maintaining confidentiality.[114] In the national security area, the government possesses

---

109. The relevant portions are 42 U.S.C. §§ 2274 & 2280 (1976), which, respectively, prohibit disclosure of certain data and authorize the enjoining of such disclosures.

110. Information in the article was published elsewhere while appeal was pending, whereupon the government withdrew its request for an injunction, and *The Progressive* published its material. For a history of the case, see Comment, A Journalist's View of *The Progressive* Case, 41 Ohio St. L.J. 1165, 1166–74 (1980).

111. See L.F. Prouty, The Secret Team 293–94 (1973).

112. The government might assert an interest in preventing the wider domestic public from obtaining information so that it might conceal illegal activities or prevent public policy discussion when secrecy is not necessary to maintain national security, cf. M. Halperin & D. Hoffman, Top Secret 31 (1977) (secrecy of covert operations of questionable legality and/or public support); this would clearly not constitute a legitimate interest. See Hill, Defamation and Privacy Under the First Amendment, 76 Colum. L. Rev. 1205, 1295 (1976). Nor is it now a legitimate ground for classification. Exec. order No. 12,356, § 1.6(a), 47 Fed. Reg. 14,874 (1982).

113. Outside observers blame CIA carelessness for the fact that intelligence identity information may be obtained by those without authorized access to it. N.Y. Times, Feb. 6, 1981, at A10, col. 6. But the CIA argues that since the information is publicly available, and since ex-employees are willing to help others find it, internal procedures instituted now would be worthless. See House Hearings, supra note 3, at 24 (statement of CIA Director William Casey).

114. Cf. New York Times Co. v. United States, 403 U.S. 713, 728–29 (1971) (Stewart, J., concurring) ("The responsibility must be where the power is. If the Constitution gives the Executive a large degree of unshared power in the conduct of foreign affairs and the maintenance of our national defense, then under the Constitution the Executive must have the largely unshared

special powers designed to allow it to control the dissemination of information.[115] When the government fails to employ these powers effectively, and the information is disclosed, it should be estopped from punishing further dissemination of the information by outsiders.[116]

III. Constitutionality of the Act

Different kinds of disclosures warrant different levels of first amendment protection. The Act itself is divided into two conceptual categories: disclosures by intelligence insiders and disclosures by the public at large.

A. *Sections 601(a) and (b): Punishment of "Insiders"*

Sections 601(a) and (b) are nearly identical, and differ from (c), in that both define the offense with respect to persons who have had "authorized access to classified information"—insiders. Because such persons have a relationship of trust with the government, their release of classified information—whether or not actually obtained during the course of authorized access—is unprotected by the first amendment. Thus, while sections 601(a) and (b) distinguish between insiders who have had access to classified information identifying a covert agent, and insiders who learn the identity as a result of having had general access to classified information, the distinction is immaterial to the scope of protection accorded expression. A statute may constitutionally punish any insider who divulges any properly classified information.[117]

Construed narrowly,[118] the Act operates within these bounds. Section 606(1) defines "classified information" to mean material "designated [as such] . . . pursuant to the provisions of a statute or Executive order." On its face, this does not require that the information be properly classified. Improper classification, however, is simply that which is not authorized by the

---

duty to determine and preserve the degree of internal security necessary to exercise that power successfully." (footnote omitted)).

115. Based on its foreign affairs power, the Executive branch of the government has special authority to regulate national security information. See New York Times Co. v. United States, 403 U.S. 713, 727–28 (1971) (Stewart, J., concurring); Chicago & S. Air Lines v. Waterman Corp., 333 U.S. 103, 111 (1948); United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936). See also Haig v. Agee, 453 U.S. 280, 307 (1981) (national security is the most compelling governmental interest, and measures to protect secrecy of intelligence operations plainly serve this interest).

116. Another argument, which would apply with equal force to non-national security information, is that if information is in the public domain, anyone repeating it has no notice that it is confidential. It would be manifestly unfair to burden the public with finding out whether information is confidential before repeating it. The unfairness is diminished if the repeater has actual knowledge that it is confidential.

117. "Properly classified" is here used as a term of art, the meaning of which is discussed supra text accompanying notes 39–41.

118. Narrow construction is required because if a limiting construction can be placed on a statute so as to remove its unconstitutional aspects, it will not be held invalid on its face. Broadrick v. Oklahoma, 413 U.S. 601, 613 (1973).

pertinent Executive order,[119] and if "pursuant to" is read to mean "as authorized by," the statute would require that the identity revealed be properly classified.[120] Furthermore, section 602(a) sets up as a defense that the government has "publicly acknowledged or revealed" the identity of an agent, so that if an identity is effectively declassified by official disclosure an insider may "disclose" it.

Neither section requires in terms that the actual information disclosed be classified, but only that it identify a covert agent, whose identity by definition[121] is classified.[122] A broad reading that mandated punishment for disclosure of unclassified information would arguably infringe protected expression. It makes more sense to characterize the section as punishing the disclosure of the classified identity itself. The connection between the information disclosed and the identity must therefore be narrowly confined. The Act does this by requiring that the individual know that the information identifies a covert agent. Furthermore, the legislative history indicates that the Act requires that the connection be direct and specific.[123] Thus, the insider is being punished for the effective disclosure of classified information learned through inside access. To this extent sections 601(a) and (b) are constitutional, since such expression is unprotected by the first amendment.

B. *Section 601(c): Punishment of "Outsiders"*

Section 601(c) differs from (a) and (b) in that it applies to individuals who do not have authorized access to classified information—outsiders.[124]

1. *Regulation of Per Se Unprotected Speech.* If section 601(c) can be said to regulate per se unprotected speech, it is constitutional. *Haig v. Agee* held that three factors indicate such speech: purpose, insider status or equivalent knowledge, and conduct.[125]

---

119. Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362, 1367 (4th Cir.), cert. denied, 421 U.S. 992 (1975). The *Knopf* holding was based on the exemption from disclosure requirements of the Freedom of Information Act, 5 U.S.C. § 552(b)(1) (1976), which applies to any information that is "in fact properly classified."

120. Legislative history supports this reading, albeit not unambiguously. The House Report, supra note 7, at 13, 20, 21, states that the identity disclosed must be "properly classified." The Senate Report, supra note 7, at 19, 24, 25, while otherwise tracking the House Report closely, leaves out the word "properly." On the other hand, it does not anywhere state that proper classification is *not* required. The dangers of reading too much into legislative silence militate against interpreting the Senate Report to support either interpretation. The Conference Report, H.R. Rep. No. 580, 97th Cong., 2d Sess. (1982), is of no help, but it does caution that "[t]he Committee of Conference expects the executive branch to exercise the utmost care in making classification decisions in this area," id. at 12, a tenor comporting with the interpretation above.

121. See supra note 22.

122. See House Report, supra note 7, at 13; Senate Report, supra note 4, at 19.

123. See House Report, supra note 7, at 13 (connection must be "direct, immediate, and obvious"); Senate Report, supra note 4, at 19 (connection must be "direct, and the information must point at a particular individual"). For instance, if the phone number, address, or automobile license number of a CIA station chief is not classified, but is disclosed so as to identify the chief, that is an offense. See House Report, supra note 7, at 13; Senate Report, supra note 4, at 19.

124. See supra text accompanying notes 26 & 27.

125. See supra text accompanying notes 56–70.

Presumably, an insider is subject to section 601(c), since by its terms it includes "any person." But since insiders can be prosecuted under sections 601(a) and (b), which require fewer elements of proof and impose harsher sanctions, and since the legislative intent of section 601(c) was clearly to reach outsiders,[126] it could be interpreted to exclude insiders from its coverage. In any case, section 601(c) does not require insider knowledge. Agee's insider position allowed him to acquire important knowledge about the significance of the information he was disclosing beyond the mere fact that it was classified. Section 601(c) does not require that the discloser have such knowledge, only that he know "that the information disclosed . . . identifies" a covert agent "and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship."

Furthermore, section 601(c) does not contain the requisite purpose element. Agee's "disclosures . . . ha[d] the declared purpose of obstructing intelligence operations."[127] Section 601(c) requires only that disclosures be made with "reason to believe that [his] activities would impair or impede the foreign intelligence activities of the United States."[128]

Arguably, section 601(c) does incorporate the third factor set forth in *Haig v. Agee*—conduct constituting a "campaign to fight the United States CIA."[129] The section specifically requires a "pattern of activities intended to identify and expose covert agents." This phrase, since it is broadly drawn, certainly describes Agee's conduct in a general sense, but it fails to define the essential characteristics of the "campaign," which involved repeated public exposures of identities intended to destroy CIA effectiveness by driving the agents out of foreign countries. Other activities, which can be distinguished from *Agee* on their facts, would fall within the "pattern" phrase—for example, a series of investigative articles in a newspaper that exposes illegal CIA infiltration of foreign governments. The legislative history, however, evinces an intent to exclude these kinds of activities, which are viewed as serving the public interest.[130] The statute can therefore be construed as requiring the highly specific conduct described in *Agee*.

---

126. The House Report, supra note 7, at 7, states that the "third . . . class of individuals affected by the bill are those who . . . never have held the position of trust which typifies members of the first and second class." The Senate Report, supra note 4, at 12, states that the "third . . . class of individuals . . . are those who . . . have never had authorized access to classified information with its accompanying duty of care."

127. Haig v. Agee, 453 U.S. 280, 309 (1981).

128. The legislative history of the Act clearly evinces a congressional purpose to attach a "reason to believe" standard rather than an "intent" standard, to the element of harm to intelligence activities, and to distinguish this from the intent to identify and expose agents that is attached to the "pattern" element. See Conference Report, supra note 120, at 7, 10. Whether to require "intent" to harm intelligence or "reason to believe" was the subject of extensive debate in Congress. See 128 Cong. Rec. S2352-58 (daily ed. Mar. 18, 1982); id. at S2281-95 (daily ed. Mar. 17, 1982); id. at S2118-36 (daily ed. Mar. 16, 1982); id. at S2070-85 (daily ed. Mar. 15, 1982); id. at S1230-40 (daily ed. Mar. 1, 1982); id. at S1164-83 (daily ed. Feb. 25, 1982); 127 Cong. Rec. H6504-40 (daily ed. Sept. 23, 1982). (The House version of the Act as reported from Committee, and the Senate version in the 1981 Congress as reported from Committee, both had an "intent" standard. See Conference Report, supra note 120, at 6.)

129. *Haig v. Agee*, 453 U.S. at 283.

130. Conference Report, supra note 120, at 8-10.

Thus, at best, section 601(c) incorporates only one of the three factors outlined in *Agee*. The section's coverage extends beyond the ambit of the per se unprotected speech defined in *Agee*. Consequently, analysis of its constitutionality must proceed with a balancing approach based on the assumption that prohibited disclosures are protected.

2. *Punishment where Information Obtained Unlawfully*. Where classified information is obtained unlawfully, a statute may, under the *Landmark* balancing test, constitutionally punish its disclosure. Section 601(c) is, by its terms, applicable to cases involving the disclosure of unlawfully obtained information. The section does not, however, explicitly require that the information disclosed be classified. Rather, like sections 601(a) and (b), it punishes the disclosure of "any information that identifies an individual as a covert agent," so long as the speaker knows he is thus revealing a classified identity. If, however, the information actually disclosed was obtained unlawfully, and the revelation of a classified identity is both knowing and significantly connected to the information obtained,[131] the individual is effectively disclosing classified information unlawfully obtained. So construed, section 601(c) is constitutional.[132]

3. *Punishment where Information Obtained Lawfully*. Section 601(c) also punishes the disclosure of lawfully obtained information. A statute cannot constitutionally punish disclosure of classified information obtained lawfully by an outsider without proof that significant harm—i.e., direct, immediate, and irreparable damage—to national security resulted from disclosure. The mere fact that the identity revealed is classified is insufficient. This, however, is all that section 601(c) requires; no proof of subsequent harm to national security is necessary under the section.[133] Section 601(c) could, however, be constitutionally applied if the element of classification were construed to require proof that the identity was in fact "properly classified," meaning that its disclosure would necessarily result in significant harm.[134]

Section 601(c) also fails to require explicitly that the information disclosed pertain to activities within the legal authority of the agency involved. Disclosures pertaining to illegal activities are protected by the first amend-

---

131. See supra note 123.

132. There is no legislative intent to support a contrary construction. Furthermore, since the broader legislative purpose was to prevent disclosure of intelligence identities, such a construction is not inconsistent with the purpose. Thus there is no obstacle to the narrowing construction. See, e.g., United States v. Thirty-Seven Photographs, 402 U.S. 363 (1971). Compare infra notes 139–42 and accompanying text.

133. Nor can it be argued that *Haig v. Agee* held that disclosure of intelligence identities must necessarily cause significant harm, since *Agee* was decided on a stipulated concession of resultant harm. See supra note 59 and accompanying text.

134. See supra note 120.

Given the current classification standards, which require at most that harm "could" result, see supra note 28, no disclosure would *necessarily* cause significant harm, so that no disclosure would be constitutionally punishable.

ment.[135] Thus, if the section is to survive constitutional scrutiny, it must be construed to exclude such disclosures.

4. *Public Domain Information.* Where the information obtained lawfully is in the public domain, a statute may not constitutionally punish its "disclosure." Section 601(c) does not require that the identity revealed be obtained from classified sources. The only qualification made is the section 602(a) defense that the United States has "publicly acknowledged or revealed" the identity at issue; the legislative history makes clear, however, that this defense does not apply where the United States has merely placed information in the public domain from which an identity may be deduced. Rather, it applies only where the United States has either specifically acknowledged an identity or made information public that leads directly to an identity.[136] Thus, on its face, section 601(c) punishes the disclosure of the identity of a covert agent when that identity is deduced entirely from sources in the public domain. Such an application is constitutionally prohibited.

A statute may not validly regulate unprotected activities if it does so by unnecessarily broad means that thereby affect protected activities.[137] "[T]he First Amendment needs breathing space," and therefore requires that statutes affecting rights of free expression "must be narrowly drawn and represent a considered legislative judgment that a particular mode of expression has to give way to other compelling needs of society."[138]

Unlike sections 601(a) and (b), section 601(c) cannot be given a narrowing construction to avoid this constitutional infirmity. Such a construction is ordinarily preferable to a finding of facial invalidity.[139] A court may not,

---

135. See supra text accompanying note 99. The narrowing construction is permissible, since there is no legislative history evidencing an inconsistent intent; indeed, the legislative history evidences a congressional intent to allow exposure of intelligence agents where intent was to expose illegal or controversial activities, Conference Report, supra note 120, at 10, and is consistent with the broad purpose of preventing harm to intelligence operations through disclosures. See supra note 132.

136. House Report, supra note 7, at 17–18; Senate Report, supra note 4, at 23. The House Report, at 18, further states, "An identification is not [subject to the defense] if it can be made only after an effort to seek out and compare, cross-reference, and collate information from several publications or sources." The Senate Report, at 23, uses nearly identical language. The aim of this language apparently is to exclude specifically from the defense those people who identify agents using the methods described by Agee, supra note 6, and in Marks, How to Spot a Spook, *in* Dirty Work, supra note 6, at 25, 31–35. These articles, written by ex-CIA employees, detail how classified intelligence identities may be deduced from public documents such as the State Department Biographic Register and the United States Foreign Service List. They also recommend using general common sense, e.g., "The Agency operative is taught early on in training that loud background sounds interfere with bugging. You can be pretty sure that the CIA man in the Embassy is the one who leaves his radio on all the time." Id. at 31. See also Intelligence Identities Protection Act, S. 2215, Hearing before the Senate Committee on the Judiciary, 96th Cong., 1st Sess. 42–45 (1980) (testimony of Deputy CIA Director F. Carlucci).

137. E.g., NAACP v. Alabama, 377 U.S. 288 (1964).

138. Broadrick v. Oklahoma, 413 U.S. 601, 611–12 (1973).

139. Arnett v. Kennedy, 416 U.S. 134, 162 (1974); United States v. Thirty-Seven Photographs, 402 U.S 363, 369 (1971). Where a state statute is measured against federal constitutional standards, only the state courts have jurisdiction to construe it authoritatively, Wainwright v. Stone, 414 U.S. 21, 22–23 (1973), but federal courts may decide whether the statute as so construed violates the Constitution. New York v. Ferber, 102 S. Ct. 3348, 3360 (1982).

however, construe a statute so as to avoid facial invalidity where such a construction is contrary to the legislative purpose.[140] To do so would constitute an invasion of Congress's lawmaking function. Thus, where a limiting construction would require that a court import into the statute elements or qualifications that Congress clearly intended not to include, the construction is impermissible.[141] The legislative history of section 601(c) clearly manifests an intention to include within its scope those disclosures based on public domain sources.[142] To construe the section so as to exclude such disclosures would thus be improper.

As the subject of an arguably overbroad statute moves from pure speech to conduct, its overbreadth must be more substantial to be fatal.[143] Section 601(c) does not regulate conduct, however, even though it requires proof of a "pattern of activities." The conduct element is defined in terms of an intent to "identify and expose covert agents." Identification and exposure are ultimately expressive actions; thus even to the extent it regulates conduct section 601(c) does so only as an incident to its regulation of speech by disclosure of identities. Finally, even if it does regulate conduct its overbroad applications are not an insubstantial portion of its prospective applications, given the magnitude of public domain information pertaining to the identity of covert agents.[144] Under these principles, section 601(c) is manifestly overbroad.

Conclusion

Anxiety over the effect of disclosures of intelligence identities on national security and the inability of current law to deal with this problem has led to the enactment of the Intelligence Identities Protection Act. While the Act validly punishes some kinds of disclosures, it also prohibits disclosures that cannot constitutionally be forbidden.

First, if they are to survive constitutional attack, sections 601(a) and (b) must be narrowly construed to apply only to intelligence identities that have been properly classified. Second, section 601(c) must be narrowly construed to

---

140. Blount v. Rizzi, 400 U.S. 410, 419 (1971); United States v. Robel, 389 U.S. 258, 267 (1967); see United States v. Reese, 92 U.S. 214, 221 (1875).

141. Blount v. Rizzi, 400 U.S. 410 (1971) (refusing to construe statute so as to incorporate constitutionally required procedures where legislative history showed congressional intent not to include such procedures); compare United States v. Thirty-Seven Photographs, 402 U.S. 363, 368–73 (1971) (distinguishing *Blount* where legislative history supports saving construction).

142. In its discussion of the "pattern of activities" requirement, the Conference Report states, "This pattern of activities must involve much more than merely restating that which is in the public domain. . . . Those who republish previous disclosures . . . would all stand beyond the reach of the law if they did not engage in [the requisite] pattern of activities . . . ." Conference Report, supra note 120, at 8–9. There was much testimony before Congress as to the constitutionality of such disclosures. See, e.g., House Hearings, supra note 3, at 29–30 (statement of R. Willard, Counsel to the Attorney General for Intelligence Policy); id. at 71–72 (statement of J. Berman & M. Halperin); id. at 104 (statement of F. Abrams); Proposals, supra note 6, at 29–32 (statement of R. Keoch, Assoc. Deputy Att'y Gen.); id. at 45–49, 56, 58 (statement of F. Abrams); id. at 76 (statement of J. Berman).

143. Broadrick v. Oklahoma, 413 U.S. 601, 611–12 (1973).

144. See supra note 136.

apply only to unlawfully obtained information and certain lawfully obtained information. Because such a narrow construction would be improper, however, section 601(c) is overbroad and therefore unconstitutional.

Concern about our national security must be tempered with a sense of the limits we voluntarily impose on our ability to authorize the creation of official secrets. The power to create secrets and the duty of keeping them are reposed in the Executive's intelligence agencies. Congress may not enact a law that unfairly burdens the populace with the duty of safekeeping while preserving the power in the government.

Susan D. Charkes