William & Mary Law Review

Volume 51 (2009-2010)
Issue 6

Article 7

5-1-2010

Blowing Its Cover: How the Intelligence Identities Protection Act Has Masqueraded as an Effective Law and Why It Must be Amended

Andrew M. Szilagyi

BLOWING ITS COVER: HOW THE INTELLIGENCE IDENTITIES PROTECTION ACT HAS MASQUERADED AS AN EFFECTIVE LAW AND WHY IT MUST BE AMENDED

TABLE OF CONTENTS

INTRODUCTION

Individuals engaged in clandestine intelligence collection are constantly placed in peril. The Central Intelligence Agency (CIA) refers to such covert officers as case officers.[1] The safety of case officers and the integrity of their work are dependent upon secrecy, especially with regard to their identities.[2] Concealment of case officers' identities not only allows them to operate covertly, but their confidence in the preservation of this information also provides them with the only sense of security they have in an otherwise dangerous, isolated, and uncertain life of public service.

In order to appreciate the importance of secrecy, the intelligence collection process must be fully understood. Intelligence agencies gather information by several methods, including the use of open, technological, and human intelligence sources.[3] Case officers typically engage in human intelligence (HUMINT) collection, which is

---

1. For purposes of this Note, the term "case officer" means any individual who is employed by the United States and clandestinely engaged in intelligence activities. Although the CIA is primarily responsible for human intelligence collection, other government agencies within the intelligence community may occasionally participate in such efforts. *See* MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 94 (3d ed. 2006). Subsequently, the term "case officer" is not exclusive to covert officers employed by the CIA. Given this definition, a "case officer" is necessarily included within the definition of a "covert agent"—the term used in federal statutory law. *See* Intelligence Identities Protection Act of 1982, 50 U.S.C. § 426(4) (2006) (including three groups of individuals within the definition of "covert agent": (1) specified current and retired employees of the intelligence community; (2) certain U.S. citizens whose intelligence relationships to the United States are classified; and (3) other individuals whose past or present intelligence relationships to the United States are classified as a result of their operational assistance to an intelligence agency as agents, informants, or sources, both past and present).

2. *See* ARTHUR S. HULNICK, FIXING THE SPY MACHINE: PREPARING AMERICAN INTELLIGENCE FOR THE TWENTY-FIRST CENTURY 30, 173 (1999) (explaining that secrecy, including the confidentiality of intelligence sources, is an essential element of espionage). The U.S. Supreme Court also declared that secrecy is implicit to the "integrity of the intelligence process." CIA v. Sims, 471 U.S. 159, 170 (1985). Without secrecy, the Court stated, the CIA would be "virtually impotent." *Id.* In further explaining this concept, the Court quoted President George Washington as writing that "'[t]he necessity of procuring good intelligence, is apparent and need not be further urged.... For upon secrecy, success depends in most Enterprises of the kind, and for want of it they are generally defeated.'" *Id.* at 172 n.16.

3. *See generally* LOWENTHAL, *supra* note 1, at 79-104 (providing an overview of the various intelligence collection methods).

also referred to as espionage or spying.[4] The HUMINT method involves clandestine surveillance and case officers' recruitment of "assets,"[5] including the use of foreign nationals to spy.[6] Because case officers must operate under a subterfuge, which provides them with plausible explanations for their presence within a foreign state,[7] secrecy is critical to their safety and the value of their work.

If a case officer's identity is compromised, then the result can have drastic effects on that officer's individual welfare.[8] A discovered case officer may be subjected to great personal and physical risk, particularly if that officer has a nonofficial cover.[9] Not only may the case officer be subjugated to adverse treatment, but those connected to that officer, including family and friends, may also be endangered.[10] Moreover, exposing a case officer's identity can negatively affect that officer's livelihood. Exposed case officers often lose their ability to operate clandestinely abroad, therefore denying that individual the opportunity to continue a career as a case officer.[11]

The unauthorized disclosure of a case officer's identity can also have significant national security implications, as it impedes the intelligence process and frustrates foreign diplomacy. These implications are illustrated by four possible consequences resulting from an unauthorized disclosure. First, the government must sacrifice both its investment in an exposed case officer and the experience,

---

4. *Id.* at 94.

5. For purposes of this Note, the term "asset" means any foreign national serving as an agent, informant, or source. An "agent" is a foreign national who engages in espionage by providing information to the United States that would otherwise be unobtainable.

6. *See* LOWENTHAL, *supra* note 1, at 94 (suggesting that most HUMINT efforts consist of case officers' recruitment of foreign agents); *see also* HULNICK, *supra* note 2, at 23.

7. LOWENTHAL, *supra* note 1, at 95 (explaining that case officers provided with official covers are perceived to hold other government positions, whereas officers with nonofficial covers are perceived to work and live in a nongovernmental capacity and avoid any display of an overt connection between themselves and their government).

8. *See* Meri West Maffet, Note, *Open Secrets: Protecting the Identity of the CIA's Intelligence Gatherers in a First Amendment Society*, 32 HASTINGS L.J. 1723, 1750 (1981).

9. LOWENTHAL, *supra* note 1, at 100.

10. *See infra* Part I.A (providing instances in which unauthorized disclosures of case officers' identities have resulted in attacks on the identified officers' homes).

11. *See infra* Part I.A.

knowledge, and ability that the officer possessed.[12] Second, similar to personal associations, an uncovered case officer's professional connections may be imperiled, which include coworkers and recruited assets.[13] Third, the effects of exposure may demoralize current case officers and reduce the future applicant pool by discouraging potential recruits from applying.[14] Finally, there is the possibility of significant political embarrassment to the government

---

12. Given the complex networking and intricate relationships inherent in intelligence collection, replacing a case officer is inefficient and costly. *See* discussion *infra* Part I.A. The time and expense applied to reestablishing intelligence networks can expose the United States to adverse repercussions that may have otherwise been avoided.

13. *See* Maffet, *supra* note 8 (citing Admiral Stansfield M. Turner, Dir. of Cent. Intelligence (DCI), Address to the San Francisco Press Club (Aug. 11, 1980)) (stating that exposure may reveal "the methods of recruitment and operation employed by the sponsoring agency, thereby facilitating the identification of additional operatives"). Both additional case officers and foreign nationals may be uncovered as part of the chain reaction of a single disclosure. Any known colleagues of an exposed officer may be jeopardized, in terms of both their physical safety and ability to conduct covert affairs. The effects of losing one case officer, therefore, are multiplied with the threat of additional personnel losses. In addition, foreign nationals whom the exposed officer recruited as assets may be discovered and executed for espionage against their respective governments. HULNICK, *supra* note 2, at 30. The possibility of impending death could deter past and future foreign nationals from continuing their intelligence relationship if they view the exposure as a breach of confidentiality and lose trust in the United States. *See* CIA v. Sims, 471 U.S. 159, 175 (1985); Snepp v. United States, 444 U.S. 507, 512 (1980) ("The continued availability of these foreign sources depends upon the CIA's ability to guarantee the security of information that might compromise them and even endanger the personal safety of foreign agents."). For example, reacting to the unauthorized disclosure of classified information, former DCI Stansfield M. Turner explained:

> [W]e have had a number of sources discontinue work with us.... [and] more ... tell us that they are very nervous about continuing work with us. We have had very strong complaints from a number of foreign intelligence services with whom we conduct liaison, who have questioned whether they should continue exchanging information with us, for fear it will not remain secret. I cannot estimate to you how many potential sources or liaison arrangements have never germinated because people were unwilling to enter into business with us.

Snepp, 444 U.S. at 512-13 (internal quotation marks omitted). This cascading effect, arising from a single disclosure, can plague intelligence collection by undermining other intelligence operations and destroying information networks.

14. Maffet, *supra* note 8, at 1750-51 (citing *Proposals To Criminalize the Unauthorized Disclosure of the Identities of Undercover United States Intelligence Officers and Agents: Hearings Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 96th Cong. 15 (1980) (statement of Frank C. Carlucci, Deputy Director of the CIA)); Admiral Stansfield M. Turner, DCI, Address to the San Francisco Press Club (Aug. 11, 1980) (explaining that, in addition to reducing the applicant pool, exposure may also prompt case officers to take fewer risks and "revert to more defensive, time consuming, and costly means of operation to avoid detection"); *see also* Halperin v. CIA, 629 F.2d 144, 149 (D.C. Cir. 1980).

that dispatches an uncovered case officer.[15] Because of the personal and national security implications identity exposure can have, case officers' identities remain secret.

Even with these cumulative threats arising from unauthorized disclosures, the U.S. intelligence apparatus remains the most transparent intelligence system in the world.[16] Throughout the history of the United States, however, there has been incessant controversy over the level of secrecy in the intelligence community.[17] Responsibility for safeguarding secrecy within the U.S. intelligence community is largely placed upon internal safeguards rather than codified law.[18] While the debate over secrecy continues, particularly regarding the prevention of unauthorized disclosures of classified information, there *is* a narrow class of information that Congress has affirmatively sought to protect—the identities of case officers. Although some U.S. presidents were importunate about the need to keep case officers' identities secret for years,[19] it was not until 1982 that Congress recognized the importance of such a measure, when it passed the Intelligence Identities Protection Act (IIPA).[20] The

---

15. *Halperin*, 629 F.2d at 148; LOWENTHAL, *supra* note 1, at 100; *see also* Maffet, *supra* note 8, at 1751 (offering a short discussion on how unauthorized exposures affect foreign relations).

16. HULNICK, *supra* note 2, at 3, 180; *see also Snepp*, 444 U.S. at 523 n.13 (referring to statements from former DCI William E. Colby that foreign states generally have a stricter secrecy code than the United States).

17. *See generally* STEPHEN F. KNOTT, SECRET AND SANCTIONED: COVERT OPERATIONS AND THE AMERICAN PRESIDENCY (1996) (providing a historical overview of the executive branch's struggle to maintain secrecy in the intelligence process).

18. *See* LOWENTHAL, *supra* note 1, at 204-05 (highlighting rules and regulations, such as the security clearance and classified information systems, which aim to ensure confidentiality in intelligence matters); *see also Sims*, 471 U.S. at 167 (citing the National Security Act of 1947, 50 U.S.C. § 403(d)(3)) ("Congress has made the Director of [National] Intelligence 'responsible for protecting intelligence sources and methods from unauthorized disclosure.'").

19. *See, e.g.*, KNOTT, *supra* note 17, at 125-26 (explaining that former presidents defended against efforts by Congress to reveal the identities of spies working on behalf of the United States). In arguing that information about covert activity was not privy to congressional inquiries, President James K. Polk stated that "'the situation of the country may make it necessary to employ individuals for the purpose of obtaining information or rendering other important services who could never be prevailed upon to act if they entertained the least apprehension that their names or their agency would in any contingency be divulged.'" *Id.*

20. The IIPA is codified under Title VI of the National Security Act of 1947. Intelligence Identities Protection Act of 1982, 50 U.S.C. §§ 421-426 (2006).

IIPA was specifically designed to outlaw the unauthorized disclosure of case officers' identities.

Despite its noble purpose and the need to protect case officers' identities, since its enactment, the IIPA has been rarely utilized and largely ineffective.[21] Its limited application is attributable to the uncovering of three factors that have plagued the IIPA throughout its over twenty-five year existence: (1) the availability of another, but equally insufficient, espionage-related statute; (2) the IIPA's inherent limitations; and (3) a lack of political initiative to enforce the IIPA.[22] The Valerie Plame Wilson affair is a glaring example of the IIPA's limited application.[23] Additionally, the Plame affair serves as a useful case study for illustrating two of the factors inhibiting the IIPA's application—namely, the law's inherent limitations and the lack of political will to enforce the law.[24] Upon analyzing the Plame affair and other instances in which the IIPA could have been applied, it is evident that, in order to effectively serve its purpose and avoid becoming completely defunct, the IIPA must be amended. This Note details the need for an immediate and comprehensive amendment to the IIPA, which will address the IIPA's three debilitating factors by expanding the class of protected persons and easing the narrowness of its offenses. Part I provides a brief background to the IIPA, including the historical events that motivated its enactment and an overview of its purpose and scope. Part II discusses the limited application of the IIPA, especially in the context of its intended purpose and scope, and the three factors inhibiting its enforcement. Part III provides policy justifications for amending the IIPA and suggests proposals to be included in an amendment—particularly, expanding the class of protected persons and easing the narrowness of its offenses. In the end, this Note concludes that the IIPA, if properly amended, can become a viable and valuable safety mechanism in preventing the unauthorized disclosure of case officers' identities. Such an amendment will add substance to a law that has been disguised as effective.

---

21. *See* discussion *infra* Part II.
22. *See infra* Part II.
23. *See* discussion *infra* Part II.B-C.
24. *See infra* Part II.B-C.

I. BACKGROUND TO THE IIPA

A. Historical Context

During the late 1970s and early 1980s, the systematic exposure of case officers' identities rattled the U.S. intelligence community. Numerous media exposures of clandestine operations prompted criticisms of the CIA for its involvement in what some believed to be questionable activities.[25] Soon, dissidents dedicated to the eradication of the CIA surfaced within the United States and abroad.[26] The movement became so pervasive that publications emerged, determined to undermine CIA operations. A former CIA case officer even authored and edited several of these publications.[27] Eventually, the intelligence community's worst fears regarding the unveiling of case officers' identities became reality.[28]

In 1975, three gunmen assassinated the CIA station chief for Greece, Richard S. Welch, outside of his Athens home.[29] Welch's murder came eighteen months following his exposure as a CIA case

---

25. *See* Robert W. Bivins, Note, *Silencing the Name Droppers: The Intelligence Identities Protection Act of 1982*, 36 U. FLA. L. REV. 841, 843 (1984) (referring to alleged CIA involvement in an attempted Chilean coup as an example of an uncovered covert operation that elicited public criticism).

26. *See id.*

27. Former CIA case officer Philip Agee founded and edited *CounterSpy*, a magazine published during the 1970s and 1980s, and *CovertAction Quarterly*, previously known as *CovertAction Information Bulletin*. "Writing in *CounterSpy*, Agee said that 'the most effective and important systematic efforts to combat the CIA that can be undertaken right now are, I think, the identification, exposure and neutralization of its people working abroad.'" *Kidnaping in Vienna, Murder in Athens*, TIME, Jan. 5, 1976, *available at* http://www.time.com/time/magazine/article/0,9171,947609,00.html. Agee also authored several books critical of the CIA, which listed the names of alleged case officers along with the location of their overseas assignments and their biographical information. *See generally* PHILIP AGEE, DIRTY WORK: THE CIA IN WESTERN EUROPE (Philip Agee & Louis Wolf eds., 1978); PHILIP AGEE, DIRTY WORK 2: THE CIA IN AFRICA (Ellen Ray et al. eds., 1979); PHILIP AGEE, INSIDE THE COMPANY: CIA DIARY (1975) [hereinafter AGEE, INSIDE THE COMPANY]. Agee's primary objective was the abolition of the CIA, and he viewed the exposure of covert officers as a means by which to accomplish this goal. *See* Haig v. Agee, 453 U.S. 280, 283-85 & n.2 (1981) (quoting a 1974 statement by Agee).

28. The framework for and much of the following information in this subsection was adapted from the extensive historical account compiled and described by Robert W. Bivins. *See generally* Bivins, *supra* note 25, at 843-45.

29. *Kidnaping in Vienna, Murder in Athens*, *supra* note 27.

officer in *CounterSpy* magazine.[30] Although *CounterSpy* editor Philip Agee denied that his actions resulted in Welch's murder,[31] the White House and the intelligence community contended that Agee's publication was indirectly responsible.[32]

In 1980, Louis Wolf, the editor of the *CovertAction Information Bulletin*, held a press conference to disclose the identities of fifteen purported CIA case officers working in the U.S. embassy in Kingston, Jamaica.[33] Wolf revealed the case officers' biographical information, home addresses, telephone numbers, and automobile descriptions, including license plate numbers.[34] He claimed that one of the named case officers, N. Richard Kinsman, was the CIA station chief for Jamaica.[35] Fewer than forty-eight hours following this press conference, Kinsman's home came under a barrage of machine gun fire and grenade attack.[36] Three days later, another unsuccessful assassination attempt was mounted against the home of one of the other identified case officers.[37] Because of these incidents, the

30. Scott Shane, *There Are Leaks. And Then There Are Leaks.*, N.Y. TIMES, Apr. 30, 2006, § 4, at 4.

31. *See* Fred Attewill, *Renegade CIA Agent Agee Dies*, GUARDIAN (London), Jan. 9, 2008, http://www.guardian.co.uk/world/2008/jan/09/cuba.usa1 (quoting Agee as contending that President George H.W. Bush "'came in as CIA director in the month after the assassination and he intensified the campaign, spreading the lie that I was the cause of the assassination'").

32. Bivins, *supra* note 25, at 844 (citing S. REP. NO. 97-201, at 7 (1981), *as reprinted in* 1982 U.S.C.C.A.N. 145, 151-52); *see also Haig*, 453 U.S. at 285 n.7 (quoting the former CIA Deputy Director for Operations, who, in speaking generally about Agee's actions, explained that the unauthorized disclosures were "'thinly-veiled invitations to violence'" that "'markedly increased the likelihood of individuals so identified being the victims of violence'"). *But see Bill To Penalize Uncovering of Agents Passed by Senate*, N.Y. TIMES, June 11, 1982, at A20 (explaining that others claimed that Welch's identity was already widely known, as he resided in a home typically occupied by senior CIA case officers).

33. Jo Thomas, *Gunmen in Jamaica Hit Home of U.S. Aide*, N.Y. TIMES, July 5, 1980, § 1, at 1.

34. *Id.*

35. Samuel T. Francis, *The Intelligence Identities Protection Act (S. 391, H.R. 4)*, HERITAGE FOUND., NAT'L SEC. & DEF. BULL., Nov. 1, 1981, at 1, 2, *available at* http://www.heritage.org/Research/NationalSecurity/IB70.cfm.

36. Thomas, *supra* note 33.

37. Francis, *supra* note 35, at 2; Bivins, *supra* note 25, at 844 (citing S. REP. NO. 97-201, at 8 (1981), *as reprinted in* 1982 U.S.C.C.A.N. 145, 152).

U.S. government was forced to remove all of the named case officers and their families from Jamaica.[38]

In 1981, the newspaper *Nuevo Diario*, a pro-Sandinista publication, identified thirteen CIA case officers stationed in the U.S. embassy in Managua, Nicaragua.[39] Some of these case officers received death threats and others were attacked in their homes.[40] The U.S. government officials in Managua insisted that there was a nexus between Agee's visit to Nicaragua and *Nuevo Diario*'s printing of the names.[41] Along with these unsuccessful assassination attempts, the same year also brought the murders of two Americans, Michael P. Hammer and Mark David Pearlman. Hammer and Pearlman were murdered in San Salvador after Agee accused their employer, the American Institute for Free Labor and Development (AIFLD), of being a CIA front organization for intelligence operations in El Salvador.[42]

In 1982, Cuban intelligence officials, along with the editors of the *CovertAction Information Bulletin*, visited Mozambique.[43] Coincidentally, following this visit, the Mozambique government expelled six Americans from its country on charges of espionage.[44]

These five incidents are only the most publicized examples—particularly because each was associated with either the infamous Agee or Wolf—of the results of unauthorized disclosures of case officers' identities. They exemplify the dangers threatening the lives of exposed case officers, their families, and those associated with the officers. It should be noted that these same threats also surround individuals *incorrectly* identified as case officers,[45] as those wishing to cause harm are unlikely to distinguish between exposures that are credible and those that are not.

---

38. Bivins, *supra* note 25, at 844 (citing S. REP. NO. 97-201, at 8 (1981), *as reprinted in* 1982 U.S.C.C.A.N. 145, 152).

39. *Id.* (citing 128 CONG. REC. S1168 (1982) (statement of Sen. Barry M. Goldwater)).

40. *Id.*

41. *Id.* (citing 128 CONG. REC. S1168 (1982) (statement of Sen. Barry M. Goldwater)).

42. Judith Miller, *Solicitor General Calls 2 Americans Killed in El Salvador 'Under Cover*,' N.Y. TIMES, Jan. 15, 1981, at A10.

43. Bivins, *supra* note 25, at 844-45 n.29.

44. *Id.*

45. *See* Francis, *supra* note 35 (indicating that some case officers are falsely identified, either by error or "deliberate fabrication").

The preceding events are also illustrative of the numerous, less dramatic effects that accompany identity exposure. For example, after a case officer is publicly identified, the value of that individual to covert operations is lost, as the officer can never operate in a clandestine position again.[46] The intelligence community must then replace the case officer, often at great difficulty and expense.[47] Moreover, the longstanding relationships and sources the case officer established must be reconstructed or abandoned.[48] Consequently, even when no physical harm ensues, the intelligence community and the exposed case officer's career may still be severely damaged.[49]

B. The Legislative Response

By the early 1980s, Agee and Wolf claimed to have revealed over three thousand intelligence-related identities combined.[50] These systematic exposures, aimed at destroying U.S. clandestine intelligence efforts, "preceded and may have contributed to circumstances resulting in the death or attempted assassination of some CIA officers, expulsion of others from a foreign country following charges of spying, and impairment of relations with foreign intelligence sources."[51] This conclusion to these dramatic circumstances prompted Congress to respond.

---

46. *Id.* at 3.

47. *See, e.g.*, Bivins, *supra* note 25, at 844 n.26 (citing S. REP. NO. 97-201, at 8 (1981), *as reprinted in* 1982 U.S.C.C.A.N. 145, 153) (stating that removing the exposed case officers from Jamaica, who were identified by Wolf, was costly and difficult).

48. Francis, *supra* note 35, at 3.

49. *Id.*; *see also* discussion *supra* text accompanying notes 8-15 (providing a more detailed discussion of the effects the unauthorized disclosure of a case officer's identity has on an individual and national security).

50. ELIZABETH B. BAZAN, CONG. RESEARCH SERV., LIBRARY OF CONG., CRS REPORT FOR CONGRESS: INTELLIGENCE IDENTITIES PROTECTION ACT 2 (2003), *available at* http://fas.org/irp/crs/RS21636.pdf (explaining that Agee revealed over one thousand intelligence-related identities and Wolf revealed over two thousand, primarily through the *CovertAction Information Bulletin* in a section entitled "Naming Names"). This number includes those Agee identified in a twenty-six page list contained within one of his books. AGEE, INSIDE THE COMPANY, *supra* note 27, at 599-624.

51. BAZAN, *supra* note 50.

Lawmakers realized that adequate legal redress was needed to prevent further exposures, given that there were no existing laws or regulations to prevent the activities in which Agee, Wolf, and others were engaged.[52] This provided the impetus for Congress to draft new legislation to address the problem directly. In 1982, after several years and many attempts to pass such a measure,[53] the House and Senate finally approved a bill that garnered overwhelming support.[54] Bipartisan support for the bill was reinforced with backing from both the Carter and Reagan administrations and the intelligence community.[55] On June 23, 1982, President Ronald W. Reagan signed the bill into law, thus establishing the Intelligence Identities Protection Act.[56]

C. An Overview of the Purpose and Scope of the IIPA

The IIPA criminalizes, under certain circumstances, the intentional unauthorized disclosure of a case officer's identity when that disclosure is accomplished by either directly naming an officer or providing information that leads to the exposure of an officer.[57] Not only does the IIPA protect the identities of case officers, but it also protects other individuals who are integral to HUMINT—specifically, foreign agents, informants, and sources.[58] These "assets" comprise the networks case officers establish while operating

---

52. *See* Bivins, *supra* note 25, at 845 (explaining that the National Security Act proved to be an inadequate remedy to situation). *See generally* Maffet, *supra* note 8, at 1725-49 (discussing how, before the enactment of the IIPA, there were no laws to protect directly against the unauthorized disclosure of case officers' identities, and those that were even remotely applicable suffered from serious deficiencies).

53. *See* James R. Ferguson, *Government Secrecy After the Cold War: The Role of Congress*, 34 B.C. L. REV. 451, 484 (1993) (explaining that there were fifteen attempts to pass legislation); Michael Wright & Caroline Rand Herron, *A Bid To Insure Secret Agents Stay That Way*, N.Y. TIMES, Sept. 27, 1981, § 4, at 2 (stating that discussion surrounding the legislation lasted for more than five years).

54. *See Bill To Penalize Uncovering of Agents Passed by Senate*, *supra* note 32. The Senate passed S. 391 with a vote of 81 to 4 and the House of Representatives passed H.R. 4 with a vote of 315 to 32. *Id.*

55. Francis, *supra* note 35, at 4-5.

56. *See* Intelligence Identities Protection Act of 1982, Remarks on Signing H.R. 4 Into Law, 18 WEEKLY COMP. PRES. DOC. 829 (June 23, 1982).

57. *See* Intelligence Identities Protection Act of 1982, 50 U.S.C. §§ 421-426 (2006).

58. *See id.* §§ 421, 426.

clandestinely abroad.[59] Penetration of these elaborate networks and the identification of the individuals comprising them can ultimately endanger case officers, as the connections may be traced back to particular officers.[60] Moreover, if exposed, assets are likely to be subject to adverse treatment.[61] Uncertainty surrounding the confidentiality of their relationship with the United States will discourage assets from providing helpful information, thus severely restricting the value of HUMINT.[62] For these reasons, Congress appropriately protected the identities of agents, informants, and sources, in addition to case officers. Assets and case officers are collectively referred to as "covert agents" in the statutory language.[63]

There are three categories of offenses under the IIPA. Applicability of each offense is based upon an individual's ability to access classified information and the nature of the subsequent unauthorized disclosure.[64] The IIPA addresses penalties for violations by both government "insiders" and "outsiders."[65] Generally, it is illegal for an individual to expose the identity of a "covert agent" when (1) the disclosing individual has or used to have access to classified information that identifies a covert agent,[66] (2) the disclosing individual learns the identity of a covert agent as a result of having access to other classified information,[67] or (3) the disclosing

---

59. *See supra* note 5 and accompanying text.

60. *See supra* note 13 and accompanying text.

61. *See supra* note 13.

62. *See supra* note 13.

63. *See* 50 U.S.C. § 426(4); *see also supra* note 1 (providing definitions of terms used within both the statutory language and this Note).

64. *See* 50 U.S.C. § 421.

65. *See* Susan D. Charkes, Note, *The Constitutionality of the Intelligence Identities Protection Act*, 83 COLUM. L. REV. 727, 730-31 (1983). "Insiders" are government employees who have access to classified information. *Id.* at 730. The IIPA distinguishes between two types of government "insiders" based upon an individual's ability to access certain categories of classified information. *Id.* Conversely, "outsiders" are nongovernment employees who are able to indirectly access classified information. *Id.* A typical "outsider" uncovers classified information through the public domain or an "inside" source. *See id.* at 731.

66. 50 U.S.C. § 421(a). This category covers current and former government "insiders" who have or had access to a specific category of classified information that directly identifies "covert agents."

67. *Id.* § 421(b). This category covers current government "insiders" who have access to classified information but not the specific class of information that identifies "covert agents."

individual has no direct access to classified information but engages in a "pattern of activities" intended to identify and expose covert agents with a reasonable belief that it will "impair or impede ... foreign intelligence activities."[68] Disclosures by government officials or personnel ("insiders") are covered under the first two categories of offenses, with the difference between the two offenses being the perpetrator's security clearance level or any other ability to access certain classified information. The third category of offenses applies to disclosures by any nongovernment personnel ("outsiders"), such as members of the media or academia.

The three categories of offenses share four elements. First, there must be an intentional unauthorized disclosure of a "covert agent's" identity.[69] Second, an individual who is not authorized to access classified information must receive the intentional, unauthorized disclosure.[70] Third, the perpetrator must know that the intentional, unauthorized disclosure will identify a "covert agent."[71] Finally, the perpetrator must also know that the U.S. government is taking affirmative steps to conceal the identity of the "covert agent" that the perpetrator is prepared to reveal.[72] If an individual qualifies under one of the three categories of offenses and these four elements are present, then that individual may be imprisoned for a period of three to ten years, with the additional possibility of a civil penalty.[73]

The remaining provisions within the IIPA set forth a number of defenses and exceptions, as well as definitions of the terminology used within the statute.[74] For example, in terms of defenses and exceptions, if the U.S. government discloses the "covert agent's" identity before the perpetrator makes the disclosure, this will serve

---

These individuals are able to infer the identity of a "covert agent" from circumstantial evidence derived from the classified information to which they are privileged access.

68. *Id.* § 421(c). This category covers any person, typically "outsiders," involved in the systematic exposure of "covert agents" with a reasonable belief that such activity will weaken U.S. intelligence efforts. Wolf is an example of an individual who would be categorized under this classification.

69. *Id.* § 421.

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.* §§ 422-426.

as a defense to prosecution.[75] A similar defense may be employed if the "covert agent" is self-identified before the perpetrator makes the disclosure.[76] These defenses are common to any of the three IIPA offenses.

II. THE IIPA'S LIMITED APPLICATION

On its surface, the purpose and scope of the IIPA appear to create an effective law to punish contemptible acts. Since its inception, however, the IIPA has faded into an insufficient and overlooked tool in criminal prosecutions. The 1985 prosecution of Sharon M. Scranage represents the only instance in which anyone has ever been charged under the IIPA.[77] While posted overseas with the CIA, Scranage leaked the identities of CIA case officers to her boyfriend Michael Soussoudis, a suspected intelligence agent in the Ghanaian intelligence service.[78] Because Scranage pleaded guilty to the charges,[79] the courts have not yet had an opportunity to comment on the IIPA.

Some critics argue that the lack of IIPA prosecutions indicates that the unauthorized disclosure of case officers' identities is no longer an issue, and therefore, the IIPA should be repealed.[80] It is evident, however, that the unauthorized disclosure of both case officers' and assets' identities remains a critical problem. Congress validated this belief when it directed the executive branch to enforce the IIPA following a number of relevant, unauthorized disclosures in the mid-1990s.[81] Since the IIPA's inception in 1982, there have

---

75. *Id.* § 421(a).

76. *Id.* § 421(d).

77. Richard B. Schmitt, *Rare Statute Figures in Rove Case*, L.A. TIMES, July 15, 2005, at A15.

78. *Id.*

79. *Id.*

80. *See, e.g.*, *id.* (suggesting that a few observers believe that the absence of prosecutions displays the success of the government's increased efforts to protect case officers' identities); Jesse Walker, *Agee's Revenge: It's Past Time To Kill the Intelligence Identities Protection Act*, REASON.COM, July 14, 2005, http://reason.com/archives/2005/07/14/agees-revenge ("The law is a solution in search of a problem.").

81. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4000.

been plenty of publicly known instances in which intelligence-related identities were wrongfully exposed.[82] These include the Valerie Plame Wilson affair.[83] In each occurrence, the disclosing individual either avoided charges or was charged under another statute, usually espionage related.[84]

Critics contend that the IIPA was passed to prevent a particular form of unauthorized disclosures of case officers' identities—specifically, the systematic exposures by Agee and Wolf.[85] Although the IIPA is a narrow law, enacted for a specific purpose, its language simply does not support the argument that its scope must be confined to thwarting only those activities in which Agee and his cohorts participated. Instead, its language criminalizes nearly every intentional, unauthorized disclosure of intelligence-related identities, not simply mass publication of those identities by "outsiders."[86]

---

82. *See, e.g.*, *id.* (indicating that, around 1997, there were several incidents involving the unauthorized disclosure of intelligence-related identities by both journalists and public officials, which, at least in one instance, might have led to a number of deaths); DEF. PERS. SEC. RESEARCH CTR., DEF. HUMAN RES. ACTIVITY, DEP'T OF DEF., ESPIONAGE CASES (1975-2004): SUMMARIES AND SOURCES 1-2, 16-17, 21, 26-28, 35, 37, 42, 44, 47 (2004), *available at* http://www.hqmc.usmc.mil/PP&O/PS/pss/Espionage_Cases_75-04.pdf [hereinafter ESPIONAGE CASES] (listing, in addition to Scranage, those indicted or convicted for activities involving the revelation of intelligence-related identities while spying: Aldrich H. Ames, Frederick C. Hamilton, Robert P. Hanssen, Edward L. Howard, Karl F. Koecher, Steven J. Lalas, Harold J. Nicholson, Earl E. Pitts, Richard C. Smith, and Douglas Tsou); Peter Finn, *Detainees Shown CIA Officers' Photos*, WASH. POST, Aug. 21, 2009, at A1 (reporting that military defense attorneys might have unlawfully identified CIA case officers in photographs provided to Guantanamo Bay detainees); *infra* note 136 (explaining that a former U.S. Senator and State Department official intentionally revealed to the public the identity of a CIA informant).

Based upon the substance of the leaked information, not all unauthorized disclosures of intelligence-related identities may be made public. *See* ESPIONAGE CASES, *supra*, at i. It is logical for the government, once it discovers that an unauthorized disclosure has occurred, to conceal that disclosure in an attempt to prevent further classified information from being exposed. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4000 (intimating that the government has not sought the prosecution of government officials under the IIPA for fear of exposing additional classified information during the course of a trial). Consequently, there could be additional examples that have simply not leaked into the public forum.

83. *See infra* Part II.B-C.

84. *See* ESPIONAGE CASES, *supra* note 82.

85. *See, e.g.*, Benjamin S. DuVal, Jr., *The Occasions of Secrecy*, 47 U. PITT. L. REV. 579, 602 (1986); Schmitt, *supra* note 77; Walker, *supra* note 80 (quoting U.S. Representative Charles W. Young during the House debate over the bill as saying, "'What we're after today are the Philip Agees of the world'").

86. *See* discussion *supra* Part I.C.

A few comments derived from the IIPA's legislative history supporting the proposition of a limited objective cannot override the actual purpose and scope of the IIPA's final language, which Congress overwhelmingly approved.[87]

It follows, therefore, that the IIPA remains a relevant protective device in the intelligence process and can serve as a useful deterrent to illegal activity. Yet, upon examining its over twenty-five year existence, there are three factors contributing to the IIPA's limited application: (1) the availability of an espionage statute that imposes more considerable penalties, (2) the IIPA's inherent limitations, and (3) a lack of political initiative to enforce the IIPA.

A. Availability of the Espionage Act

Most exposures of case officers, agents, informants, and sources occur when individuals illegally transmit information to foreign sources.[88] Consequently, many of these unauthorized disclosures can be packaged as part of an amalgamated charge of spying under the Espionage Act. Compared to the IIPA, the broader Espionage Act imposes a more significant penalty for the unauthorized disclosure of intelligence-related identities only if that exposure arises out of the more inclusive crime of spying.[89] Limitations of the Espionage Act were revealed, however, when the government was unable to halt the publication of case officers' identities by individuals other than spies, predominately "outsiders." Although distinguishable from espionage, these systematic exposures by nonspies have a similar effect, in that they undermine U.S. intelligence efforts.[90] Because the Espionage Act is inapplicable to this type of unauthorized

87. *See supra* note 54.

88. *See* ESPIONAGE CASES, *supra* note 82 (indicating that, of the listed occasions in which intelligence-related identities were illegally disclosed, in only one instance—the Scranage case—was the disclosing individual someone other than a spy).

89. *See* Espionage Act of 1917, 18 U.S.C. §§ 792-799 (2006) (containing several offenses that are punishable by death or life imprisonment, including the dissemination of defense information, which can, under certain circumstances, encompass the unauthorized disclosure of intelligence-related identities). *But see infra* notes 90-91 and accompanying text (summarizing potential difficulties in applying the Espionage Act to the unauthorized disclosure of intelligence-related identities).

90. *See* discussion *supra* Part I.A.

disclosure, the government recognized the need for an acceptable resolution to address the loophole.[91] This prompted the passage of the narrower IIPA.

Despite the existence of the Espionage Act, the IIPA remains essential to preventing a particular class of exposures. Nevertheless, if an unauthorized disclosure is punishable under either the IIPA or the Espionage Act, prosecutors will usually charge the perpetrator under the latter, because it will yield a greater penalty for the same wrong.[92] As long as most unauthorized disclosures of intelligence-related identities occur during the course of spying, prosecutions under the Espionage Act will substantially outnumber those under the IIPA. The opportunity for IIPA prosecutions, therefore, will be reduced. Notwithstanding this natural limitation on its use, there remain situations in which the IIPA is ideal. Even in those situations, however, the following two factors have considerably impeded the IIPA's application.

B. Inherent Limitations

Following the Scranage prosecution, the IIPA experienced eighteen years of dormancy. Once a prominent topic of discussion during the early 1980s, the IIPA eventually became an obscure law hidden within the U.S. Code. As it has aged, the IIPA's limitations have become apparent. The narrowness of the IIPA creates intrinsic defects in its application. For example, the IIPA protects an exceptionally limited class of intelligence-related individuals that manages to qualify under the statutory definition of a "covert agent."[93] Additionally, the restrictiveness of its offenses discourages prosecutors from utilizing the IIPA, because the evidentiary

---

91. *See* Maffet, *supra* note 8, at 1738-41 (surveying the possibility of applying the Espionage Act to the protection of intelligence-related identities and the difficulties that arise therefrom, with much focus as to whether such unauthorized disclosures always relate to "national defense" and whether the Espionage Act is applicable to the prosecution of "outsiders").

92. *See supra* note 89 and accompanying text.

93. *See* Intelligence Identities Protection Act of 1982, 50 U.S.C. §§ 421, 426(4)(A) (2006).

burdens are too great.[94] The IIPA, therefore, is largely ignored. These inherent shortcomings, accounting for the second factor in the IIPA's limited application, are most clearly illustrated by the Plame affair.

It was not until 2003 that the IIPA was thrust back into the limelight, causing people to question this little-known law. Discussion of the IIPA resurfaced after Valerie Plame Wilson was exposed as a CIA case officer in a newspaper column written by Robert D. Novak.[95] Members of the George W. Bush administration, namely Richard L. Armitage (former U.S. Deputy Secretary of State), I. Lewis "Scooter" Libby (former Chief of Staff to Vice President Richard B. Cheney), and Karl C. Rove (former Deputy Chief of Staff to the President), were investigated for their possible roles in leaking Plame's identity to various journalists.[96] As the investigation commenced, the law for which President George H.W. Bush had fought so vigorously,[97] ironically, was contemplated as the principal tool for criminally charging senior officials within his son's administration.[98]

---

94. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4000 (suggesting that the constrictiveness of the elements of an IIPA offense may be a reason behind its lack of enforcement by the U.S. Department of Justice, as prosecutors are unsure whether they can prove each element).

95. Robert D. Novak, *Mission to Niger*, WASH. POST, July 14, 2003, at A21 ("Wilson never worked for the CIA, but his wife, Valerie Plame, is an agency operative on weapons of mass destruction.").

96. *See generally* Wilson v. Libby, 498 F. Supp. 2d 74, 79-82 (D.D.C. 2007) (providing a comprehensive overview of the alleged circumstances surrounding the leaking of Plame's identity and the individuals purportedly involved in her exposure), *aff'd*, 535 F.3d 697 (D.C. Cir. 2008), *cert. denied*, 129 S. Ct. 2825 (2009).

97. The IIPA garnered enthusiastic support from the Reagan administration. *See supra* notes 53-56 and accompanying text. At the time of the IIPA's enactment by President Reagan, George H.W. Bush was Vice President and former DCI. Speaking on the topic of the unauthorized disclosure of intelligence-related identities, President George H.W. Bush stated, "'I have nothing but contempt and anger for those who betray the trust by exposing the name [sic] of our sources. They are, in my view, the most insidious of traitors.'" 151 CONG. REC. S8268 (2005) (statement of Sen. Harry M. Reid (quoting President George H.W. Bush)).

98. *See* Government's Sentencing Memorandum at 12-14, United States v. Libby, 495 F. Supp. 2d 49 (D.C. Cir. 2005) (No. 05-394).

Ultimately, only Libby was indicted for the events surrounding the unauthorized disclosure of Plame's identity.[99] Although Plame's identity was unlawfully exposed, the U.S. Department of Justice Special Counsel assigned to the case, Patrick J. Fitzgerald, opted to forgo IIPA charges against Libby due to a lack of evidence.[100] As an alternative, Fitzgerald charged Libby with making false statements, obstruction of justice, and perjury.[101] Even though it is uncertain exactly what or how much evidence was lacking to charge Libby under the IIPA, the problems in meeting the evidentiary requirements were likely correlative to the narrowness of the statute and its offenses. Two of the elements, in particular, present complications when applied to the facts of the case.

One difficulty in applying the IIPA was determining Plame's status at the time of the unauthorized disclosure. The first element of any IIPA offense requires that the exposed individual be within a limited class of protected persons.[102] Plame, therefore, must have fallen within the definition of a "covert agent."[103] To qualify under this definition, Plame's identity and relationship with the CIA must have been classified information,[104] she must have served outside of the United States at the time of her exposure or within five years before her exposure,[105] and the CIA must have been taking "affirmative measures" to conceal her identity at the time of the exposure.[106] Although this language appears straightforward, many complications arise when the definition is applied. First, it is unclear what assignments constitute clandestine service abroad during the five-year period. For example, a case officer may have short, sporadic clandestine assignments outside of the country during a period when that officer is officially stationed within the United States for

---

99. *See generally* Indictment, United States v. Libby, 495 F. Supp. 2d 49 (D.C. Cir. 2005) (No. 05-394).

100. *See In re* Grand Jury Subpoena, Miller, 438 F.3d 1141, 1181 (D.C. Cir. 2005) (Tatel, J., concurring); *see also* Government's Sentencing Memorandum, *supra* note 98.

101. *See generally* Indictment, *supra* note 99.

102. *See* Intelligence Identities Protection Act of 1982, 50 U.S.C. § 421 (2006); *see also supra* Part I.C (discussing briefly the four elements common to any IIPA offense).

103. 50 U.S.C. § 421.

104. *See id.* § 426(4)(A)(i).

105. *See id.* § 426(4)(A)(ii).

106. *See id.* § 421.

domestic assignments.[107] Such a scenario may or may not constitute clandestine service abroad.[108] Second, there is inconsistency in interpreting the standard for "affirmative measures" taken in concealing a case officer's identity. For instance, criticism may arise over the adequacy of both the government's and the case officer's efforts in concealing the officer's identity, leading to skepticism that there was an actual intent to maintain complete secrecy.[109] In the Libby prosecution, there were many questions regarding these two issues, and therefore, debate ensued over whether Plame was, by statutory definition, a "covert agent."[110] Eventually, Fitzgerald concluded that Plame was a "covert agent" at the time of her exposure, but this statement came only after he abandoned the possibility of pursuing IIPA charges.[111] Even though this was Fitzgerald's determination, it is unclear that a court would come to the same conclusion given the ambiguity surrounding the term's definition. Fitzgerald's recognition of this uncertainty regarding Plame's inclusion in the statutory class of protected persons might have contributed to his decision not to charge Libby under the IIPA.

Even if Plame satisfied the "covert agent" element, the narrowness of the IIPA offenses presented difficulties in proving a second element. Fitzgerald had to demonstrate that Libby possessed the requisite knowledge that Plame was, indeed, covert and that the

---

107. *See, e.g.*, Joel Seidman, *Plame Was 'Covert' Agent at Time of Name Leak*, MSNBC, May 29, 2007, http://www.msnbc.msn.com/id/18924679/ ("[W]hile she was assigned to [CIA headquarters], Plame, 'engaged in temporary duty travel overseas on official business .... [S]he traveled at least seven times ...., sometimes in true name and sometimes in alias—but always using cover—whether official or non-official ... with no ostensible relationship to the CIA.'" (quoting Plame's unclassified CIA employment history)).

108. *Cf.* Adam Liptak, *C.I.A. Inquiry May Hinge on What the Leaker Knew*, N.Y. TIMES, July 18, 2005, at A14 ("'I don't believe the statute requires a permanent assignment abroad. It can be trips abroad.'" (quoting Christopher Wolf, legal counsel for the Wilsons)).

109. *See, e.g.*, Schmitt, *supra* note 77 ("[A former] deputy assistant attorney general under President Reagan .... doubted Plame qualified as a 'covert' operative, and ... said that the CIA was 'cavalier' about protecting her status." (quoting Victoria Toensing)).

110. *See generally* Byron York, *Valerie Plame: Was She, or Wasn't She?*, NAT'L REV. ONLINE, Feb. 6, 2006, http://www.nationalreview.com/york/york200602060919.asp (analyzing evidence used by the court regarding Plame's covert status and efforts to conceal Plame's identity at and before the unauthorized disclosure).

111. Seidman, *supra* note 107 ("'[Plame] was a covert CIA employee for who [sic] the CIA was taking affirmative measures to conceal her intelligence relationship to the United States.'" (quoting Plame's unclassified CIA employment history)).

government was taking affirmative steps to conceal her identity.[112] He, however, possessed no direct evidence to this effect.[113] Proving the "knowledge" element would have been a demanding task for Fitzgerald. If Fitzgerald and others had difficulty interpreting the ambiguity of the term "covert agent," then it is highly unlikely that Libby unequivocally knew that Plame satisfied this statutory definition. Likewise, interpreting the term "affirmative measures" presents complications, and so proving Libby's actual knowledge of this would have been equally challenging. The difficulty in establishing the presence of such knowledge increased exponentially when Libby failed to cooperate with the investigation. This uncooperativeness led to Libby's conviction for making false statements, obstruction of justice, and perjury.[114] Without Libby's cooperation, it is doubtful that Fitzgerald could have successfully pursued IIPA charges, as proving the "knowledge" element required Fitzgerald to elicit information that only Libby likely possessed. Fitzgerald could have possibly gathered circumstantial evidence from conversations or statements that demonstrated Libby's constructive knowledge of Plame's covert status, but this would have occurred in only the most fortunate of scenarios given the confidential nature of the information at issue. In the end, the "knowledge" element exemplifies the burdensome evidentiary demands necessary to establish culpability under the narrow IIPA offenses and the investigative complications that arise in satisfying those requirements.

Based on investigative reports and his decision not to pursue Libby under the IIPA, Fitzgerald appeared to doubt that he could overcome the two elemental difficulties the case presented: (1) establishing that Plame fell within the limited class of protected persons, and (2) proving that Libby possessed the requisite knowledge of both Plame's covert status and the measures taken by the government to conceal her identity. Ultimately, the uncertainty surrounding the "covert agent" definition and the IIPA's overwhelm-

---

112. *See* Intelligence Identities Protection Act of 1980, 50 U.S.C. § 421(a)-(b) (2006).

113. Affidavit of Patrick J. Fitzgerald at 28 n.15, *In re* Special Counsel Investigation, 374 F. Supp. 2d 238 (D.C. Cir. 2008) (No. 04-MS-407) ("To date, we have no direct evidence that Libby knew or believed that Wilson's wife was engaged in covert work.").

114. Neil A. Lewis, *Libby Guilty of Lying in C.I.A. Leak Case*, N.Y. TIMES, Mar. 6, 2007, http://www.nytimes.com/2007/03/06/washington/06cnd-libby.html.

ing evidentiary demands—both results of the statute's narrowness—precluded its use against Libby and others involved in the leak. These inherent limitations undermined the IIPA's prosecutorial value in penalizing the illegal activity it was anticipated to prevent.

C. Lack of Political Initiative

A third factor inhibiting the IIPA's application is a lack of political will to have a firm and consistent response to unauthorized disclosures of intelligence-related identities,[115] especially when such disclosures come from within the government.[116] Contributing to this apathetic approach is (1) a concern that questions regarding the IIPA's constitutionality may produce political backlash,[117] (2) a fear that IIPA prosecutions may lead to the disclosure of further classified information at trial,[118] and (3) the desire to use unautho-

---

115. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 34-35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 3999-4000 (expressing congressional displeasure with an "apparent unwillingness" to enforce the IIPA).

116. *See* James B. Bruce, *The Consequences of Permissive Neglect: Laws and Leaks of Classified Intelligence*, 47 STUD. INTELLIGENCE 39, 43-44 (2003), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v47i1a04p.htm (citing a 1996 National Counterintelligence Policy Board (NACIPB) study reporting on the government's ability to control leaks of classified information) (explaining that the absence of political initiative in enforcing unauthorized disclosures of classified information has evolved into a mindset of "permissive neglect").

117. *See* David Ignatius, Op-Ed., *When Does Blowing Secrets Cross the Line?*, WASH. POST, July 2, 2000, at B7 (discussing how the lack of prosecutions regarding leaks of classified information results from the Department of Justice wanting "to avoid a politically explosive hunt for a journalist's sources"); *see also infra* notes 120-24 and accompanying text (providing further insight into the First Amendment concerns surrounding the IIPA).

118. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4000 (suggesting that the risk of further disclosure of classified information during court proceedings may be a reason behind the IIPA's weak enforcement by the U.S. Department of Justice); Bruce, *supra* note 116, at 47 ("The US government has shown a debilitating reluctance to pursue legal remedies for the most serious leaks partly because subsequent courtroom publicity of sensitive information subverts its first objective of protecting such information from further disclosures."); *cf.* United States v. Morison, 844 F.2d 1057, 1067 (4th Cir. 1988) (citing Haig v. Agee, 453 U.S. 280 (1981)) (explaining the difficulties in balancing the need for prosecution and the possible damage resulting from the disclosure of secrets in a public trial when charging an individual under the Espionage Act).

rized disclosures as a vehicle to influence policy.[119] Regardless of the motivation, this lack of political initiative by the executive branch has greatly contributed to the IIPA's limited application.

One issue contributing to the lack of political will in enforcing the IIPA is the constitutional concerns surrounding its language. There is disquiet among commentators regarding the IIPA's language when applied to the First Amendment.[120] Some believe that the IIPA's language—particularly § 421(c), relating to the censoring of "outsiders"—violates the freedoms of speech and press.[121] At the time of its enactment, however, there was bipartisan agreement that the IIPA was constitutional,[122] even following testimony by several interest groups, including civil rights organizations, journalists, and legal scholars.[123] Although there are informed arguments on each side of the constitutionality debate, the courts have yet to weigh in on the issue because no IIPA prosecutions have made their way to the bench.[124]

A general hesitancy to avoid uncertainty and constitutional debate may assist in explaining the lack of political will in enforcing the IIPA. From the standpoint of the government, it is better served

---

119. *See* Bruce, *supra* note 116, at 44 (citing a 1996 NACIPB study reporting on the government's ability to control leaks of classified information); *see also* LOWENTHAL, *supra* note 1, at 204-05 ("Leaks occur for a variety of reasons: to show off some special knowledge, to settle scores, or to promote or stop a policy.").

120. Most discussion and analysis of the IIPA's constitutionality has been limited to student commentary. *See infra* note 121.

121. *See generally, e.g.*, Charkes, *supra* note 65, at 748-53 (concluding that § 421(c) violates the First Amendment, even if narrowly construed); Lawrence P. Gottesman, Note, *The Intelligence Identities Protection Act of 1982: An Assessment of the Constitutionality of Section 601(c)*, 49 BROOK. L. REV. 479, 482-83, 515-16 (1983) (concluding that § 421(c) violates the First Amendment). *But see generally* Ferguson, *supra* note 53, at 483, 489 (concluding that Congress struck a proper balance between executive secrecy and free speech); Bivins, *supra* note 25, at 842-43, 851, 859-61, 864 (concluding that the IIPA constitutes a permissible speech restriction under either the compelling interest test or present danger test of the First Amendment).

122. *See* BAZAN, *supra* note 50, at 4 (citing S. REP. NO. 97-201, at 14-18 (1982), *as reprinted in* 1982 U.S.C.C.A.N. 145, 158-62; H.R. REP. NO. 97-580, at 7-10 (1982) (Conf. Rep.), *as reprinted in* 1982 U.S.C.C.A.N. 170, 171-75) (explaining that the Senate Judiciary Committee and the Conference Committee considered the constitutionality of the IIPA at length, especially with regard to § 421(c) and its First Amendment implications, and both concluded that its language would pass constitutional muster).

123. Ferguson, *supra* note 53, at 484-85.

124. *See supra* note 79 and accompanying text.

prosecuting individuals under less confined, more reliable, and well-established laws. Greater predictability in evidentiary standards, especially given the national security implications that accompany a crime of this magnitude, can be a desirable asset when handling a prosecution.[125] From the perspective of elected officials within the executive branch, they may want to avoid IIPA prosecutions, particularly against journalists and other "outsiders," because the press will surely brand any attempt at doing so as a trampling of its rights under the First Amendment. The constitutional concerns surrounding the IIPA and the underlying political effects accompanying those apprehensions have contributed to the lack of political will in enforcing the IIPA.

Another issue influencing the lack of political initiative in enforcing the IIPA is the fear that prosecution will lead to further disclosures of classified information in court, especially if the trial is public. Deciding whether to charge an individual under the IIPA involves a calculated cost-benefit analysis. For example, in debating whether to pursue charges in the Plame affair, the CIA concluded, "'the public interest in allowing the criminal prosecution to proceed outweighed the damage to national security that might reasonably be expected from the official disclosure of [Plame's] employment and covert status.'"[126] Although the Classified Information Procedures Act (CIPA) exists to protect from further dissemination of classified information under these circumstances,[127] this safeguard has not eased apprehension among prosecutors, as evidenced by the lack of IIPA prosecutions.[128]

The final issue influencing the lack of political will in enforcing the IIPA is the desire to use unauthorized disclosures as a vehicle to influence policy. Along with serving as a case study in examining the inherent limitations of the IIPA, the Plame affair also provides a quintessential example of the lack of political will in keeping case

---

125. *See, e.g.*, Part II.B.

126. Seidman, *supra* note 107.

127. Classified Information Procedures Act, 18 U.S.C. app. §§ 1-16 (2006); *see also* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4000.

128. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4000.

officers' identities secret. Regardless of whether the IIPA was violated, the Plame affair makes evident that the initial exposure of Plame's identity was motivated by the desire of some members of the Bush administration to use the disclosure as a means to achieve political ends.[129]

As a corollary to this, the obvious inferential question is whether the executive branch zealously supported and pursued IIPA charges. Trepidation about the possibility that the executive branch would not actively pursue charges led to Fitzgerald's appointment as special counsel.[130] Supporting the assertion that political forces were lurking throughout the Plame affair is President Bush's response to the situation. The President quickly refined his position with regard to how he would respond to members within his administration who were discovered to be responsible for the exposure. He went from saying that he would immediately dismiss anyone found to have leaked Plame's identity to stating that he would discharge members of his administration only if they were found to have broken the

---

129. As an attempt to refute a report by Ambassador Joseph C. Wilson IV, in which Ambassador Wilson concluded that Iraq did not attempt to purchase uranium from Niger, senior members of the Bush administration spoke with journalists and provided them with evidence to discredit Ambassador Wilson. *See generally* Wilson v. Libby, 498 F. Supp. 2d 74, 78-81 (D.D.C. 2007). In so doing, these officials reportedly criticized the CIA's handling of Ambassador Wilson's trip, given that Ambassador Wilson traveled to Niger at the request of the CIA. *See id.* at 78-80. Armitage, Libby, and Rove all engaged in conversations with the press, and each leaked Plame's CIA status to various journalists. *See id.* at 78-81. The exposure was motivated by the fact that Plame was Ambassador Wilson's wife, and she was allegedly responsible for arranging her husband's trip to Niger. *See id.* at 78. According to the Wilson complaint, Rove supposedly told a reporter that Plame was "fair game" in the debate over the validity of Ambassador Wilson's report. *Id.* at 80. Although it is obvious from personal admissions and press reports that these three government officials played a distinct role in the leaking of Plame's identity, it is less clear that they actually violated the IIPA. The difficulty in investigating and charging each official was likely attributable to various factors, such as Libby's uncooperativeness and the confining elements comprising an IIPA offense. *See supra* Part II.B. For example, in terms of the IIPA's confining elements, it is plausible that Armitage, Libby, and Rove simply did not maintain the requisite knowledge that Plame was a "covert agent" in accordance with the statutory definition. *See supra* notes 112-14 and accompanying text (providing in detail the difficulties in proving the "knowledge" element). Ultimately, one must presume that they did not violate the IIPA, given that Fitzgerald did not pursue IIPA charges.

130. *See* David Johnston, *Top Bush Aide Is Questioned in C.I.A. Leak*, N.Y. TIMES, Feb. 10, 2004, at A1.

law.[131] Such a quick refinement of his position could be a result of the Bush administration's understanding that convicting anyone under the IIPA would prove exceedingly difficult. Irrespective of whether Armitage, Libby, or Rove violated the IIPA, the fact that senior officials within a presidential administration, who publicly exposed a CIA employee, can avoid adverse repercussions for that action, simply because the sitting administration deemed they did not technically violate the law, displays where protecting case officers' identities ranks on politicians' priorities. This point is further emphasized by President Bush's decision to commute Libby's sentence for his conviction in the Plame affair before Libby had even served any prison time.[132]

The Plame affair, however, is only one example of the lack of political initiative in enforcing the IIPA.[133] Over the past twenty-five years, there have been several opportunities for the IIPA to be tested against other potential defendants,[134] but it has been used only once.[135] This lack of political will to enforce the IIPA has been present throughout both Democratic and Republican presidential administrations.[136] Although specific reasons for the hesitancy to

---

131. *See Examining the Intelligence Identities Protection Act* (NPR radio broadcast July 19, 2005), http://www.npr.org/templates/story/story.php?storyId=4760261 (follow "Listen" hyperlink).

132. Amy Goldstein, *Bush Commutes Libby's Prison Sentence*, WASH. POST, July 3, 2007, at A1.

133. This does not suggest that the absence of IIPA charges following Fitzgerald's investigation was a result of political influence. The available evidence suggests only that political forces were behind the initial unauthorized disclosure, not the decision of whether to pursue IIPA charges. *See supra* note 129. The facts Fitzgerald elicited from the Plame affair and the circumstances surrounding that investigation are not completely known, including the government's investigative capabilities in light of Libby's obstruction of justice. For this reason, any assertion that political influence was behind Fitzgerald's decision to exclude the IIPA from the Plame affair is unfounded, especially given Fitzgerald's appointment as independent special counsel.

134. *See supra* notes 81-84 and accompanying text.

135. *See supra* note 77 and accompanying text (noting that Scranage represents the only IIPA prosecution).

136. The Plame affair does not signify that the lack of political will in enforcing the IIPA lies exclusively with Republicans. For instance, during the William J. Clinton administration, Democrats failed to pursue charges against Richard A. Nuccio—an official within the Department of State—and Democratic U.S. Senator Robert G. Torricelli after they both publicly disclosed the identity of a CIA informant who they believed was involved in the murder of a Guatemalan. *See* Shane, *supra* note 30. Furthermore, a congressional report,

use the IIPA in each of the circumstances are unknown, the IIPA's inherent limitations and a lack of political will to overcome those limitations are at least two contributing factors. Unless this pervasive mindset within the executive branch suddenly changes, it will continue to impede the IIPA's application and effectiveness.

III. THE CRITICAL NEED FOR AN AMENDMENT

Even with evidence that the unauthorized disclosure of intelligence-related identities remains a critical problem,[137] the IIPA's application has been severely limited. The three preceding factors have encumbered the IIPA's effectiveness and enforcement in situations when it was intended to penalize egregious behavior.[138] As currently written, the IIPA is not only ineffective in its enforcement, but also it is not a formidable deterrent because it is used so infrequently that its existence is unbeknownst to most people. Consequently, the IIPA has failed to follow through in its intended purpose—to protect case officers' identities by imposing penalties on those who intentionally disclose those identities without proper authorization.[139] Yet, case officers rely on the secrecy the IIPA is supposed to protect as the final guardian of their safety while they serve their country abroad.[140] Unless the IIPA is significantly amended, it risks falling into another extensive period of quiescence

---

published in late 1996, conveyed displeasure with the Clinton administration's failure to enforce the IIPA in several applicable situations. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 34-35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 3999-4000.

137. *See supra* notes 80-84 and accompanying text.

138. *See supra* Part II.

139. *See* discussion *supra* Part I.C.

140. This is especially true given that case officers cannot always rely upon policymakers and politicians to protect their identities. *See supra* Part II.C. Furthermore, case officers do not have an adequate civil remedy to seek compensation for the adverse personal effects they must endure as a result of their exposure. *Cf.* Near v. Minnesota, 283 U.S. 697, 718-19 (1931) (stating that *public officers*, whose character and conduct are open to free discussion and debate in the press, have remedies in libel law rather than attempts to restrain publication). *See generally* Wilson v. Libby, 498 F. Supp. 2d 74, 77-78, 82, 96 (D.D.C. 2007) (denying plaintiffs the ability to seek civil compensation under a *Bivens* remedy for the unauthorized disclosure of a case officer's identity), *aff'd*, 535 F.3d 697 (D.C. Cir. 2008), *cert. denied*, 129 S. Ct. 2825 (2009).

with the increased possibility that it will become completely defunct. Properly amending the IIPA will result in an effective law capable of both punishing and deterring the unauthorized disclosure of intelligence-related identities, thereby establishing a critical protective device for the intelligence community to utilize in enhancing case officers' safety and ensuring national security.

A. Policy Justifications

Even though the U.S. Supreme Court has recognized that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation,"[141] there has long been debate over the balance of openness and secrecy in conducting national security operations. Emerging from this debate is general agreement that certain segments of classified information must absolutely be protected from public disclosure,[142] including the identities of case officers.[143] Exposing a case officer's identity serves no legitimate public purpose.[144] Such unauthorized disclosures go

> far beyond information that might contribute to informed public debate on foreign policy or foreign intelligence activities.... It does not alert to abuses; it does not further civil liberties; it does not enlighten public debate; and it does not contribute one iota to the goal of an educated and informed electorate. Instead, it reflects a total disregard for the consequences that may jeopardize the lives and safety of individuals and damage the ability of

---

141. Haig v. Agee, 453 U.S. 280, 307 (1981) (quoting Aptheker v. Sec'y of State, 378 U.S. 500, 509 (1964)).

142. *See* Snepp v. United States, 444 U.S. 507, 510 n.3 (1980) ("The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service.").

143. *See, e.g.*, RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM 16-17 (2006); DuVal, *supra* note 85, at 598.

144. Intelligence Identities Protection Act of 1982, Remarks on Signing H.R. 4 Into Law, 18 WEEKLY COMP. PRES. DOC. 829 (June 23, 1982); *see also* Bivins, *supra* note 25, at 859-60 (setting forth reasons why identifying case officers to promote oversight and informed debate is an unacceptable premise).

> the United States to safeguard the national defense and conduct an effective foreign policy.[145]

Although public and media oversight of the executive branch is an indispensible component in maintaining an honest and responsible representative democracy, recklessly accusing the U.S. government of misdeeds by identifying intelligence personnel endangers lives and compromises national security. Promoting accountability in the executive branch is achieved just as successfully by alerting the public to abuses and wrongs without exposing names or supplying personal, identifying information. This belief prompted bipartisan support for the enactment of the IIPA.[146] The IIPA, however, has failed miserably,[147] thus justifying the need for an amendment.

B. Constructing an Amendment

Upon analyzing the three factors contributing to the IIPA's limited application, the most significant of those factors—the IIPA's inherent limitations—can be addressed directly through an amendment. The IIPA's shortcomings emanate from its narrowness.[148] Propelling this narrowness is the exceptionally limited class of intelligence-related identities the IIPA protects and the restrictiveness of the IIPA's offenses. These two intrinsic defects must be the primary focus of any amendment. Using the IIPA's past failures, the most helpful of which is the Plame affair, a comprehensive and effective amendment can be devised to address the inherent limitations that have plagued the IIPA from its beginning.

1. Expanding the Class of Protected Persons

One priority of an IIPA amendment must be expanding the class of protected individuals. After over a decade passed without the

---

145. BAZAN, *supra* note 50, at 4 (quoting statements of the Conference Committee contained within H. REP. NO. 97-580, at 7-8 (1982) (Conf. Rep.), *as reprinted in* 1982 U.S.C.C.A.N. 170, 171-72) (internal quotation marks omitted).

146. *See supra* Part I.B.

147. *See supra* Part II.

148. *See supra* Part II.B.

IIPA being used, Congress, in 1999, confirmed that it had not forgotten about the obscure law. Realizing that the scope of those protected needed to be expanded, Congress amended the IIPA to allow for the protection of retired case officers.[149] Because of this amendment, it is generally illegal to expose a retired case officer whose identity remains classified and who has served outside of the United States within the prior five years,[150] provided that the other statutory elements common to any IIPA offense are present.[151] Although this amendment was an improvement to the IIPA, it was not expansive enough.

The most exacting language restricting the class of protected persons is the statutory definition of a "covert agent." This definition excludes from protection any current or former case officer that has *not* served clandestinely outside of the United States within five years of the exposure.[152] Five years is simply an arbitrary period imposed by legislators.[153] In place of this arbitrary five-year period, case officers' identities should be protected indefinitely.[154] Indefinite protection will permit exposure of a case officer's identity in instances only when the IIPA's statutory defenses apply (including self-identification by the officer),[155] the government is not taking "affirmative measures" to conceal the officer's identity,[156] or the officer's identity is declassified.[157]

There are three justifications for indefinite protection. First, the continued protection of a case officer's identity is a matter that deserves an informed determination by the respective intelligence

---

149. *See* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2000, H.R. REP. NO. 106-457, at 6, 37 (1999) (Conf. Rep.), *as reprinted in* 1999 U.S.C.C.A.N. 304, 308.

150. *See* Intelligence Identities Protection Act of 1982, 50 U.S.C. § 426(4)(A) (2006).

151. *See* discussion *supra* Part I.C.

152. *See* 50 U.S.C. § 426(4)(A)(ii).

153. According to Victoria Toensing, the former chief counsel to the Senate Select Committee on Intelligence who assisted in drafting the IIPA, a time frame from one year to ten years was discussed. *See Examining the Intelligence Identities Protection Act*, *supra* note 131.

154. *But see* Nathan Alexander Sales, *Secrecy and National Security Investigations*, 58 ALA. L. REV. 811, 876-79 (2007) (arguing that although the government may occasionally need to keep information secret for lengthy periods, indefinite secrecy is never warranted).

155. *See supra* notes 74-76 and accompanying text (providing a short overview of the defenses and exceptions found within the IIPA).

156. *See* 50 U.S.C. § 421.

157. *See id.* § 426(4)(A)(i).

agency on a case-by-case basis, as compared to an arbitrary blanket rule applied by a disconnected third party[158]—in this case, Congress. Indefinite protection will provide intelligence agencies with the power, through the declassification process, to make the critical decision of when a case officer's identity no longer necessitates protection rather than placing that authority with the legislature. Second, indefinite protection is supported by the assertion that exposing case officers' identities serves no legitimate public purpose.[159] Unlike law enforcement officers, who differ emphatically from intelligence operatives, there is no need for case officers' identities to be exposed for purposes of due process.[160] Furthermore, exercises in government oversight are equally successful when case officers' identities are not exposed.[161] Third, the IIPA, inexplicably, already provides indefinite protection for all assets but not all case officers. According to the IIPA, the identity of any foreign national who is or has served as an agent, informant, or source to an intelligence agency, provided that the connection to the United States is classified, will be protected for as long as that relationship remains classified.[162] Because Congress has deemed it necessary to protect foreign nationals, it is imperative that their case officer counterparts are granted equal treatment. For these reasons, the identities of case officers must be protected indefinitely, without artificial limitations on disclosure.

Providing a framework for indefinite protection will also bring many advantages to both case officers and the intelligence community, thereby enhancing the usefulness of HUMINT. First, indefinite protection will strengthen protection of the intelligence networks that case officers establish abroad. These networks include case

158. *Cf.* CIA v. Sims, 471 U.S. 159, 176 (1985) ("We seriously doubt whether a potential intelligence source will rest assured knowing that judges, who have little or no background in the delicate business of intelligence gathering, will order his identity revealed.").

159. *See* Bivins, *supra* note 25, at 859-60.

160. Law enforcement officers' duties differ drastically from those of intelligence operatives, in that law enforcement officers are directly involved in the criminal justice process. Law enforcement officers, for example, have arrest powers and often testify at trial, requiring them to be present and identifiable. *See* U.S. CONST. amend. VI. Conversely, there is no such requirement for intelligence operatives who simply gather information.

161. *See* discussion *supra* Part III.A.

162. 50 U.S.C. § 426(4)(C). These intelligence relationships typically remain classified for an extensive period.

officers' fellow colleagues and assets.[163] Such connections and relationships do not terminate after a five-year period; instead, they last for the lifetimes of the individuals involved.[164] No matter if an unauthorized disclosure of a case officer's identity occurs either five years or fifteen years following that officer's clandestine service abroad, there is always the possibility that foreign governments can reconstruct the actions, contacts, and affiliations of the exposed officer.[165] Second, indefinite protection will instill current and potential assets with increased confidence that the identities of the case officers with whom they interact will remain secret. This added security will lead to a greater flow of information from a larger number of assets. Third, the integrity of the covert operations with which departing case officers were involved will remain intact. Not only will the established networks of those operations continue undamaged, but also CIA front organizations[166] and companies[167] integral to those operations will not be compromised as a consequence of a case officer's exposure following five years of inactive clandestine service abroad. Finally, indefinite protection will remove unneeded restrictions on both intelligence agencies' personnel management and the personal career choices of case officers. Exposure of a case officer's identity typically destroys any future possibility for that officer to serve clandestinely.[168] For this reason, under the current framework, if a case officer rotates out of the clandestine service for more than five years, then that officer should

---

163. *See supra* notes 5-7, 13 and accompanying text.

164. One military media analyst insists, "Clandestine intelligence officers and their recruited assets need protection virtually the rest of their lives." Posting of Lt. Col. Rick Francona to Hardblogger, http://hardblogger.msnbc.msn.com/Archive/2007/03/06/81133.aspx (Mar. 6, 2007, 14:50 EST) (arguing that the five-year protection period in the IIPA is an arbitrary time frame).

165. *See* Walter Pincus & Mike Allen, *Leak of Agent's Name Causes Exposure of CIA Front Firm*, WASH. POST, Oct. 4, 2003, at A3 ("A former diplomat ... said ... that every foreign intelligence service would run Plame's name through its databases within hours of its publication to determine if she had visited their country and to reconstruct her activities.").

166. Those organizations include ones such as the AIFLD in Nicaragua. *See supra* note 42 and accompanying text.

167. These companies include the former Brewster Jennings & Associates of the Plame affair. *See* Pincus & Allen, *supra* note 165 (explaining that the disclosure of Plame's identity revealed that Brewster Jennings & Associates was a CIA front company for which Plame purportedly worked).

168. Francis, *supra* note 35, at 3.

be restricted from returning to clandestine service abroad.[169] By removing these restrictions on rotation, the confusion regarding whether an intelligence professional is statutorily defined as a "covert agent" will be avoided. For instance, if indefinite protection was provided during the Plame affair, then there would have been few questions as to whether Plame qualified as a statutorily protected individual, even with her sporadic and questionably clandestine assignments abroad.[170] Easily resolving this question would have relaxed the burdensome evidentiary requirements that prevented Fitzgerald from pursuing IIPA charges, as the prosecution would have needed to show only that Plame, at any point, was a case officer, her identity remained classified information, and there were "affirmative measures" taken to protect her identity.[171] Lessening the evidentiary requirements by simplifying the definition of statutorily protected persons will assist prosecutors in clearly identifying instances when the IIPA has been violated. Furthermore, implementing indefinite protection will eradicate the ambiguities in applying the "covert agent" definition, thereby appropriately shifting the burden of making the delicate interpretation of the term "covert agent" away from the judiciary when the courts finally have the opportunity to comment on the IIPA.

The justifications for and results of a framework for indefinite protection make it clear that an amendment is essential and long

---

169. Whether the intelligence community maintains internal policies preventing this type of situation is unknown. Nevertheless, it is imprudent for an intelligence agency to allow a former case officer to recommit to the clandestine service following more than five years of inactive clandestine service abroad because that officer's identity, under the current law, could have been *legally* disclosed in the interim. *See* Intelligence Identities Protection Act of 1982, 50 U.S.C. § 426(4)(A) (2006). Given the ever-increasing capability of communication technology, it is impossible for the intelligence community to be cognizant of or monitor every publication regarding the identification of its current and former case officers during periods when they are not considered "covert agents." Allowing an employee to reenter the clandestine service under such circumstances will not only endanger that officer but also those associated with him or her. *See supra* notes 10, 13 and accompanying text. The potential calamity of the consequences, therefore, is equal to that as if the case officer's identity is illegally exposed.

170. *See* discussion *supra* Part II.B.

171. Although this proposal does not address the ambiguity surrounding the standard for evaluating "affirmative measures," it increases the likelihood of the IIPA's application by expanding the class of protected persons, which would finally allow the courts to address the definition of "affirmative measures." In cases in which the standard is disputed, defining "affirmative measures" is a matter upon which the judiciary should expound.

overdue. Eliminating the arbitrary five-year component within the "covert agent" definition will expand protection to numerous, deserving current and former case officers. Moreover, a framework for indefinite protection of case officers' identities will serve the interests of the intelligence community by strengthening HUMINT, allowing greater application of the IIPA, and assisting in eradicating one of the IIPA's inherent limitations that became evident during the Plame affair.

2. Easing the Narrowness of Its Offenses

Another priority of an IIPA amendment must be easing the narrowness of its offenses. This narrowness has contributed to its lack of application in many instances.[172] The elements comprising an IIPA offense are so restrictive that prosecuting individuals under the statute becomes exceedingly difficult.[173] There is a joint solution to this issue, which will disturb neither the IIPA's intended purpose nor its constitutionality.

a. Replacing the "Knowledge" Element

First, the IIPA must be amended to replace the "knowledge" element for those offenses relating to disclosures by government officials or personnel. As the offenses under § 421(a) and § 421(b) currently read, government "insiders" prosecuted under the IIPA must possess knowledge both "that the information disclosed so identifies [a] covert agent and that the United States is taking affirmative measures to conceal [that] covert agent's intelligence relationship to the United States."[174] This element is simply too demanding. In place of the "knowledge" element, a "reason to believe" standard should be substituted.

The current "knowledge" element places an excessive burden on the government when prosecuting "insiders" under the IIPA. As exemplified by the Plame affair, the prosecution was hesitant to use

172. *See supra* Part II.B.
173. *See* discussion *supra* Part II.B.
174. Intelligence Identities Protection Act of 1982, 50 U.S.C. § 421(a)-(b) (2006).

the IIPA due to skepticism that it could prove that there was requisite knowledge.[175] Fitzgerald had to prove first that Libby, or anyone else involved in the leak, knew that Plame was indeed "covert."[176] Even if Fitzgerald could have proven knowledge of Plame's "covert" status, the prosecution then had to demonstrate that Libby, or the others involved in the leak, knew that the government was taking "affirmative measures" to conceal her identity.[177] These became impossible tasks for the prosecution.[178]

By retaining the "knowledge" element, a claim of ignorance becomes a guilty defendant's best defense. A defendant can simply claim that he or she lacked positive knowledge that the disclosure identified a "covert agent" or that the United States was taking "affirmative measures" to conceal the exposed "covert agent's" identity. The difficulty in establishing knowledge is exacerbated by the ambiguity surrounding the terms "covert agent" and "affirmative measures."[179] Therefore, when claiming an ignorance defense, a culpable defendant may not even have to resort to dishonesty, because these terms are so convoluted that, in many situations, it is plausible that the ambiguity of the terms will prevent the defendant from possessing actual knowledge. Without demonstration of the requisite knowledge, an otherwise culpable defendant must be acquitted. To counter a claim of ignorance, the prosecution is left to rely upon only circumstantial evidence, as the existence of mere constructive knowledge must be evaluated using the defendant's public and private statements and any information available to and accessed by the defendant. Such evidence, however, is not easily discernible. Additionally, the government may have to go as far as proving motive to convince the fact-finder that the defendant had positive knowledge regarding the substance of the information disclosed. Given the gravity of the offense, this is an overly demanding standard for the government to meet, and it provides defendants with a simple escape route to bypass conviction.

---

175. *See supra* text accompanying notes 112-14.
176. *See* 50 U.S.C. § 421(a)-(b).
177. *See id.*
178. *See* Government's Sentencing Memorandum, *supra* note 98.
179. *See supra* text accompanying notes 102-14.

Further supporting the replacement of the "knowledge" element is that it is nearly impossible to demonstrate knowledge under a § 421(b) offense. This subsection addresses disclosures by government "insiders" who have access to classified information, but who are not cleared to access materials that directly identify case officers.[180] When a § 421(b) offense occurs, the identity of a case officer is typically inferred from an individual's access to other classified material.[181] Provided this inference, these government "insiders" will almost never possess positive knowledge that the identified case officer qualifies as a "covert agent."[182] Information pertinent to proving knowledge, including details of a case officer's assignments or a timeline of an officer's operational history, will not be directly accessible by this class of government "insiders."[183] As a result, proving the "knowledge" element in a § 421(b) offense is rare.

In place of the "knowledge" element, a less demanding "reason to believe" standard should be implemented. Replacing the "knowledge" element with a "reason to believe" standard will remove barriers to IIPA prosecutions and create realistic objectives for related criminal investigations. Under such a standard, prosecutors will have to prove that a reasonable person under the circumstances would have known that the disclosed information identified a "covert agent" and that the government was taking "affirmative measures" to conceal that identity.

There are three reasons why the "reason to believe" standard should prevail. First, the "reason to believe" standard is particularly well-suited for its application to government "insiders." Simply by working within the public sector and having interaction and familiarity with the intelligence apparatus, government "insiders" are innately aware of the sensitivity of the information they handle.[184] Consequently, before a government "insider" intentionally discloses potentially sensitive information, that individual is

180. *See supra* note 67 and accompanying text.

181. Francis, *supra* note 35, at 3-4.

182. *See id.* at 3 (stating that those with positive knowledge are principally case officers who have the ability to expose their colleagues).

183. *See id.* at 2 (explaining the most common ways individuals gain access to classified information).

184. *See supra* note 18 and accompanying text.

already on notice of the possible illegality of his or her actions.[185] This also holds true for the class of government "insiders" that § 421(b) addresses. Because the information from which these government "insiders" make an inference is classified, and because they are not cleared to access directly the sensitive material verifying their inference, these "insiders" must presume that disclosing this inference will be unlawful.[186] Substituting a "reason to believe" standard, therefore, will increase prudence when handling classified information, as reckless behavior will be punished. Government "insiders" will no longer be able to disregard their increased awareness for the sensitivity of the classified information they handle, thus resulting in fewer leaks. Second, Congress has already taken into account the heightened culpability of government "insiders" by subjecting them to more severe criminal penalties.[187] Such heightened culpability is correlative to an "insider's" increased awareness of the sensitivity of the classified information that was compromised.[188] Third, implementing the "reason to believe" standard under § 421(a) and § 421(b) is constitutionally sound,[189] especially given that the subsections do not apply to "outsiders." The "reason to believe" standard is already present in a § 421(c)

185. *See* United States v. Morison, 844 F.2d 1057, 1083 (4th Cir. 1988) (Wilkinson, J., concurring) (finding unpersuasive the defendant's claim that he was not on notice that his misuse of classified information may lead to prosecution, given that he was a trained government officer with a security clearance).

186. *See supra* notes 179-82 and accompanying text.

187. *Compare* Intelligence Identities Protection Act of 1982, 50 U.S.C. § 421(a)-(b) (2006), *with id.* § 421(c) (displaying that the severity of criminal penalties in each subsection decreases significantly when the perpetrator's access to the classified information containing the identities of case officers and awareness of the sensitivity of that material is reduced).

188. *See supra* notes 18, 179-80 and accompanying text.

189. Francis, *supra* note 35, at 9 (citing United States v. Bishop, 555 F.2d 771 (10th Cir. 1977); Schmeller v. United States, 143 F.2d 544 (6th Cir. 1944)) (explaining that the "reason to believe" standard has been upheld by courts against claims that it is unconstitutionally vague); *see also* Snepp v. United States, 444 U.S. 507, 509-10 (1980) (holding that, even in the absence of an express secrecy agreement, the government may act to protect substantial government interests, such as the identities of case officers, by imposing reasonable restrictions on current or former employees' activities that may, in other contexts, be protected by the First Amendment).

offense[190] and other espionage-related statutes.[191] This signifies that Congress is not opposed to lessening the standard.

By eliminating the "knowledge" element and substituting a "reason to believe" standard in § 421(a) and § 421(b), the IIPA will finally have complete authority to punish unauthorized disclosures by government "insiders" and hold a particular class of perpetrators responsible for their actions that, otherwise, go unpunished under the current framework. This will allow the IIPA to stop leaks at their source—government "insiders." Through the increased enforcement of leaks by "insiders," fewer unauthorized disclosures will make their way outside of the government. This reduction in unauthorized disclosures will compensate for the IIPA's inability, for constitutional reasons, to monitor "outsiders" as closely as it does government "insiders."[192]

b. Eliminating the "Pattern of Activities" Element

Second, abolishing the "pattern of activities" element of § 421(c)[193] will alleviate the narrowness of the IIPA. Requiring a "pattern of activities" allows certain deliberate and malicious unauthorized disclosures of case officers' identities to go unpunished.[194] This element, therefore, must be stricken from § 421(c).

The "pattern of activities" element places too many unauthorized disclosures of case officers' identities outside of the purview of the IIPA.[195] Under the current language, a single, isolated unauthorized disclosure by an "outsider" will go unpunished even though that individual knows that the information he or she reveals identifies a "covert agent" and the United States is taking "affirmative measures" to conceal that identity.[196] The IIPA defines a "pattern of

190. 50 U.S.C. § 421(c) ("Whoever ... intended to identify and expose ... with *reason to believe* that such activities would impair or impede the foreign intelligence activities of the United States." (emphasis added)).

191. Francis, *supra* note 35, at 9; *see, e.g.*, Internal Security Act of 1950, 50 U.S.C. § 783(a) (2006).

192. *See supra* note 121 and accompanying text.

193. 50 U.S.C. § 421(c).

194. *See* Bruce, *supra* note 116, at 47.

195. *Id.*

196. *See* Ferguson, *supra* note 53, at 488-89.

activities" as a "series of acts with a common purpose or objective."[197] Therefore, once an unauthorized disclosure of a case officer's identity occurs, prosecutors must wait for evidence of multiple acts by the "outsider," all of which must relate to the unauthorized disclosure, before they can pursue IIPA charges. A single disclosure, unrelated to any pattern, however, can be calamitous in itself.[198] If classified information is in the wrong hands, then requiring the occurrence of numerous acts allows for the exposure of additional case officers' identities before law enforcement officials can intervene. Furthermore, the amount of harm that an "outsider" can cause during the course of an investigation to uncover a "pattern of activities" surrounding that individual's initial exposure may be catastrophic.[199] If several individuals or means of publication are involved, the time it takes for investigators to discover that numerous acts or disclosures are associated with an initial unauthorized disclosure could render the IIPA impotent. Given recent advancements in communication technologies, investigators, in many situations, may never be able to discover and link numerous acts or disclosures together. For these reasons, the "pattern of activities" element must be eliminated.

Although striking the "pattern of activities" element will enable more prosecutions, this change will neither chill the rights and freedoms of "outsiders" nor discourage their lawful activity. Prosecutors still must prove four key elements. First, the government must show that there was an intent "to identify and expose covert agents."[200] Second, the government must demonstrate that the "outsider" had a reasonable belief that his or her actions "would impair or impede the foreign intelligence activities of the United States."[201] Third, the government must display that the "outsider" knew the disclosed information identified a "covert agent."[202] Fourth, the government must prove that the "outsider" knew that

197. 50 U.S.C. § 426(10).

198. *See* Bruce, *supra* note 116, at 47.

199. *See id.*

200. 50 U.S.C. § 421(c).

201. *Id.*

202. *Id.* This is in contrast to the "reason to believe" standard proposed for the prosecution of "insiders" under § 421(a) and § 421(b). *See supra* Part III.B.2.a.

the U.S. government was "taking affirmative measures to conceal" that identity.[203] As displayed in cases involving government "insiders," proving the "knowledge" element can be nearly impossible.[204] When applied to "outsiders," this evidentiary burden is increased considerably, as information pertinent to proving knowledge will never be directly available to any "outsider."[205] For these reasons, the government is currently prevented from charging "outsiders" under the IIPA for any or every unauthorized disclosure.

Abolishing the "pattern of activities" requirement will expand the IIPA's application and enable it to be utilized swiftly, thereby restricting the number and effect of unauthorized disclosures of case officers' identities. Allowing for such an amendment will effectuate these positive results without senselessly restricting the activities of the media and other "outsiders." Together, deleting the "pattern of activities" element and replacing the "knowledge" element with a "reason to believe" standard will serve to ease the narrowness of the IIPA, which will facilitate its enforcement and allow the IIPA to fulfill its purpose of protecting case officers' identities regardless of the source or means of disclosure.

C. Addressing the Other Factors

Properly amending the IIPA by expanding the class of protected persons and easing the narrowness of its offenses addresses only one factor, albeit the most significant factor, contributing to its limited application. As compared to the external measures that can resolve the IIPA's inherent limitations, addressing the two other factors—the availability of the Espionage Act[206] and a lack of political initiative in enforcing the IIPA[207]—is possible from only internal advancements within the executive branch.

---

203. 50 U.S.C. § 421(c).

204. This is especially true in § 421(b) offenses. *See supra* Part III.B.2.a.

205. Such information includes details of a case officer's assignments and/or timeline of operational history. *See supra* text accompanying note 182.

206. *See supra* Part II.A.

207. *See supra* Part II.C.

With regard to the availability of the Espionage Act, it is clear that there will be a natural limitation on the IIPA's use.[208] Prosecutors, however, must realize that a revamped IIPA can serve as a valuable lesser-included offense to espionage, when applicable. For example, the IIPA can be particularly useful in plea-bargaining situations or when charges of espionage are weak. Under the proper circumstances, simply charging perpetrators with IIPA offenses will alert the public to this law, allowing it to become a deterrent to the unauthorized disclosure of case officers' identities.

Conversely, addressing the lack of political initiative in enforcing the IIPA requires discussion of three issues: (1) concerns regarding the IIPA's constitutionality, (2) fear that pursuing IIPA charges will lead to the disclosure of further classified information during trial, and (3) the desire to use unauthorized disclosures as a means of influencing policy.[209] First, prosecutors must not let potential concerns regarding the IIPA's constitutionality deter its use. This Note does not seek to provide a comprehensive discussion of the IIPA's constitutionality, as previous articles have already done so.[210] Until the courts are afforded an opportunity to comment on the IIPA, there is nothing further to discuss on the subject. From a cursory perspective, however, prosecutors must not let this issue control their decisions to use the IIPA. Given its meticulous drafting and the lengthy discussion over its language, both of which are documented in its legislative history,[211] it must be presumed that the IIPA is constitutionally sound. One of the legal scholars summoned to comment on the IIPA was then professor and current U.S. Supreme Court Justice Antonin G. Scalia.[212] At the time, Justice

---

208. *See supra* Part II.A.

209. *See supra* Part II.C.

210. *See* sources cited *supra* note 121.

211. Debate over such a measure lasted for more than five years with fifteen bills drafted over that period. *See supra* note 53 and accompanying text. Numerous interest groups participated in congressional testimony concerning the final bill, including the Society of Professional Journalists, the American Civil Liberties Union, and the American Bar Association Committee on Freedom of Expression. *See* Ferguson, *supra* note 53, at 484-85. Following these comments and lengthy debate, Congress felt so confident about the soundness of the measure that it overwhelmingly approved the bill. *See supra* notes 54, 122 and accompanying text.

212. *See* Thomas S. Blanton, Op-Ed., *Keeping Secrets at Too High a Price*, N.Y. TIMES, Aug. 22, 2001, at A19.

Scalia concluded, "'the necessity of this particular, narrow category of disclosure to the free and open political debate which the [F]irst [A]mendment is intended primarily to assure' is 'negligible.'"[213] Supporting Justice Scalia's analysis are several legal decisions, which have restricted individuals' ability to disseminate information and deferred to the executive branch's measures to maintain secrecy when the information involves issues of national security.[214] Moreover, the constitutionality issue confronts only § 421(c) offenses involving "outsiders," not § 421(a) or § 421(b) offenses covering government "insiders."[215] Concerns about constitutionality, therefore, should not be a factor in enforcing the IIPA against government officials or personnel. Continued inaction due to constitutional concerns makes the IIPA no more effective than if it did not exist at all. Second, government officials must continue to carefully calculate the risk that further classified information could be disclosed during an IIPA trial.[216] When doing so, however, both prosecutors and the affected agency must jointly conduct a cost-benefit analysis, with the possibility of further disclosures not being the sole determinant in enforcing the IIPA.[217] Congress has reiterated that, in most circumstances, the CIPA will be effective in lessening the

---

213. *Id.*

214. *See generally, e.g.*, CIA v. Sims, 471 U.S. 159 (1985) (upholding the DCI's refusal to allow disclosure of records containing intelligence sources); Haig v. Agee, 453 U.S. 280 (1981) (holding that unauthorized disclosures of classified information, specifically case officers' identities, are not protected by the Constitution, even if those exposures are part of a larger critique of the government); Snepp v. United States, 444 U.S. 507 (1980) (holding that intelligence agencies can act to protect the secrecy of national security information and the appearance of constitutionality by imposing reasonable restrictions on employees' activities that in other contexts may be protected by the First Amendment); Near v. Minnesota, 283 U.S. 697 (1931) (holding that the freedoms of speech and press are not absolute, as the government may restrict publication of information relating to the number and location of troops); United States v. Morison, 844 F.2d 1057 (4th Cir. 1988) (holding that the First Amendment does not prohibit prosecutions for unauthorized leaks of damaging national security information); Halperin v. CIA, 629 F.2d 144 (D.C. Cir. 1980) (holding that the legislative and executive branches have discretion, nonreviewable by the judiciary, to require secrecy regulations involving restricting the dispersal of classified information).

215. *See supra* note 121 and accompanying text.

216. *See supra* text accompanying notes 126-28.

217. INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 1997, H.R. REP. NO. 104-832, at 35 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4000.

risks of a trial.[218] Third, the desire to use unauthorized disclosures as a means of influencing policy will dissipate if the IIPA is properly amended. With a stronger law in place, the executive branch will no longer have an excuse for failing to monitor itself. Political pressure to enforce a viable and effective IIPA will eventually lead to fewer exposures of case officers' identities. Although the lack of political initiative in enforcing the IIPA can be rectified, it requires the executive branch to take the initiative to address each of these three issues influencing its behavior.

CONCLUSION

The intended purpose of the IIPA is commendable; yet its application and enforcement have been disappointing. For over twenty-five years, the IIPA has been disguised as an important safety mechanism for the protection of case officers' identities. Its existence, however, has been marked by ineffectiveness. Since its inception in 1982, the IIPA has been enforced only once, while going overlooked in numerous instances when case officers' identities were unlawfully exposed. Unless the IIPA is significantly amended now, it risks becoming obsolete.

Although the IIPA has been a disappointment to the intelligence community, it remains a necessary protective device in preventing unauthorized disclosures of the most sensitive classified information—case officers' identities. Upon discovering the three factors contributing to its limited application, it is clear that the IIPA must be amended in order to serve its intended purpose and ensure its vitality. Lessons from the Plame affair indicate that an IIPA amendment must address two primary issues—expanding the class of protected persons and easing the narrowness of its offenses. By properly amending the IIPA, its inherent limitations can be resolved. This added strength will allow it to overcome the remaining two factors limiting its application, thus creating a valuable tool for law enforcement.

---

218. *See id*. *But see* Bruce, *supra* note 116, at 47 (arguing that better protection is needed than presently afforded by the CIPA).

The IIPA must become an attractive option for prosecutors so that it can punish and deter deplorable activity. The men and women who place their lives in daily peril while serving their country abroad deserve sincere advocates at home who are willing to provide them with adequate protection. If these critical amendments are implemented, then the IIPA can finally achieve its potential and fulfill the aspirations of its creators and those it is intended to protect.

Andrew M. Szilagyi[*]

* J.D. candidate 2010, William & Mary School of Law; B.A. 2007, Baldwin-Wallace College. I would like to recognize my parents, Bruce and Becky, for their unyielding support. In addition, I wish to extend my sincere gratitude to the numerous members of the academic and intelligence communities whom I consulted for their comments and advice in this endeavor. Finally, I would like to thank the members of the *William and Mary Law Review* for their assistance in improving my Note.