

Boston College Law School

Digital Commons @ Boston College Law School

Boston College Law School Faculty Papers

2-27-2008

Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information

Mary-Rose Papandrea

Boston College Law School, papandrm@bc.edu

Follow this and additional works at: <https://lawdigitalcommons.bc.edu/lspf>



Part of the [Constitutional Law Commons](#), [First Amendment Commons](#), [National Security Law Commons](#), [President/Executive Department Commons](#), and the [Social Influence and Political Communication Commons](#)

Recommended Citation

Mary-Rose Papandrea. "Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information." *Indiana Law Journal* 83, no.1 (2008): 233-306.

This Article is brought to you for free and open access by Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law School Faculty Papers by an authorized administrator of Digital Commons @ Boston College Law School. For more information, please contact abraham.bauer@bc.edu.

Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information

MARY-ROSE PAPANDREA*

In the United States, the executive branch possesses virtually unbridled authority to keep national security information from the public. Although the Freedom of Information Act and whistleblower protection laws serve as some check on the executive's power, these tools remain largely ineffectual. Because the desire for tight information control competes with the demands of newsgathering, a "game of leaks" has developed among government officials and reporters in which the press alternatively serves as lapdogs, watchdogs, and scapegoats for the executive branch.

This Article demonstrates that the government has been communicating information to the public through leaks ever since the administration of President Theodore Roosevelt. Legal developments in the current climate, including the ongoing prosecution of two lobbyists for violations of the Espionage Act in the American-Israeli Public Affairs Committee case, have the potential to establish precedents that could impose dire consequences upon this crucial information flow. This Article scrutinizes the constitutionality of prosecuting nongovernmental parties for the publication of classified information by examining the long and complicated history of the relationship between the press and the executive branch, and the role leaks play in the dissemination of classified information to the public today.

After examining the relationship between the press and the executive branch, as well as tracing the development of the reasoning behind the applicable First Amendment doctrine, this Article ultimately argues that in any prosecution against a nongovernmental actor for disseminating national security information, the government must demonstrate not only that the disclosure posed an immediate, serious, and direct threat to national security, but also that the offender either intended the disclosure to harm the United States or help a foreign nation, or that the offender was recklessly indifferent to the harm that the disclosure would cause. Given that the executive branch has so much power to control the dissemination of national security information to the public, and itself leaks information to support its agenda, its power to punish the publication of leaks must be extremely limited. An intent requirement is consistent with the Supreme Court's free speech jurisprudence and helps achieve this goal.

An intent requirement will encourage the government and the press to continue their historical cooperation when the publication of certain information poses a serious threat to national security interests. It will create an incentive for government officials to explain their national security concerns to the press, and it will simultaneously hold the press accountable for any reckless disregard shown toward genuine threats. This approach seeks to strike the proper balance between the

* Assistant Professor, Boston College Law School. I would like to thank David Ardia, William Banks, Michael Cassidy, Lawrence Cunningham, Brian Murchison, Diane Ring, Geoffrey Stone and the workshop participants at the Syracuse University College of Law for their thoughtful comments and suggestions on earlier drafts of this Article. I would also like to thank Daniel McFadden, Ronaldo Rauseo-Ricupero, and Shaileen Stillmank for their invaluable research assistance. A summer research grant from the Boston College Law School Fund made this project possible.

executive branch's vast ability to control the dissemination of national security information to the public—often through calculated leaks—and the need to maintain the secrecy of information that is truly sensitive.

INTRODUCTION.....	234
I. EXECUTIVE BRANCH CONTROL OF NATIONAL SECURITY INFORMATION.....	238
A. <i>The Conflict Between the Democratic Demand for Openness and Need for Secrecy</i>	238
B. <i>Executive Means of Information Control</i>	240
II. THE GAME OF LEAKS.....	248
A. <i>History of Leaks</i>	249
B. <i>Controlling Leaks</i>	255
C. <i>A Generally Responsible Press</i>	257
III. THE CURRENT STATUTORY REGIME.....	262
A. <i>No Official Secrets Act</i>	262
B. <i>The Espionage Act</i>	263
C. <i>Atomic Energy Act</i>	270
D. <i>Intelligence Identities Protection Act</i>	274
E. <i>Federal Larceny Statute</i>	277
F. <i>Inchoate Liability Provisions</i>	277
IV. CURRENT FIRST AMENDMENT DOCTRINE.....	278
A. <i>Speech Concerning National Security Information is Protected Speech</i>	278
B. <i>The Pentagon Papers Case</i>	279
C. <i>First Amendment Rights of Government Employees</i>	281
D. <i>Newsgathering Rights</i>	283
E. <i>Protection for the Publication of “Lawfully Acquired” Information</i>	286
F. <i>Constitutional Analysis in United States v. Morison and United States v. Rosen</i>	296
V. STRIKING THE BALANCE: REQUIRE INTENT AND ELIMINATE INCHOATE LIABILITY.....	298
A. <i>Requiring Intent to Any Prosecution for the Disclosure of National Security Information</i>	298
B. <i>Drawing the Line Against Inchoate Liability</i>	303
CONCLUSION.....	305

INTRODUCTION

In December 2005, the *New York Times* published a story revealing that the National Security Administration (NSA) had been secretly engaging in domestic eavesdropping without obtaining a search warrant as federal law requires.¹ In response, President Bush made no apologies for circumventing the Foreign Intelligence Surveillance Act (FISA), and instead called the leak of the program's existence “a shameful act.”² Other critics went so far as to declare the *New York Times* guilty of

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

2. David Stout, *Bush Says U.S. Spy Program Is Legal and Essential*, N.Y. TIMES, Dec. 19, 2005, at A1.

treason.³ Three months later, Gabriel Schoenfeld, a senior editor at *Commentary* magazine, published an article arguing that the Department of Justice has statutory authority under the Espionage Act to prosecute the *New York Times* for the publication of the NSA story.⁴ Soon after, as if heeding this call to arms, Attorney General Gonzales convened a grand jury to investigate who leaked the NSA story to the press, and indicated on ABC's news program "This Week" that the Department of Justice is considering the possibility of bringing criminal prosecutions against reporters who publish classified information.⁵ Although no such charges have been brought, the Bush Administration's reaction to the *New York Times* publication decision has led some to declare that this Administration is waging a war on the press.⁶

Such charges are well founded. The pending prosecution of two lobbyists for violations of the Espionage Act has the potential to establish precedent to support the constitutionality of a prosecution against the press. The defendants in the case, Steven Rosen and Keith Weissman, are former lobbyists for the American Israel Public Affairs Committee (AIPAC)⁷ in Washington, D.C., and they are currently under indictment for allegedly violating the Espionage Act by conspiring to transmit national defense information to those "not entitled to receive it."⁸ The indictment charges that Rosen and Weissman cultivated a relationship with Lawrence Franklin, a former Department of Defense employee, and other government officials in order to gather classified national defense information pertaining to U.S. policy in the Middle East. Rosen and Weissman in turn transmitted the information to members of the media, foreign policy analysts, and foreign officials.⁹ Rosen faces an additional charge of aiding and abetting Franklin's illegal disclosure of classified national security information by providing a fax machine on which to receive Franklin's

3. Rachel Smolkin, *Judgment Calls*, AM. JOURNALISM REV., Oct.–Nov. 2006, at 22, 23–24.

4. Gabriel Schoenfeld, *Has the "New York Times" Violated the Espionage Act?*, COMMENT., Mar. 2006, at 23, 31.

5. *This Week* (ABC television broadcast May 21, 2006); see Scott Shane, *Leak of Classified Information Prompts Inquiry*, N.Y. TIMES, July 29, 2006, at A10.

6. Eric Alterman, *Bush's War on the Press*, THE NATION, May 9, 2005, at 11; Dan Eggen, *White House Trains Efforts on Media Leaks*, WASH. POST, Mar. 5, 2006, at A1 (quoting *New York Times* Executive Editor Bill Keller as saying "I don't know how far action will follow rhetoric, but some days it sounds like the administration is declaring war at home on the values it professes to be promoting abroad"); Interview by *Frontline* with James Goodale, First Amendment Attorney (PBS television broadcast Oct. 18, 2006) (transcript available at <http://www.pbs.org/wgbh/pages/frontline/newswar/interviews/goodale.html>) ("The Bush administration, in my humble view, has waged a war against the press, and using the Espionage Act is part of its program to wage that war.").

7. AIPAC lobbies Congress and the executive branch on issues of interest to Israel, including the United States's foreign policy in the Middle East. See *What is AIPAC?*, http://www.aipac.org/about_AIPAC/default.asp.

8. *United States v. Rosen*, 445 F. Supp. 2d 602, 607–08 (E.D. Va. 2006).

9. *Id.* at 609. Franklin has already pleaded guilty to conspiracy to communicate national defense information to one not entitled to receive it, in violation of 18 U.S.C. §§ 793(d) and (g), and to conspiracy to communicate classified information to an agent of a foreign government in violation of 50 U.S.C. § 783 and 18 U.S.C. § 371. *Rosen*, 445 F. Supp. 2d at 608 n.3.

communications.¹⁰ The district court judge presiding over the case held that the First Amendment posed no bar to the prosecutions.¹¹

Although no media outlet or reporter has been indicted in connection with the AIPAC case, and the Department of Justice has publicly denied that it is trying to establish precedent that could be used later against the press, the mainstream media is reasonably concerned that the next Espionage Act prosecution could be directed at them.¹² There is no coherent way of distinguishing between the “press” and the lobbyists who have been indicted in the AIPAC case, either as a statutory matter or as a constitutional matter under current First Amendment case law. If it is constitutional to prosecute a lobbyist for obtaining and communicating national defense information that he received from a source, there is nothing aside from prosecutorial discretion to stop the prosecution of the press for doing the same thing. Reporters routinely gather classified information from government officials and transmit that information to others not entitled to receive it, whether it be to their editors or, if published, to the American public.¹³ Furthermore, the most disturbing aspect of the AIPAC case for future media defendants is the aiding and abetting charge. It takes little imagination to see the dangers the press would face if prosecutors decided to bring such charges against reporters who knowingly receive leaked classified information, much less reporters who actively cultivate their sources. Criminal prosecutions based on the acquisition or publication of information would have a dire chilling effect on the press and would necessarily involve an unwarranted intrusion into their information-gathering processes. The AIPAC case and the Attorney General’s thinly veiled threats to prosecute the press have brought a number of constitutional questions to the forefront, and current First Amendment doctrine fails to offer clear answers.

This Article argues that any inquiry into the appropriate constitutional standard must first examine the complicated relationship between the executive branch and the press, particularly with respect to national security information. Under our current system, the executive branch is given virtually unbridled classification authority to keep information out of the public eye. Although the Freedom of Information Act and whistleblower protection laws serve as checks on the executive’s power over information, these checks are largely ineffectual in the context of national security information. As a result of the executive’s control over national security information, a “game of leaks” has developed among government officials and employees and the press. During this game, the press alternatively serves as lapdogs, watchdogs, and scapegoats for the executive branch. The press depends upon the government for news; the government in turn depends upon the press to communicate with the public. Ever since President Theodore Roosevelt, who was the first President to consciously use anonymous leaks to his political advantage, leaks of classified information, including classified national security information, have become one of the primary ways the government communicates information to the public. The press has been largely

10. *Id.* at 607–08, 644.

11. *Id.* at 637.

12. See Dorothy Rabinowitz, *First They Came for the Jews: A Prosecution Under the Espionage Act Threatens the First Amendment*, WALL ST. J., Apr. 2, 2007, at A1 (arguing that if the AIPAC prosecution is successful, the press has every reason to fear that it could be next).

13. E.g., Fred Kaplan, *You’re a Spy*, SLATE, Feb. 15, 2006, <http://www.slate.com/id/2136324>.

cooperative and responsible; if anything, history demonstrates that it has been *too* willing at times to engage in self-censorship in times of war. The perjury prosecution of Scooter Libby indicates that the game of leaks can be sloppy and imperfect, but the reality is that this is the system of information control and dissemination in the United States.

This Article ultimately argues that any prosecution against a nongovernmental actor for disseminating national security information must satisfy a rigorous intent standard. Given that the executive branch has so much power to control the dissemination of national security information to the public, and itself leaks information to support its agenda, its power to punish the publication of leaks must be extremely limited. This Article argues that in any prosecution for the disclosure of classified national security information, the government should be required to prove that the individual acted either with intent to harm the United States or help a foreign nation, or with reckless indifference to whether the release of information would have that result.

An intent standard would encourage the government and the press to continue their historical cooperation concerning when the publication of certain information would harm legitimate national security interests. The hope is that this approach will strike the proper balance between the Executive's vast ability to control the dissemination of national security information to the public—often through calculated leaks—and the need to maintain the secrecy of truly sensitive information. A corollary conclusion of this Article is that prosecutions against nongovernmental actors for inchoate crimes of conspiracy and aiding and abetting violations of the Espionage Act and related laws violate the First Amendment because they are backdoor attempts to punish the publication of classified information in situations when a prosecution based on publication would be impermissible.

Part I discusses the vast and largely unchecked control the executive branch enjoys over national security information. Part II discusses the complicated “game of leaks” the executive branch and the press play on a daily basis. This Part includes a summary of the various methods the government has to prevent, control, and punish the unauthorized dissemination of national security information. Part III discusses the protection the First Amendment provides for those who engage in the unauthorized disclosure of national security information, whether to the press, public, or agents of a foreign country. Part IV analyzes the scope and constitutionality of the current statutory regime prohibiting the disclosure of national security information. Part V concludes that, as a matter of policy and First Amendment doctrine, any statute that authorizes the prosecution of an unrelated third party for the publication of national security information must require not only that the disclosure caused immediate, serious, and direct harm to national security, but also that the offender acted with an intent to harm the United States or advantage a foreign nation, or with reckless indifference to any such harm.

I. EXECUTIVE BRANCH CONTROL OF NATIONAL SECURITY INFORMATION

A. *The Conflict Between the Democratic Demand for Openness and Need for Secrecy*

As many judges, scholars, and legal philosophers have noted, an open government is essential to the democratic political process.¹⁴ The public's right to receive information about government affairs is rooted in democratic theory. In a democracy, the public is the true sovereign, and elected officials are their agents. As Alexander Meiklejohn, the foremost theorist of the democratic basis of the First Amendment, explained, "[p]ublic discussions of public issues, together with the spreading of information and opinion bearing on those issues, must have a freedom unabridged by our agents. Though they govern us, we, in a deeper sense, govern them. Over our governing, they have no power. Over their governing we have sovereign power."¹⁵

The democratic principles of open government have often clashed with the Executive's asserted need for secrecy in diplomatic and military affairs. Patrick Henry, who once said that "[Congress] may carry on the most wicked and pernicious schemes under the dark veil of secrecy,"¹⁶ recognized that not all government activities could be publicized, such as "military operations or affairs of great consequence."¹⁷ Thomas Jefferson agreed, explaining that "[a]ll nations have found it necessary, that for the advantageous conduct of their affairs, some [private] proceedings, at least, should remain known to their executive functionary only."¹⁸ The Supreme Court has repeatedly noted the importance of keeping intelligence operations secret in order to protect their effective operation.¹⁹

The United States Constitution lacks any specific provisions concerning secrecy in the executive branch. The only mention of secrecy occurs in Article I in a provision

14. *E.g.*, *N.Y. Times Co. v. United States*, 403 U.S. 713, 724 (1971) (Douglas, J., concurring) ("Secrecy in government is fundamentally anti-democratic, perpetuating bureaucratic errors. Open debate and discussion of public issues are vital to our national health."). See generally HAROLD L. CROSS, *THE PEOPLE'S RIGHT TO KNOW: LEGAL ACCESS TO PUBLIC RECORDS AND PROCEEDINGS* (1953); ALEXANDER MEIKLEJOHN, *FREE SPEECH AND ITS RELATIONSHIP TO SELF-GOVERNMENT* (1948); JOHN RAWLS, *A THEORY OF JUSTICE* 224–25 (1971); Vincent Blasi, *The Checking Value in First Amendment Theory*, 3 AM. B. FOUND. RES. J. 523, 554–67 (1977).

15. Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245, 257 (1961).

16. 3 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION AS RECOMMENDED BY THE GENERAL CONVENTION AT PHILADELPHIA IN 1787, at 170 (Jonathan Elliot ed., New York, Burt Franklin 1888).

17. *Id.*

18. 3 HENRY S. RANDALL, *LIFE OF THOMAS JEFFERSON* 211 (1858), reprinted in JAMES RUSSELL WIGGINS, *FREEDOM OR SECRECY* 67 (1964).

19. *E.g.*, *Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980) (per curiam) (noting that "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"); *United States v. Curtiss-Wright Corp.*, 299 U.S. 304, 320 (1936) ("Secrecy in respect of information gathered by [the Executive's diplomatic and consular officials] may be highly necessary, and the premature disclosure of it productive of harmful results.").

requiring the House and Senate to keep journals of their proceedings and to publish them “from time to time . . . excepting such Parts as may in their Judgment require Secrecy.”²⁰ In the absence of specific constitutional authority, presidents tend to draw on structural arguments as justification for the right to keep information secret, arguing that effective military actions, foreign policy, and diplomatic relations cannot be conducted without some ability to control information.²¹

Indeed, there is evidence that some framers thought secrecy was essential to the conduct of government affairs. For example, Alexander Hamilton said that the Constitution would not have been ratified if the Convention had been open to the public because “the clamours of faction would have prevented any satisfactory result.”²² In addition, the public had only limited access to the Bill of Rights debates, and the Senate met in secret for the first five years.²³

No one disputes that the public release of *some* information could pose a significant threat to our national security and diplomatic relations and undermine the government’s duty to provide for the common defense. That said, democratic principles of self-government do not lose their force whenever the government asserts a national security interest in secrecy. Information concerning national security and foreign policy is necessary for citizens to engage in meaningful debate of important public issues. Permitting the government to limit what information the public is given threatens the democratic process. As Harold Koh has explained, “the National Security Constitution requires that the public, as well as Congress, receive as much information as is necessary to evaluate the wisdom and legality of executive conduct.”²⁴ Since the Vietnam War it has been a matter of concern “whether the public and Congress receive enough information about defense and foreign policy matters to be able to influence policy decisions and to exercise an effective external check on the power of the executive.”²⁵ There are no more important issues than the defense and security of our nation, and decisions in this area affect everyone in our society.²⁶ This is true even more in the age of terrorism as the government demands that the public give up many of its civil liberties, especially its right to privacy.

As a result of the tension between the Executive’s asserted need for secrecy and the democratic requirements of openness and transparency, the government and the press

20. U.S. CONST., art. I, § 5, cl. 3.

21. See, e.g., *Curtiss-Wright*, 299 U.S. at 319–21.

22. Alexander Hamilton, *Reply to Anonymous Charges*, in 3 THE RECORDS OF THE FEDERAL CONVENTION 1787, at 368 (Max Farrand ed., 1966).

23. Martin E. Halstuk, *Policy of Secrecy—Pattern of Deception: What Federalist Leaders Thought About a Public Right to Know, 1794–98*, 7 COMM. L. & POL’Y 51, 59 (2002) (citing Margaret Blanchard, *Freedom of the Press*, in THE MEDIA IN AMERICA: A HISTORY 108 (William David Sloan & James G. Stovall eds., 1989)). Congress has occasionally conducted secret sessions, typically during impeachment deliberations and discussions of national security issues and confidential information. See generally MILDRED AMER, CONG. RESEARCH SERV., SECRET SESSIONS OF CONGRESS: A BRIEF HISTORICAL OVERVIEW (2004), <http://www.fas.org/sgp/crs/RS20145.pdf>.

24. HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION 201 (1990).

25. Note, *Developments in the Law: The National Security Interest and Civil Liberties*, 85 HARV. L. REV. 1130, 1190 (1972).

26. *United States v. Morison*, 844 F.2d 1057, 1081 (4th Cir. 1988) (Wilkinson, J., concurring).

enjoy an uneasy and complicated relationship. During wartime and other times of crisis, this tension frequently comes to a head. At these times, the government would love to have more—not less—control over the press. When fighting the enemy, the ability to control the flow of information to the public can serve as a means to bolster military and civilian morale, undermine the confidence of our enemies, increase enlistments in our military forces, and perhaps even bring a quicker end to hostilities.²⁷

B. Executive Means of Information Control

The executive branch has virtually unbridled power to control the flow of national security information to the public. The classification system is the executive branch's principal method of information control,²⁸ although it may also attempt to shroud its actions by asserting the executive privilege²⁹ or the state secret doctrine³⁰ or by generally invoking a need for secrecy for its actions.³¹

27. MICHAEL SWEENEY, *THE MILITARY AND THE PRESS: AN UNEASY TRUCE* 5 (2006).

28. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 985 (1973).

29. *See, e.g.*, *Cheney v. U.S. Dist. Court for D.C.*, 542 U.S. 367 (2004) (suggesting that courts may act independently to preserve executive confidentiality when executive privilege has not yet been asserted); *Nixon v. Admin. of Gen. Servs.*, 433 U.S. 425, 454–55 (1977) (concluding Presidential Recordings and Materials Preservation Act did not violate the presidential privilege of confidentiality); *United States v. Nixon*, 418 U.S. 683, 713 (1974) (recognizing a qualified executive privilege); *In re Sealed Case*, 121 F.3d 729, 751–52 (D.C. Cir. 1997) (concluding that the presidential communications privilege extends to communications made by presidential advisors in the course of preparing advice for the President, even when the President is not personally involved in the communication); *see also* Mark J. Rozell, *Executive Privilege and the Modern Presidents: In Nixon's Shadow*, 83 MINN. L. REV. 1069 (1999) (discussing the invocation of the executive privilege in the post-Watergate era).

30. *See, e.g.*, *Tenet v. Doe*, 544 U.S. 1 (2005) (reaffirming the existence of the state secrets doctrine); *United States v. Reynolds*, 345 U.S. 1 (1953) (explicitly recognizing the state secret doctrine); *ACLU v. NSA*, 493 F.3d 644 (6th Cir. 2007) (holding that state secrets privilege prevented plaintiffs from establishing standing to challenge NSA warrantless surveillance program); *In re Sealed Case*, 494 F.3d 139 (D.C. Cir. 2007) (concluding that state secrets doctrine did not mandate dismissal of government employee's claim that another government employee engaged in electronic eavesdropping of plaintiff's telephone conversation in violation of the Fourth Amendment); *El-Masri v. United States*, 479 F.3d 296 (4th Cir. 2007) (affirming dismissal of challenge to extraordinary rendition on basis of state secret doctrine), *cert. denied*, 128 S. Ct. 373 (2007); *United States v. Adams*, 473 F. Supp. 2d 108, 123 (D. Me. 2007) (enjoining Maine Public Utilities Commission from pursuing contempt proceedings against a telecommunications company that refused to disclose whether or not it provided information to the NSA); *Al-Haramain Islamic Found., Inc. v. Bush*, 451 F. Supp. 2d 1215 (D. Or. 2006) (rejecting government's state secrets claim in case challenging NSA warrantless surveillance program), *rev'd* 507 F.3d 1190 (9th Cir. 2007); *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899 (N.D. Ill. 2006) (granting government's motion to dismiss challenge to NSA wiretapping program on state secrets grounds); *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (rejecting government's state secrets claim in case alleging that AT&T collaborated with the NSA's warrantless surveillance program); *see also* Amanda Frost, *The State Secret Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931 (2007) (arguing that the state secrets doctrine undermines the executive oversight power of Congress). Congress is considering

Until the New Deal, military regulations governed classification determinations.³² In 1940, President Franklin Roosevelt issued an executive order expressly recognizing the classification system.³³ In issuing the order, he relied on statutory authority, the Espionage Act of 1938, which authorized him to specify military and naval installations and equipment for protection.³⁴ In 1951, President Truman issued an executive order extending classification authority to all executive agencies—military and nonmilitary alike—when they deemed secrecy necessary in the interest of “national security,”³⁵ a broader and more elastic concept that replaced the “national defense” standard under President Roosevelt.³⁶ Unlike President Roosevelt, Truman based his authority for the classification system on inherent executive authority rather than statutory authority from Congress.³⁷ When President Eisenhower took office, he responded to concerns about the breadth of the classification system by reducing the number of executive agencies with classification authority, reinstating the “national defense” standard, narrowing the criteria for classification, and instituting review of classification decisions.³⁸

Under the current Executive Order, information may be classified if the unauthorized disclosure of the information “reasonably could be expected” to damage national security.³⁹ Information may be classified at one of three levels.⁴⁰ The three

whether to codify and standardize the application of the privilege. *See* State Secrets Protection Act, S. 2533, 110th Cong. (2008).

31. *E.g.*, Press Release, President Signs Intelligence Authorization Act, Statement by the President (Dec. 28, 2001), <http://www.whitehouse.gov/news/releases/2001/12/20011228-3.html> (asserting President has constitutional authority to withhold from Congress information the disclosure of which could impair foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive’s constitutional duties).

32. NATHAN BROOKS, CONG. RESEARCH SERV., THE PROTECTION OF CLASSIFIED INFORMATION: THE LEGAL FRAMEWORK 1 (2004), <http://www.firstamendmentcenter.org/pdf/CRS.security4.pdf>.

33. Exec. Order No. 8381, 5 Fed. Reg. 1147 (Mar. 22, 1940).

34. Espionage Act of 1938, ch. 2, § 1, 52 Stat. 3. President Roosevelt interpreted “equipment” broadly to include documents held by the Secretaries of War and the Navy. *See Developments in the Law*, *supra* note 25, at 1194.

35. Exec. Order No. 10,290, 16 Fed. Reg. 9795 (Sept. 27, 1951).

36. HAROLD C. RELYEA, CONG. RESEARCH SERV., SECURITY CLASSIFIED AND CONTROLLED INFORMATION: HISTORY, STATUS, AND EMERGING MANAGEMENT ISSUES 3 (2007), <http://www.fas.org/sgp/crs/secrecy/RL33494.pdf>.

37. Exec. Order No. 10,290, *supra* note 35; *see also* Christina Wells, *Information Control in Times of Crisis: The Tools of Repression*, 30 OHIO N.U. L. REV. 451, 454–57 (2004) (outlining the history of the classification system). The Supreme Court eventually agreed that the Executive has inherent authority to classify information and withhold it from the public. *Dep’t of the Navy v. Egan*, 484 U.S. 518, 527 (1988).

38. Wells, *supra* note 37, at 456; RELYEA, *supra* note 36, at 3.

39. Exec. Order No. 13,292, § 1.1, 68 Fed. Reg. 15,315, 15,315 (Mar. 25, 2003). Such information includes:

military plans, weapons systems, or operations; foreign government information; intelligence activities, intelligence sources/methods, cryptology; foreign relations/activities of the United States; scientific, technological, or economic matters relating to national security; federal programs for safeguarding nuclear materials or facilities; vulnerabilities or capacities of national security systems; or weapons of mass destruction.

Id. at § 1.4.

levels of classification depend upon the level of danger the disclosure could be expected to cause. Information designated as “top secret” is such that its disclosure could reasonably be expected to cause “exceptionally grave damage” to national security, whereas the disclosure of “secret” information would cause “serious damage,” and “confidential” information would merely cause “damage.”⁴¹ When classifying information, the classifying officer must specify the danger the disclosure of the information might cause. The officer must attempt to set a date for declassification of the information. If no date is set it will be marked for declassification in ten or twenty-five years, depending on its sensitivity,⁴² although this date can be extended if the threat posed by disclosure persists.⁴³ The Executive Order provides that information must be classified to protect a risk to national security and cannot be classified to “conceal violations of law, inefficiency, or administrative error” or to “prevent embarrassment to a person, organization, or agency.”⁴⁴

With each new administration, the rules for classification can shift significantly.⁴⁵ For example, under President Clinton, the Executive Order concerning classification provided that “[i]f there is significant doubt about the need to classify information, it shall not be classified.”⁴⁶ When President Bush took office, he deleted this provision and replaced it with a statement that “[t]he unauthorized disclosure of foreign government information is presumed to cause damage to national security.”⁴⁷ In addition, the Bush Administration deleted a provision prohibiting the reclassification of declassified information and replaced it with a provision permitting reclassification of such information in certain circumstances, even if already released to the public.⁴⁸ With the change in administrations, the classification system went from one based on a presumption against secrecy to a presumption in favor of secrecy.

The Information Security Oversight Office (ISOO), which operates under the auspices of the National Archives, oversees compliance with the classification standards.⁴⁹ In April 2006, an ISOO audit of reclassification efforts determined that twenty-four percent of documents withdrawn from the public domain were improperly reclassified, and twelve percent of the remaining reclassification determinations were questionable.⁵⁰ The audit report noted that in many instances “insufficient judgment

40. *Id.* at § 1.2.

41. *Id.*

42. *Id.* at § 1.5.

43. *Id.* at § 1.5(c).

44. *Id.* at § 1.7(a).

45. *See* S. DOC. NO. 105-2, at 11 (1997) (reporting that in the last fifty years, every administration except the Kennedy administration has issued a new executive order on classification).

46. Exec. Order No. 12,958 § 1.2(b), 60 Fed. Reg. 19,825, 19,826 (Apr. 17, 1995).

47. Exec. Order No. 13,292, *supra* note 39, at § 1.1(c).

48. *Id.* at § 1.7(c).

49. *Id.* at § 5.2(b); *see also* ISOO’s Mission, Functions, and Goals, <http://www.archives.gov/isoo/about/>.

50. INFORMATION SECURITY OVERSIGHT OFFICE, AUDIT REPORT, WITHDRAWAL OF RECORDS FROM PUBLIC ACCESS AT THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION FOR CLASSIFICATION PURPOSES (2006), <http://www.archives.gov/isoo/reports/2006-audit-report.html#found> [hereinafter ISOO AUDIT]. For example, the CIA redacted from a document a sentence indicating that the American and British intelligence services worked together during World War II, as well as detailing the number of American spies in 1946, even though this

was applied to the decision to withdraw the record from public access,” especially in situations where the information was already published elsewhere.⁵¹ In some instances, the CIA violated the classification provisions by withdrawing unclassified information in order to obfuscate what information was truly sensitive.⁵² In addition, many documents that were not classified when created were classified over fifty years later on the sole basis they contained the name of a CIA official in a list of individuals provided a copy.⁵³ Since September 11, over one million historical documents—some over 100 years old—have been reclassified.⁵⁴

Overclassification has become an epidemic. J. William Leonard, ISOO Director, testified before Congress that “it is no secret that the Government classifies too much information,” and that in his experience “many senior officials will candidly acknowledge the problem of excessive classification.”⁵⁵ As Leonard noted, in many cases information is classified not to protect any real national security interests, but to protect the government from embarrassment or harsh scrutiny.⁵⁶ Former New Jersey Governor and 9/11 Commission Chairman Thomas Keane similarly told Congress that “three-quarters of the classified information he reviewed for the Commission should not have been classified in the first place.”⁵⁷ These observations echo those of former Solicitor General of the United States Erwin Griswold, who argued on behalf of the United States in *New York Times Co. v. United States*, the *Pentagon Papers* case.⁵⁸ Griswold said “[i]t quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another.”⁵⁹

information was contained in a State Department historical volume. Scott Shane, *Why the Secrecy? Only the Bureaucrats Know*, N.Y. TIMES, Apr. 16, 2006, at D1.

51. ISOO AUDIT, *supra* note 50.

52. *Id.*

53. *Id.*

54. Frank Bass & Randy Herschaft, *IM Archived Pages Removed Post-9/11*, USA TODAY, Mar. 15, 2007, http://www.usatoday.com/news/washington/2007-03-13-archives_N.htm.

55. *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on National Security, Emerging Threats, and International Relations of the H. Comm. on Government Reform*, 108th Cong. 28 (2004) (statement of J. William Leonard).

56. *Id.*

57. Lance Gay, *9/11 Panel Says Too Many Documents Are Being Stamped Secret*, SEATTLE POST-INTELLIGENCER, May 15, 2004, http://seattlepi.nwsourc.com/national/173449_911_panel15.html.

58. 403 U.S. 713, 718 (1971).

59. Erwin N. Griswold, *Secrets Not Worth Keeping: The Courts and Classified Information*, WASH. POST, Feb. 15, 1989, at A25. Another contributing cause of overclassification is the large number of people who are given classification authority, often without adequate training. See Heidi Kitrosser, *Classified Information Leaks and Free Speech*, (2007) (unpublished manuscript at 15–17, on file with the Indiana Law Journal), available at <http://ssrn.com/abstract=958099>.

The Freedom of Information Act (FOIA)⁶⁰ and the federal whistleblower statutes⁶¹ are two means by which Congress has attempted to provide a check on the executive branch's natural tendency to be excessively secretive. Although both types of legislation have gone a long way toward promoting an open government, they do not offer a perfect counterbalance to the Executive's efforts to control the dissemination of information. Getting information through FOIA requests has become harder and more expensive. For example, when the People for the American Way asked the Justice Department for information concerning sealed prisoner cases, the organization was required to pay \$373,000 in search fees before the government would even begin to locate responsive documents.⁶² David Schultz, who assists the Associated Press with its FOIA requests, notes that under the Bush Administration, "[a]gencies seem to view their role as coming up with techniques to keep information secret rather than the other way around."⁶³

FOIA has proven particularly ineffective when it comes to alleged national security information. FOIA does not contain a broad "national security" exemption. Instead, the only portion of FOIA that directly addresses national security is Exemption 1, which exempts from disclosure documents that are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order."⁶⁴ In 1973, the Supreme Court held that when the government claimed Exemption 1 applied, it had to prove merely that the document had been classified; courts could not view the documents in camera or otherwise inquire whether the documents had been in fact properly classified.⁶⁵ The following year, in reaction to the Court's decision, Congress voted to amend Exemption 1 to make clear that it did not intend the judiciary to simply rubber-stamp the Executive's classification decisions.⁶⁶ Congress specifically designed the amendments to Exemption 1 to empower courts to

60. 5 U.S.C. § 552 (2000), amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524.

61. Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, 112 Stat. 2413 (codified as amended at 50 U.S.C. § 403(q) (2000 & Supp. IV 2004) (for CIA) and 5 U.S.C. app. 3 § 8H (2000 & Supp. IV 2004) (for other intelligence activities)); Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16 (codified as amended at 5 U.S.C. § 2302 (2000 & Supp. IV 2004)) (covers most civil service employees); Military Whistleblower Protection Act of 1988, Pub. L. No. 100-456, 102 Stat. 2027 (codified as amended at 10 U.S.C. § 1034 (2000 & Supp. IV 2004)).

62. Alterman, *supra* note 6, at 14.

63. *Id.*

64. 5 U.S.C. § 552(b)(1) (2000). Exemption 3 provides that FOIA does not apply to information that is exempted from disclosure under a separate statute. 5 U.S.C. § 552(b)(3) (2000). These separate statutory exemptions often raise national security issues. In addition, FOIA specifically permits the Federal Bureau of Investigation to exercise its discretion in determining whether to disclose documents that "pertain[] to foreign intelligence or counterintelligence, or international terrorism," provided these documents constitute classified information as provided in subsection (b)(1). 5 U.S.C. § 552(c)(3) (2000).

65. *EPA v. Mink*, 410 U.S. 73, 84 (1973).

66. Freedom of Information Act, Pub. L. No. 93-502, 88 Stat. 1561, 1562 (1974); see generally Mary-Rose Papandrea, *Under Attack: The Public's Right to Know and the War on Terror*, 25 B.C. THIRD WORLD L. J. 35, 51 (2005).

exercise “effective judicial review of executive branch classification decisions”⁶⁷ in order to rectify the “widespread overclassification abuses in the use of classification stamps.”⁶⁸ The 1974 amendments made clear that courts were authorized to review classified documents in camera for a de novo determination of their classification.⁶⁹ Despite these amendments, courts have been extremely deferential to the government’s classification determinations and have not engaged in a rigorous review of classified information.⁷⁰

In addition, after September 11, 2001, Attorney General John Ashcroft released a new policy essentially advising agencies to refrain from releasing information pursuant to a FOIA request whenever possible, a complete reversal from the operating presumption under Janet Reno that information should be withheld only when there was a foreseeable risk of harm.⁷¹ The Ashcroft announcement stated that “[a]ny discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information.”⁷² Agencies were assured that the Department of Justice would defend their decisions to withhold information “unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.”⁷³

Existing protections for whistleblowers are also insufficient to check the use of the classification system to cover up illegal practices.⁷⁴ In theory, federal employees are

67. 120 CONG. REC. 17,015, at 17,020 (1974) (remarks of Sen. Kennedy).

68. *Id.* at 17,019.

69. 5 U.S.C. § 552(a)(4)(B) (2000).

70. *See* *Military Audit Project v. Casey*, 656 F.2d 724, 752 (D.C. Cir. 1981) (concluding that, in the absence of evidence of agency bad faith, summary judgment is properly granted to an agency in Exemption 1 cases without an in camera inspection or discovery by the plaintiffs when the affidavits submitted by the agency describe the sensitive documents at issue with reasonably specific detail, present justifications for nondisclosure that are detailed and persuasive, and demonstrate that the information withheld logically falls within the claimed exemption); *Hayden v. NSA*, 608 F.2d 1381, 1386–87 (D.C. Cir. 1979) (stating that, before conducting in camera review of classified records, courts must first afford agencies the opportunity to prove the records are properly classified by submission of an affidavit or other evidence); *People for the Am. Way Found. v. NSA*, 462 F. Supp. 2d 21, 33–34 (D.D.C. 2006) (concluding that, in the absence of contrary evidence or evidence of agency bad faith, an agency declaration is sufficient to demonstrate proper classification when the declaration indicates that the proper procedures were followed and that the information logically fits into Exemption 1); Patricia M. Wald, *Two Unsolved Constitutional Problems*, 49 U. PITT. L. REV. 753, 760 (1988) (noting that judicial review of classified information under FOIA “often seems to be done in a perfunctory way”). *But see* *Fensterwald v. CIA*, 443 F. Supp. 667, 669–70 (D.D.C. 1977) (initiating limited in camera review of a sampling of documents where agency offered only “skeletal” justifications to support broad claim of exemption and would risk compromising secrets if required to provide additional explanation).

71. Memorandum from John Ashcroft, Attorney General, to the Heads of all Federal Departments and Agencies (Oct. 12, 2001), *available at* <http://www.usdoj.gov/oip/011012.htm>.

72. *Id.*

73. *Id.*

74. *See National Security Whistleblowers in the Post-September 11th Era: Lost in a Labyrinth and Facing Subtle Retaliation: Hearing Before the Subcomm. on Nat’l Sec.,*

encouraged to report their concerns to officials in their chain of command, the Inspector General's Office, or the relevant Congressional oversight committee. In practice, however, the current legal regime is confusing and has significant limitations.⁷⁵

First, employees seeking to disclose misconduct may be confused by the fact that federal whistleblower protection statutes do not provide uniform levels of protection, but rather differentiate between employees in the intelligence community,⁷⁶ those elsewhere in the civil service,⁷⁷ and members of the military.⁷⁸ This uncertainty is exacerbated by the fact that the President may, at his discretion, shift certain groups of employees from the civil service category to the intelligence community category without effective notice to the employees.⁷⁹ For example, although the Whistleblower Protection Act of 1989, the general federal whistleblower law, explicitly excludes employees of the FBI, the CIA, the National Security Agency, the Defense Intelligence Agency, and the National Geospatial-Intelligence Agency,⁸⁰ it also excludes, "as determined by the President, any Executive agency or unit thereof the principle function of which is the conduct of foreign intelligence or counterintelligence activities."⁸¹ In other words, employees of an agency involved in intelligence activities

Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform, 109th Cong. 292, 293 (2006) (statement of Beth Daley, Senior Investigator, Project on Gov't Oversight).

75. See, e.g., H.R. REP. NO. 110-42, pt. 1, at 3-5 (2007) (detailing numerous loopholes and weaknesses in current federal whistleblower protections).

76. Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 702, 112 Stat. 2396, 2414-17 (codified as amended at 5 U.S.C. app. 3 § 8H (2000 and Supp. IV 2004) and 50 U.S.C. § 403q(d)(5) (2000 & Supp. IV 2004)). Employees of specified intelligence organizations are protected from retaliation if they intend to report to Congress "an urgent concern," a narrowly defined category of information that includes evidence of flagrant lawbreaking, lying to Congress, and reprisal against whistleblowers protected by the Act. 5 U.S.C. app. 3 § 8H(a)(1)(A)-(C), (g)(1)(A)-(C) (2000); 50 U.S.C. § 403q(d)(5)(A), (G)(i)(I)-(III) (2000). In addition, prior to passing information to one of the congressional intelligence committees, the employee making the disclosure must adhere to a detailed procedure, which includes reporting to the Inspector General, providing notice and a statement to the head of the organization, and receiving direction concerning the communication of the information in a manner consistent with appropriate security practices. 5 U.S.C. app. 3 § 8H(d)(1)-(2) (2000); 50 U.S.C. § 403q(d)(5)(D)(i)-(ii) (2000).

77. 5 U.S.C. § 2302(a)(2) (2000 and Supp. IV 2004).

78. 10 U.S.C. § 1034 (2000 and Supp. IV 2004). No person may restrict a member of the military from lawfully communicating with a member of Congress or an Inspector General. *Id.* at § 1034(a)(1)-(2). Service members are protected from retaliatory personnel actions in response to a lawful communication to Congress or an Inspector General or in response to any communication to Congress or various military officials that reasonably constitutes evidence of a violation of law or regulation or of gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial danger to public health or safety. *Id.* at § 1034(b)(1)(A)-(B), (c)(2)(A)-(B).

79. 5 U.S.C. § 2302(a)(2)(C)(ii) (2000); 5 U.S.C. app. 3 § 8H(a)(1)(C) (2000); *Czarkowski v. Merit Sys. Prot. Bd.*, 390 F.3d 1347, 1351 (Fed. Cir. 2004) (concluding that, when transferring a group of employees from the general whistleblower framework to the intelligence community framework, the President must make an express determination on the public record, but he is not required to provide actual notice to employees).

80. 5 U.S.C. § 2302(2)(C)(ii) (2000).

81. *Id.*

could—without warning—suddenly find themselves excluded from the much broader protections of the general federal whistleblower law.⁸²

Even if government employees can figure out which federal whistleblower law applies to them, the protections these laws offer is minimal, particularly when the disclosure involves national security information. The general federal whistleblower law protects a government employee for any disclosure of information that he “reasonably believes” demonstrates either a violation of any law, rule, or regulation, or instance of gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.⁸³ A member of the intelligence community, however, is covered under the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA),⁸⁴ and is protected only if he discloses a matter of “urgent concern.” Urgent concern is narrowly defined to include “a serious or flagrant” violation of law or executive order, a false statement to Congress (or willful withholding of information from Congress), or the reprisal against a person who reported a matter of urgent concern.⁸⁵ Members of the armed forces are protected under the Military Whistleblower Protection Act of 1988 (“Act”).⁸⁶ The protected disclosures under this Act are similar to those covered under the general federal whistleblower law, but the Act excludes communications that are “unlawful.”⁸⁷ The Act does not define the term “unlawful,” leaving open the possibility that any unauthorized disclosure of classified information would not be covered.

Furthermore, when disclosing wrongdoing involving classified information, most federal employees who bypass designated agency officials and instead report directly to Congress are not protected from retaliation.⁸⁸ National security employees in particular must follow very specific procedures in order to receive any protection. Any disclosure must be made first to the appropriate Inspector General or a designee.⁸⁹ The Inspector General then must assess the credibility of any report and forward any credible report to the head of the intelligence agency within fourteen days.⁹⁰ The employee may report directly to the congressional intelligence committees only if all of the following conditions are met: (1) the Inspector General fails to accurately transmit the report within the 14 calendar day period; (2) the employee, before making such a

82. Jamie Sasser, Comment, *Silenced Citizens: The Post-Garcetti Landscape for Public Sector Employees Working in National Security*, 41 U. RICH. L. REV. 759, 780–82 (2007) (giving the DHS example).

83. 5 U.S.C. § 2302(b)(8)(A)-(B) (2000).

84. This Act was codified at 50 U.S.C. § 403(q) (2000) for the CIA; for all other intelligence activities, it was codified under 5 U.S.C. app. 3 § 8H.

85. 50 U.S.C. § 403q(d)(5)(G)(i) (2000).

86. 10 U.S.C. § 1034 (2000).

87. *Id.* § 1034(a)(2).

88. 5 U.S.C. § 2302(b)(8)(A) (2000) (providing that if an employee makes a disclosure to a person other than the Special Counsel or Inspector General of an agency (or a designee), the disclosure is protected only if it “is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs”); 5 U.S.C. app. 3 § 8H(a)(1)(A)-(C) (2000 & Supp. IV 2004); 50 U.S.C. § 403q(d)(5)(A) (2000).

89. *See* 5 U.S.C. app. 3 § 8H(a)(1); 50 U.S.C. § 403q(d)(5)(A).

90. 5 U.S.C. app. 3 § 8H(b) (2000 & Supp. IV 2004); 50 U.S.C. § 403q(d)(5)(B) (2000 & Supp. IV 2004).

contact, furnishes the head of the activity, through the Inspector General, a statement of the employee's complaint and notice of the employee's intent to contact the intelligence committees directly; and (3) the employee obtains and follows from the head of the activity, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices.⁹¹

Finally, and perhaps most significantly, the current whistleblower statutes do not prohibit federal agencies from retaliating against a whistleblower by revoking his security clearance, a decision that is generally not subject to independent judicial review⁹² and that can lead to the employee's indefinite suspension or termination.⁹³ Given these substantial weaknesses, it is not surprising that the Congressional Research Service concluded in 2005 that one reason federal employees leak information to the press is that the government has failed to provide adequate protection for whistleblowers.⁹⁴

II. THE GAME OF LEAKS

Although the press is commonly regarded as the "watchdog" of the government, in reality the relationship between the press and the government is a much more complicated, symbiotic relationship.⁹⁵ At various times through our nation's history,

91. 5 U.S.C. app. 3 § 8H(d) (Supp. IV 2004); 50 U.S.C. § 403q(d)(5)(D) (Supp. IV 2004).

92. *Dep't of Navy v. Egan*, 484 U.S. 518, 529 (1988) (holding that the courts and the Merit Systems Protection Board do not have the authority to review security clearance revocations made by the executive branch); *Cheney v. Dep't of Justice*, 479 F.3d 1343, 1351–52 (Fed. Cir. 2007) (concluding that the court and the Merit Systems Protection Board may review whether revocation of a security clearance conformed to procedural requirements, but may not review the underlying merits of the decision to revoke the clearance without an explicit grant of statutory authority); *Hesse v. Dep't of State*, 217 F.3d 1372, 1380 (Fed. Cir. 2000) (concluding that the Merit Systems Protection Board lacks authority to review security clearance determinations in the context of the whistleblower actions without specific statutory authority); *see also National Security Whistleblowers in the Post-September 11th Era*, *supra* note 74, at 244 (statement of Mark S. Zaid, Managing Partner, Krieger & Zaid, PLLC) (explaining how whistleblowers risk losing security clearance without meaningful review). The House recently passed the Whistleblower Protection Enhancement Act, which adds the revocation of a security clearance to the list of prohibited adverse personnel actions. H.R. 985, 110th Cong. § 10 (2007). This bill is currently under review in a Senate committee. 153 CONG. REC. S3198 (2007).

93. While it is not clear that the revocation of a security clearance would result in the termination of employment for members of the military (since separating a service member is generally more difficult than firing a civilian employee), such a revocation would clearly be a deterrent for potential whistleblowers in the armed services.

94. LOUIS FISHER, CONG. RESEARCH SERV., NATIONAL SECURITY WHISTLEBLOWERS 12–16 (2005), <http://www.fas.org/sgp/crs/natsec/RL33215.pdf>. In addition, even if the statutory regime were perfect, whistleblowers who suffer an illegal personnel action would have to deal with the inconvenience and uncertainty of bringing a legal challenge against that action because there is no guarantee that federal agencies will follow the protections of the whistleblower laws. *See, e.g.,* Petitioner's Opening Brief, *MacLean v. Dep't of Homeland Sec.*, No. 06-75112 (9th Cir. Jan. 29, 2007) (arguing that the TSA retroactively labeled a communication as "Sensitive Security Information" in order to specifically target an employee for retribution in response to the employee's protected whistleblowing activity).

95. Richard Halloran, *A Primer on the Fine Art of Leaking Information*, N.Y. TIMES, Jan.

the press has just as frequently served as the lapdog of the executive branch as it has the watchdog for the American people. In some sense, this is not at all surprising. The press depends upon the government for news; in turn, the government depends upon the press to communicate with the public.⁹⁶ Government officials feed information to the press to advance their public image, promote new policies, and communicate with their constituents. They are literally at the mercy of the press, who hold the power to emphasize a new policy or ignore it entirely.⁹⁷ In turn, reporters who cover affairs in Washington enjoy a certain level of prestige and depend upon the federal government to supply them with the content for their publications.⁹⁸ The relationship between the President and the press is not a perfect one, nor is it particularly well designed either to promote a President's agenda or to inform the public fully and completely about important issues.⁹⁹ But it is essential to understand all the complexities of the current system before determining under what circumstances, if any, the government should be entitled to punish the collection and publication of national security information.

A. History of Leaks

Leaks have played an important role in the governance of the United States since its founding. One of the first major leaks in the United States occurred during George Washington's presidency when chief negotiator John Jay returned from Great Britain in 1795 with a treaty designed to end hostilities left over from the Revolution.¹⁰⁰ Washington insisted that the Federalist Senate (with which he sided at that time) first review the treaty in secret in order to generate support for it before it was revealed to the public.¹⁰¹ It did not take long for an Anti-Federalist newspaper to publish the full text of the treaty.¹⁰² Although the source of many of the leaks of treaties and cabinet meetings was rumored to be Washington's Secretary of State Thomas Jefferson, Washington himself engaged in leaking when he gave an advance copy of his farewell address to a partisan newspaper.¹⁰³

Every president has relied on the press to inform the public about government policy.¹⁰⁴ In *The Federalist* No. 84, Alexander Hamilton noted the important role of the

14, 1983, at A16 (noting the "symbiotic relationship between the Government and the press"); Cass Sunstein, *Government Control of Information*, 74 CAL. L. REV. 889, 902 (1986) (rejecting common assumption that the government and the press are "locked in combat").

96. Richard B. Kielbowicz, *The Role of News Leaks in Governance and the Law of Journalists' Confidentiality, 1795–2005*, 43 SAN DIEGO L. REV. 425, 430 (2006) (noting that "officials use the media to govern").

97. DEBORAH HOLMES, *GOVERNING THE PRESS: MEDIA FREEDOM IN THE U.S. AND GREAT BRITAIN* 13 (1986).

98. STEPHEN PONDER, *MANAGING THE PRESS: ORIGINS OF THE MEDIA PRESIDENCY, 1897–1933*, at 164 (1999).

99. See, e.g., JODY POWELL, *THE OTHER SIDE OF THE STORY* 35 (1984) (arguing that the relationship between the president and the press is "seriously flawed").

100. JOHN TEBBEL & SARAH MILES WATTS, *THE PRESS AND THE PRESIDENCY: FROM GEORGE WASHINGTON TO RONALD REAGAN* 15 (1985).

101. *Id.* at 14–15.

102. *Id.* at 15.

103. Mark Feldstein, *The Jailing of a Journalist: Prosecuting the Press for Receiving Stolen Documents*, 10 COMM. L. & POL'Y 137, 149 n.87 (2005).

104. PONDER, *supra* note 98, at xii.

press, stating that “[t]he public papers will be expeditious messengers of intelligence to the most remote inhabitants of the Union.”¹⁰⁵ From 1789 to the late nineteenth century, public officials frequently planted information in openly partisan news outlets in order to gain political leverage and to expose government corruption.¹⁰⁶ During the 1800s, with the rise of the “penny press” and the advertising-supported daily paper, the media began to shift away from party-sponsored publications, and by the late nineteenth century, commercial, mass media had emerged.¹⁰⁷ As the media changed and editors were no longer blindly loyal to political parties, public officials had to adapt in order to be able to continue to use the media for their own purposes.¹⁰⁸ Presidents McKinley and Roosevelt began generating press releases, staging newsworthy events, holding press conferences, hiring press secretaries, and opening press offices.¹⁰⁹ It did not take long for the executive branch to discover the value of a well-placed leak.

President Theodore Roosevelt was one of the first presidents to realize that to be a strong leader he needed to use the modern press to his advantage.¹¹⁰ This meant not only dominating the front page of the newspapers by making news, but also controlling the way in which news was disseminated to the press.¹¹¹ By speaking off the record to reporters, he created a bond between himself and the press; and in turn, the press kept quiet news that might have otherwise come out from other sources.¹¹² He frequently floated “trial balloons” of possible policies to test public reaction, to discredit congressional opposition to legislation he desired, to keep his opponents off the front page, and to release unfavorable information about political allies without them knowing he was the source.¹¹³ If the trial balloon proved unpopular, Roosevelt would denounce reporters as being liars and frauds.¹¹⁴

By leaking information to trusted reporters himself, Roosevelt knew he could gain popular support for a program without alienating a group he relied on for political support.¹¹⁵ He knew that any leaked information would receive high-profile attention in the newspapers, who like to advertise their access to exclusive information.¹¹⁶ Whenever possible, he preferred to provide information to opposition news outlets as a

105. *Id.* (quoting THE FEDERALIST PAPERS NO. 84, at 517 (Alexander Hamilton) (Clinton Rossiter ed. 1961)).

106. *Id.* at xii–xiii; *see also* TEBBEL & WATTS, *supra* note 100, at 9–10; Kielbowicz, *supra* note 96, 432–41 (detailing the history leaks during this time period).

107. PONDER, *supra* note 98, at xiii–xvi, 3.

108. *Id.* at xiii–xv.

109. *Id.* at xv–xvi.

110. *See* GEORGE JUERGENS, NEWS FROM THE WHITE HOUSE: THE PRESIDENTIAL-PRESS RELATIONSHIP IN THE PROGRESSIVE ERA 4 (1981).

111. *Id.* at 7–8.

112. *Id.* at 20.

113. *Id.* at 41–42 (discussing Roosevelt’s use of trial balloons to test public reaction to proposed policies); PONDER, *supra* note 98, at 47 (noting how President Roosevelt used the press to appeal to the public for support, frequently over congressional opposition); TEBBEL, *supra* note 100, at 337–38; Kielbowicz, *supra* note 96, at 444.

114. JUERGENS, *supra* note 110, at 41–42.

115. *Id.* at 44.

116. *Id.*

means of covering his tracks and giving a sense of credibility to the leaked information.¹¹⁷

Executive agencies took note of all the “free” publicity Roosevelt was generating in the press, and sought to similarly expand their ability to communicate with a national audience, rather than simply disseminating information through congressionally supervised pamphlets published by the Government Printing Office.¹¹⁸ Not surprisingly, as the President and executive agencies began to have more direct contact with the press, the number of leaks increased dramatically.¹¹⁹ Public officials began selectively leaking information to reporters to cultivate relationships with them while simultaneously exercising some control over the news. Some of the agency leaks promoted positions that were contrary to President Roosevelt’s views, and there began the constant presidential struggle to prevent and minimize leaks.¹²⁰ Roosevelt read the papers looking for undesirable stories. According to his military aide Archie Butt, when Roosevelt spotted an unfavorable story, “he would at once begin an investigation as to how it got there, and if he could locate the author of the leak he would dismiss him or have him transferred to some other department.”¹²¹ Very often, however, Roosevelt could not determine the source of the leak. He was particularly upset that his own cabinet secretaries were telling the press details of cabinet meetings, and in fact, called a specific cabinet meeting to discuss this very subject.¹²² After this meeting, Roosevelt’s press secretary William Loeb optimistically told the press that no more leaks would be coming from the executive departments, but within a very short time, the departments were again leaking like “a worn-out hose.”¹²³

Almost all presidents since Roosevelt have used leaks as part of their efforts to promote their agendas and persuade the public.¹²⁴ President William Taft—one of the only modern presidents to spurn the press—made no effort to prevent leaks or to coordinate executive branch publicity, and he quickly discovered that the media instead wrote about rumors and information spread by those who did not agree with him.¹²⁵ Not surprisingly, his popularity declined as he failed to use the press to influence public opinion.¹²⁶

Former executive branch officials have admitted that they selectively released sensitive information in a conscious effort to generate public support for its policies or to serve some other bureaucratic or personal agenda.¹²⁷ For example, President

117. *Id.*

118. PONDER, *supra* note 98, at 35–36.

119. *Id.* at 48.

120. JUERGENS, *supra* note 110, at 51; PONDER, *supra* note 98, at 48.

121. PONDER, *supra* note 98, at 48 (quoting Letter from Archie Butt to Mrs. Lewis F.B. Butt (Mar. 28 1909), in *THE LETTERS OF ARCHIE BUTT* 1:28–32 (Lawrence F. Abbot ed., 1924)).

122. LOUIS KOENIG, *THE INVISIBLE PRESIDENCY* 177 (1960).

123. *Id.*

124. *See generally* Tom Wicker, *Leak On, O Ship of State!*, N.Y. TIMES, Jan. 26, 1982, at A15 (summarizing the different types of leaks from government officials and their motivations for leaking information).

125. JUERGENS, *supra* note 110, at 97–98; PONDER, *supra* note 98, at 51–61, 63–65; TEBBEL, *supra* note 100, at 353.

126. PONDER, *supra* note 98, at 59, 74–75; *see also* JUERGENS, *supra* note 110, at 112 (discussing Taft’s failure to use the newspapers to influence public opinion).

127. MARTIN LINSKY, *IMPACT: HOW THE PRESS AFFECTS FEDERAL POLICYMAKING* 172 (1986)

Carter's former National Security Advisor Zbigniew Brzezinski admitted that he released otherwise sensitive information for "explicit administrative purposes."¹²⁸ President Carter's former Assistant Secretary of Defense conceded that "he 'had the authority to declassify particular pieces of information when that seemed necessary.'"¹²⁹ And a White House official under President Kennedy agreed that "high ranking administration officials knowingly and deliberately disseminated [classified information] from time to time in order to advance the interests of a particular person, [or] policy."¹³⁰ As one commentator has noted, "the executive's power to classify and declassify information raises the specter of government misinformation, or its weaker and less noxious relative, 'spin control.'"¹³¹ The result is a distortion of the public debate on fundamental public issues.

President Reagan's Former Secretary of State Alexander Haig has said that even though leaks can be troublesome, "in the end I concluded that they were a way of governing. Leaks constituted policy; they were the authentic voice of the government."¹³² The government and its employees and officials selectively release classified or otherwise secret information in a conscious effort to test or generate public support for certain policies or to serve some other bureaucratic or personal agenda.¹³³ Very often, government officials leak information to the press as a way of communicating with other parts of the government.¹³⁴ The government also uses selective leaks to the press to communicate with foreign governments—or, just as

(explaining that one study reported that 42% of federal officials admitted to leaking information to the press, and that in reality, the number is probably even higher); Note, *Keeping Secrets: Congress, the Courts, and National Security Information*, 103 HARV. L. REV. 906, 911 (1990).

128. ELIE ABEL, LEAKING: WHO DOES IT? WHO BENEFITS? AT WHAT COST? 36 (1987).

129. *Id.*

130. James A. Goldston, Jennifer M. Granholm & Robert J. Roberson, Comment, *A Nation Less Secure: Diminished Public Access to Information*, 21 HARV. C.R.-C.L.L. REV. 409, 412–13 n.16 (1986) (quoting affidavit of Theodore C. Sorenson).

131. Note, *supra* note 127, at 913.

132. ALEXANDER M. HAIG, JR., CAVEAT: REALISM, REAGAN, AND FOREIGN POLICY 17 (1984).

133. See, e.g., PONDER, *supra* note 98, at 121 (discussing how President Coolidge would frequently make newsworthy comments during press briefings "off the record," requiring the press to identify the source as a source "close to the President" or as the "White House spokesman," so that if the comments proved erroneous or controversial he could deny them); LEON V. SIGAL, REPORTERS AND OFFICIALS: THE ORGANIZATION AND POLITICS OF NEWSMAKING 140–42 (1973); Robert Pear, *Health Aides See a Tax on Benefits Beyond Basic Plan*, N.Y. TIMES, Sept. 5, 1993, at A1 (noting that the Clinton administration openly used leaks to float "trial balloons" concerning proposed health care reforms; a White House spokesman admitted that "[w]e want to explain and communicate our policies to the American people, and we think background discussions are a good way of doing it").

134. HOLMES, *supra* note 97, at 12 (describing the press as a form of "in-house mail system" for government officials); SIGAL, *supra* note 133, at 143; Halloran, *supra* note 95, at A16 (explaining that "'leaking' is not solely nor even largely the province of the dissident. Rather, it is a political instrument wielded almost daily by senior officials within the Administration to influence a decision, to promote policy, to persuade Congress and to signal foreign governments."); see also *Frontline: News Wars: Secrets, Sources, & Spin (Part I)* (PBS television broadcast Feb. 13, 2007) (explaining that the government uses the elite press, for example *The New York Times*, the *Los Angeles Times*, and *The Washington Post*, to communicate with government bureaucrats and elected officials).

often, to disseminate “disinformation” and propaganda.¹³⁵ Given that the government routinely leaks information for its own purposes, it is not surprising that a presidential aide once noted that “the people at 1600 Pennsylvania Avenue are not really worried about all leaks—only those that originate outside the White House.”¹³⁶

Leaks from the executive branch have frequently concerned the military, national security, and foreign affairs. For example, when the United States’ involvement in World War I was becoming increasingly imminent, President Woodrow Wilson and Secretary of State Robert Lansing leaked to the Associated Press the infamous Zimmerman telegram, sent from the former Secretary of the German Empire to Germany’s ambassador in Mexico instructing the ambassador to approach Mexico about forming an alliance against the United States.¹³⁷ During the Eisenhower administration, an Army program director critical of a proposed program to transfer a team of rocket experts from the Army to NASA chose to leak information about the proposal to a Baltimore Sun reporter instead of appealing to his immediate supervisors in order to “make sure that the President knew that this was a highly controversial matter.”¹³⁸ And during the Reagan administration, it was Attorney General Edwin Meese who first revealed that the United States had sold arms to Iran.¹³⁹

During the Scooter Libby criminal prosecution, the public gained insight into the various ways in which the Bush Administration has attempted to manipulate the press. President Bush was criticized for selectively declassifying portions of the National Intelligence Estimate on Iraq to provide support for going to war against Iraq in 2003.¹⁴⁰ When former ambassador Joseph Wilson wrote an editorial in the *New York Times* calling into question Bush’s claim that Iraq was developing nuclear weapons, the White House authorized aide Lewis “Scooter” Libby to leak selective sensitive national security information—including the identity of Wilson’s wife, then-CIA operative Valerie Plame—to discredit Wilson’s claims.¹⁴¹ Although the President argued that he merely selectively declassified bits of information,¹⁴² the line between leaking and selectively declassifying information is hazy at best, and illustrates the vast control the executive branch has over the dissemination of national security information to the public.

Given this history, it should be no surprise that most leaks do not come from disgruntled employees or whistleblowers, but rather from high-level officials.¹⁴³

135. SIGAL, *supra* note 133, at 151.

136. *Id.* at 145 (quoting aide to President Johnson); *see also* Wicker, *supra* note 124, at A15 (explaining that President Reagan “can’t stop leaks; no President can and no President really wants to. They only want to stop the leaks they don’t like.”).

137. PONDER, *supra* note 98, at 89.

138. SIGAL, *supra* note 133, at 140–41.

139. ABEL, *supra* note 128, at 2.

140. Editorial, *A Bad Leak*, N.Y. TIMES, Apr. 16, 2006, § 4, at 11 (criticizing President Bush for permitting Scooter Libby to leak “cherry-picked portions of the report”).

141. E.J. Dionne, Jr., Editorial, *All the President’s Leaks*, WASH. POST, Apr. 11, 2006, at A21; David Johnston & David E. Sanger, *In Court Filings, Cheney Aide Says Bush Approved Leak*, N.Y. TIMES, April 6, 2006, at A1.

142. Tom Hamburger, *Bush Speaks on Disclosure*, L.A. TIMES, Apr. 11, 2006, at A4 (reporting on speech in which Bush claimed he did not authorize a “leak” of information from the National Intelligence Estimate in 2003 but rather “declassified” information).

143. ABEL, *supra* note 128, at 4, 17, 35; MICHAEL BARUCH GROSSMAN & MARTHA JOYNT

Everyone from the President on down, as well as Congress and their staffers, leak information from time to time to gain an advantage or protect their reputations. Max Frankel, the former Executive Editor of the *New York Times*, noted that “[h]igh officials of the government reveal secrets in the search for support of their policies, or to help sabotage the plans and policies of rival departments.”¹⁴⁴ Frankel explained that “[l]earning always to trust each other to some extent, and never to trust each other fully—for their purposes are often contradictory and downright antagonistic—the reporter and the official trespass regularly, customarily, easily and un-self-consciously (even unconsciously) through what they both know to be official ‘secrets.’”¹⁴⁵ He added that

everything that our Government does, plans, thinks, hears, and contemplates in the realms of foreign policy is stamped and treated as secret—and then unraveled by that same government, by the Congress, and by the press in one continuing round of professional and social contacts and cooperative and competitive exchanges of information.¹⁴⁶

As one author studying the game of leaks has noted, the government would like to be able “to disclose the information they want, when they want, and in the way that they want.”¹⁴⁷ Of course at times there are leaks that the government does not authorize—from disgruntled current or former employees, to self-styled “patriots” trying to do what they see as a public service, to politicians. Regardless of their motivation, leaks too are an important part of the “game” and often contribute in important ways to the public debate. This game of having secrets, keeping secrets, revealing secrets, learning secrets, and publishing secrets is a game the press and the government play on a regular basis. In this game, all the players have their wins and losses.¹⁴⁸ The game is far from perfect; Louis Henkin aptly noted that the “trial by battle and cleverness” between the three branches and the press “hardly seems the way best to further the various aims of a democratic society” because it does not guarantee that information that is improperly classified will be revealed, or that genuinely sensitive information will remain secret.¹⁴⁹

As long as the executive branch controls the flow of government information, leaks play an undeniably important role not only in informing the American public, but also in checking the executive branch. Leaks of classified information have played an important role in informing the public throughout our country’s history. For example, through leaks, the public also has learned the details of the Iran-Contra Affair;¹⁵⁰ the

KUMAR, PORTRAYING THE PRESIDENT: THE WHITE HOUSE AND THE NEWS MEDIA 159 (1981); STEPHEN HESS, THE GOVERNMENT/PRESS CONNECTION: PRESS OFFICERS AND THEIR OFFICES 76 (1984).

144. Max Frankel, *The Washington Back Channel*, N.Y. TIMES, Mar. 25, 2007, § 6 (Magazine), at 40.

145. *Id.*

146. *Id.*

147. SIGAL, *supra* note 133, at 143.

148. Frankel, *supra* note 144.

149. Louis Henkin, *The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers*, 120 U. PA. L. REV. 271, 278 (1971).

150. See *The White House Crisis; Excerpts from the Tower Commission’s Report Part IV: What Was Wrong*, N.Y. TIMES, Feb. 27, 1987, at A17.

government's radiation and biological weapon experiments on unwitting Americans;¹⁵¹ the effectiveness of weapons systems;¹⁵² human rights abuses in Latin America, Asia, and Africa;¹⁵³ and many other illegally or morally reprehensible government practices. More recently, leaks of secret or classified information have led to the public discovery of several questionable—if not illegal—practices, including the treatment of prisoners in Abu Ghraib¹⁵⁴ and Guantanamo Bay,¹⁵⁵ wiretapping outside of the provisions of FISA,¹⁵⁶ and extraordinary rendition.¹⁵⁷

B. Controlling Leaks

Threatening reporters with criminal prosecution for publishing classified national security information is just one of many ways the executive branch attempts to stem the tide of leaks of which it does not approve.

First and foremost, presidents have attempted to limit leaks by surrounding themselves with loyalists and by excluding dissidents. Although President Bush is notorious for this practice, he is by no means the first president to use this method. President Wilson was so disturbed by leaks coming from the publicity offices of his Cabinet that he held Cabinet meetings less frequently and limited the scope of discussion, choosing instead to communicate with Cabinet members individually.¹⁵⁸ Similarly, to reduce leaks, President Kennedy excluded staff subordinates from sensitive meetings concerning the Cuban missile crisis; President Johnson limited his weekly luncheons discussing Vietnam War policy to a small group of senior officials; and President Nixon demanded that those working under him pledge to him personally that they would not leak any information to the press.¹⁵⁹ President Reagan issued an order forbidding all but a handful of executive branch officials from speaking on

151. *U.S. Promises to Release Data on Plutonium Test*, N.Y. TIMES, Nov. 21, 1993, § 1, at 30.

152. Eric Schmitt, *Israel Plays Down Effectiveness of Patriot Missile*, N.Y. TIMES, Oct. 31, 1991, at A8.

153. Raymond Bonner, *News Organizations Ask White House to Veto Secrecy Measure*, N.Y. TIMES, Nov. 1, 2000, at A32; Steven Lee Meyers, *Be All That You Can Be: Your Future as an Extortionist*, N.Y. TIMES, Oct. 6, 1996, § 4, at 7.

154. James Risen, *G.I.'s Are Accused of Abusing Iraqi Captives*, N.Y. TIMES, Apr. 29, 2004, at A15 (discussing details of the Abu Ghraib prisoner abuse scandal that was discovered through leaked photographs); *60 Minutes II: Abuse of Iraqi POWs by GIs Probed* (CBS television broadcast Apr. 28, 2004) available at <http://www.cbsnews.com/stories/2004/04/27/60II/main614063.shtml> (breaking story that prisoners at Abu Ghraib were abused).

155. Dana Priest & Joe Stephens, *Pentagon Approved Tougher Interrogations*, WASH. POST, May 9, 2004, at A1 (breaking story of abuse of prisoners at Guantanamo Bay; sources were military personnel who did not want their identities disclosed).

156. Josh Meyer, *U.S. to Hunt Source of Wiretap Leak*, CHI. TRIB., Dec. 30, 2005, at C1 (discussing leak of sensitive information concerning wiretapping); Risen & Lichtblau, *supra* note 1, at A1 (breaking NSA warrantless wiretapping story).

157. Jane Mayer, *Outsourcing Torture: The Secret History of America's "Extraordinary Rendition" Program*, THE NEW YORKER, Feb. 14, 2005, available at http://www.newyorker.com/archive/2005/02/14/050214fa_fact6.

158. PONDER, *supra* note 98, at 87. Wilson's plan to limit Cabinet meetings was, somewhat ironically, itself leaked to the press. *Id.*

159. SIGAL, *supra* note 133, at 147.

background to the press.¹⁶⁰ He was also the first president to issue an executive order requiring all federal workers to sign contracts agreeing to the censorship of any publications they might write for the rest of their lives.¹⁶¹

In addition, the executive branch has required government employees either to obtain permission before speaking to the press or to report to a supervisor the substance of any conversations they have with a member of the media. In searching for the identity of a leaker, the government may force employees to take a lie detector test,¹⁶² or to sign a statement waiving any confidentiality agreement they might have had with a member of the press.¹⁶³ Recently, the government has begun passing out different versions of official documents to each individual with slight grammatical differences, such as an extra or missing comma; if a document is leaked, these small differences can help the government identify the individual who leaked it.¹⁶⁴ In cases where the identity of an unauthorized leaker becomes known, the employee is made an “object lesson” for other employees, whether by subjecting the employee to criminal prosecution, stripping the employee of his security clearance, or firing him from his job.¹⁶⁵

The government also has methods of punishing the press for publishing leaks. Because the press and the government are in a symbiotic relationship—with the press depending on the government, and vice versa—government officials can temporarily stop returning the phone calls of disfavored journalists.¹⁶⁶ The press can be excluded from a press briefing, denied access to other proceedings, or even an invitation to the White House Christmas Party.¹⁶⁷ President Theodore Roosevelt, one of the first

160. TEBBEL & WATTS, *supra* note 100, at 540.

161. *Id.* at 546–47. The Supreme Court has held that the First Amendment does not invalidate these contracts. *Snepp v. United States*, 444 U.S. 507, 512 (1980) (per curiam) (upholding the right of the CIA to require its employees to sign nondisclosure agreements); *United States v. Marchetti*, 466 F.2d 1309, 1317 (4th Cir.), *cert. denied*, 409 U.S. 1063 (1972) (rejecting First Amendment challenge to nondisclosure agreement).

162. *See* Wicker, *supra* note 124, at A15 (noting how President Reagan, fed up with leaks, forced four-star generals and admirals to take lie-detector tests).

163. FBI agents conducting the Valerie Plame leak investigation sought such waivers from senior Bush Administration officials. Adam Liptak, *Reporters Face Scrutiny in C.I.A. Leak Inquiry*, N.Y. TIMES, Sept. 28, 2004, at A18.

164. David Barstow, Reporter, *The New York Times*, ABA Forum on Communications Law panel (Feb. 2007).

165. For example, a CIA officer named Mary McCarthy was fired in April 2006 for having unreported media contacts in violation of her security agreement. Although it was initially reported that she was fired because she leaked the black-site story to Dana Priest of *The Washington Post*, a senior intelligence official later denied that she was the source for that story. R. Jeffrey Smith & Dafna Linzer, *Dismissed CIA Officer Denies Leak Role*, WASH. POST, Apr. 25, 2006, at A1; *see also* James Kelly, *Shifting the Attack on Leaks*, TIME, May 19, 1986, at 91 (noting that Assistant Under Secretary for Defense Michael Pillsbury was fired for leaking details of an Administration plan to give Stinger missiles to anti-Communist rebels in Angola and Afghanistan).

166. HOLMES, *supra* note 97, at 6; *see also* Wicker, *supra* note 124, at A15 (noting that President Reagan, like other Presidents before him, reacted to unauthorized leaks by reducing communication with the press).

167. POWELL, *supra* note 99, at 310 (mentioning that one tactic for dealing with reporters is to intimidate them by threatening never to talk to them again, striking them from the White

presidents to take advantage of the press for his own publicity, divided reporters by those he could trust and those he could not, and if a reporter violated his trust, he would cut off not only that reporter but also that reporter's newspaper from access to the news.¹⁶⁸ Those who stayed in Roosevelt's good graces were treated to "almost astonishing frankness" about sensitive matters of state.¹⁶⁹

The Bush Administration has recently demonstrated a willingness to issue subpoenas to reporters and publishers when they publish a story that the government does not want disclosed. In the trial of Scooter Libby, 10 of the 19 witnesses called were journalists.¹⁷⁰ After the *New York Times* revealed that the National Security Agency was monitoring telecommunications outside of the oversight of the FISA court,¹⁷¹ the Department of Justice began a leak investigation.¹⁷²

C. A Generally Responsible Press

Some commentators charge journalists with ignoring the national security implications of publishing classified information, but this accusation has little foundation. Indeed, the press has exercised remarkable self-restraint by routinely considering the ramifications of its publications and frequently holding stories or limiting their scope in order to soften their impact. The government has often tried to convince the media to exercise publishing restraint. Although the government and the press are natural adversaries, this mediation approach has largely worked. History demonstrates that, if anything, the press has often been too willing to engage in self-censorship in times of war.

The press has played an important role in wartime since the nation's founding. During the American Revolution, the anti-British press helped stir up sentiment against the British and contributed to the unification of the thirteen colonies into a nation.¹⁷³ Francis Hopkinson, who signed the Declaration of Independence, noted the essential role the press played in the colonies' victory because "by influencing the minds of the multitude, [it] can perhaps do more towards gaining a point than the best rifle gun or sharpest bayonet."¹⁷⁴ These early newspapers lacked reporters; instead, they gathered their news from official pronouncements, letters, and other publications, including those supporting the British.¹⁷⁵ Although from time to time the colonial newspapers

House Christmas list, or revealing the reporter's affair to his spouse).

168. JUERGENS, *supra* note 110, at 17; KOENIG, *supra* note 122, at 172 (noting that President Theodore Roosevelt banished journalists who displeased him to the "Ananias Club," a journalistic doghouse).

169. JUERGENS, *supra* note 110, at 19 (quoting veteran journalist Isaac Marcossou).

170. Adam Liptak, *After Libby Trial, New Era for Government and Press*, N.Y. TIMES, Mar. 8, 2007, at A18. Criminal investigations continue to rely on the extraction of source identities from reporters. Philip Shenon, *Times Reporter Subpoenaed over Source for Book*, N.Y. TIMES, Feb. 1, 2008, at A17.

171. Risen & Lichtblau, *supra* note 1.

172. Scott Shane, *Criminal Inquiry Opens into Leak in Eavesdropping*, N.Y. TIMES, Dec. 31, 2005, at A1.

173. MICHAEL S. SWEENEY, *THE MILITARY AND THE PRESS: AN UNEASY TRUCE* 8-9 (2006) (alteration in original).

174. *Id.* at 9.

175. *Id.*

published troop movements, there is little evidence that the disclosure of such information undermined the nascent country's struggle for independence.¹⁷⁶

In World War I, the United States fought a "total war," harnessing every possible resource it could to secure victory. One resource it did not have to harness, however, was the press; as one commentator has described it, "the press enlisted to fight World War I."¹⁷⁷ Once the United States entered the war, President Wilson established, with an executive order, a new office called the Committee on Public Information (CPI), which provided the news media with press releases suitable for immediate publication and provided guidelines for the publication of any other information.¹⁷⁸ In addition, the media agreed to abide by vast censorship provisions and to publish the propaganda the government provided.¹⁷⁹ The press occasionally violated the CPI guidelines, but they generally honored them and may have been more circumspect than the guidelines required.¹⁸⁰

In addition, the government engaged in activity that certainly would be considered unconstitutional today. Under the Espionage Act of 1917, Congress had authorized criminal penalties for anyone who willfully made or conveyed "false reports or statements with intent to interfere with the operation or success of the military or naval forces of the United States," willfully causing, or attempting to cause, "insubordination, disloyalty, mutiny, or refusal of duty" in the Army or Navy, or willfully obstructing recruitment and enlistment.¹⁸¹ Any publications deemed to violate these provisions were considered "unmailable." The postmaster general, whose decisions were not subject to judicial review, used this authority to threaten the second-class mailing permits of seventy-five newspapers.¹⁸² On the battlefield, journalists agreed to follow a voluntary code of self-censorship.¹⁸³ They were required to sign a statement swearing to report the truth and not to report any information that could assist the enemy.¹⁸⁴

During World War II, the Office of Censorship was created to identify information that the press should refrain from publishing.¹⁸⁵ American broadcasters and newspapers were asked not to publish information about weather reports, troop movements, naval and merchant ships, military plans, selective service enrollment, fortifications, war material experiments, casualty lists, and the location of national treasures unless the appropriate authority released the information or gave specific permission for publication.¹⁸⁶ In addition, the Office of Censorship requested that

176. *Id.*

177. *Id.* at 36.

178. *Id.* at 45; PONDER, *supra* note 98, at 93–96.

179. *Id.* at 36; PONDER, *supra* note 98, at 96.

180. JUERGENS, *supra* note 110, at 189.

181. MICHAEL S. SWEENEY, *SECRETS OF VICTORY: THE OFFICE OF CENSORSHIP AND THE AMERICAN PRESS AND RADIO IN WORLD WAR II* 17 (2001).

182. *Id.*

183. *Id.* at 54.

184. *Id.* at 52.

185. Christina E. Wells, *Information Control in Times of Crisis: The Tools of Repression*, 30 OHIO N.U. L. REV. 451, 455 (2004).

186. U.S. GOVERNMENT OFFICE OF CENSORSHIP, *CODE OF WARTIME PRACTICES FOR AMERICAN BROADCASTERS*, at 1–4 (1942) [hereinafter *AMERICAN BROADCASTERS*]; U.S. GOVERNMENT OFFICE OF CENSORSHIP, *CODE OF WARTIME PRACTICES FOR THE AMERICAN PRESS*

broadcasters take precautions with respect to request programs, quiz programs, interviews, commentaries, and foreign language programming to guard against “enemy exploitation.”¹⁸⁷ The government asked the media to use “good common sense”¹⁸⁸ and to ask themselves before publication, “‘Is this information I would like to have if I were the enemy?’”¹⁸⁹ In addition, the media was advised that if they “desire[d] clarification or advice as to what disclosures might or might not aid the enemy, the Office of Censorship [would] cooperate gladly.”¹⁹⁰

Compliance with the censorship codes was voluntary, but no print journalist and only one radio journalist knowingly violated them.¹⁹¹ For example, “liberal crusading journalist” Drew Pearson and *New York Times* reporter William Lawrence knew about the development of the atomic bomb long before it was dropped on Japan, but they did not publish that information until after the war was over.¹⁹² Commentators have noted that the reason the press largely complied with the codes was probably because the Office of Censorship limited itself to matters involving a definite military risk.¹⁹³ The Roosevelt administration contemplated prosecuting a member of the press only once during World War II.¹⁹⁴ In 1942, the *Chicago Tribune* published accounts of the Battle of Midway that revealed that the United States had broken the Japanese code.¹⁹⁵ The government ultimately decided not to prosecute the newspaper because it subsequently became clear that the Japanese had not noticed the story, and administration officials were concerned that a prosecution would bring attention to the matter.¹⁹⁶

In 1961, during the Cold War, President Kennedy addressed the American Newspapers Publishers Association and asked that the press exercise extra caution before publishing information that might bear on national security. Emphasizing that he would never tolerate censorship, Kennedy offered to open the communication channels between his administration and the press in order to promote more thoughtful and informed publication decisions.¹⁹⁷ Eighteen months later, Kennedy’s promise of open communication was put to the test. The *New York Times* had received information that the Soviet Union had stationed nuclear weapons in Cuba, but it delayed publishing this information after President Kennedy explained to the newspaper’s editors that he would be addressing the nation the following day and

1–4 (1942) [hereinafter AMERICAN PRESS].

187. AMERICAN BROADCASTERS, *supra* note 186, at 6–8.

188. *Id.* at 6.

189. AMERICAN PRESS, *supra* note 186, at 1.

190. *Id.* at 5.

191. SWEENEY, *supra* note 181, at 3.

192. *Id.* at 3–4.

193. *Developments in the Law*, *supra* note 25, at 1194; see JAMES RUSSELL WIGGINS, FREEDOM OR SECRECY 95–99 (1956).

194. SWEENEY, *supra* note 173, at 5.

195. *Id.*

196. SANFORD J. UNGAR, THE PAPERS & THE PAPERS: AN ACCOUNT OF THE LEGAL AND POLITICAL BATTLE OVER THE PENTAGON PAPERS 111–12 (1972).

197. John F. Kennedy, U.S. President, The President and the Press: Address before the American Newspaper Publishers Association (Apr. 27, 1961), (transcript available at <http://www.jfklibrary.org/historical+resources/archives/reference+desk/speeches/jfk/003POF03Newspaperpublishers04271961.htm>).

needed time to solidify diplomatic and military contingencies in case his public announcement enflamed the situation with the Soviets.¹⁹⁸

During the Iran hostage crisis during President Jimmy Carter's administration, the press held many stories that might have caused harm to the hostages.¹⁹⁹ For example, most reporters covering Iran knew of embassy officials who had escaped during the takeover and were hiding somewhere in the city of Tehran, but not a single story concerning these officials—who ultimately escaped disguised as Canadian businessmen—appeared in the media.²⁰⁰ Katharine Graham ordered the *Washington Post* and *Newsweek* to comply with a request from the President's office not to disclose the secret negotiations between the United States and Iranian lawyers.²⁰¹ The media's willingness to cooperate with the President's request for secrecy is yet another example of its respect for legitimate national security concerns. This cooperation did not immunize the press from criticism, however; *The Nation* magazine criticized the press for abdicating its role as a watchdog, stating in an editorial that "the media appear to have abandoned all critical scrutiny of the Administration's decision-making process."²⁰²

In 1986, President Reagan personally asked Katherine Graham of the *Washington Post* to refrain from publishing information concerning a spy project called "Ivy Bells," in which the United States was conducting underwater eavesdropping in Russian harbors.²⁰³ Reagan told Graham that the continued secrecy of the spy program was extremely important for national security, and that if her newspaper revealed its existence, he would support its prosecution.²⁰⁴ Acceding to the President's request because it "was unable fully to judge the validity of the national security objections of the senior officials and because of its lawyers' concerns," the *Washington Post* removed all mention of Ivy Bells from its report and instead published a relatively innocuous story about the interactions of accused spy Ronald Pelton with Soviet agents.²⁰⁵ Much to the paper's surprise, NBC revealed the exact same story on the *Today* show.²⁰⁶ When threatened with prosecution, NBC News President Lawrence Grossman said NBC was surprised because the network had published the exact same information a year earlier when Pelton was arrested; in addition, Pelton's attorney had identified the spy program in open court during a pretrial proceeding, and the *Washington Post* and the *New York Times* had revealed the existence of a similar program a decade earlier.²⁰⁷

The press has continued to be mindful that its responsibility to the nation is not to pass along every bit of classified information it receives, but to weigh carefully the public's right to know what its government is doing against the national security harms that might result from publication. Indeed, Benjamin Bradlee noted in his memoir *A*

198. MAX FRANKEL, *HIGH NOON IN THE COLD WAR: KENNEDY, KHRUSHCHEV, AND THE CUBAN MISSILE CRISIS* 108–110 (2004).

199. HOLMES, *supra* note 97, at 61.

200. *Id.*

201. *Id.* at 62.

202. Editorial, *Lost Chance?*, *THE NATION*, January 26, 1980, at 67.

203. Richard Zoglin, *Questions of National Security*, *TIME*, June 2, 1986, at 67.

204. *Id.*

205. *Id.*

206. *See id.*

207. *Id.*

Good Life that while he was editor at the *Washington Post*, he “kept many stories out of the paper because [he] felt—without any government pressure—that the national security would be harmed by their publication.”²⁰⁸ Kenneth Wainstein, Assistant Attorney General for National Security in the Bush Administration, recently confirmed this view of the press as largely responsible, noting that he has found the press reasonable and cooperative in not publishing sensitive information.²⁰⁹

Some of the most recent stories revealing questionable, if not illegal, government activities were published only after the most thorough consideration of the national security implications, often in consultation with government officials. For example, the *New York Times* held its story about the National Security Agency’s warrantless surveillance program for over a year based on arguments from officials in the Bush Administration that publishing the article would cause grave harm to national security efforts. It was only after extensive additional reporting that the newspaper realized that publishing the story would not provide useful information to terrorists who were the targets of the program. To date there has been no credible explanation of how the *New York Times’* decision to publish this story harmed the government’s counterterrorism efforts.²¹⁰

Similarly, the *Washington Post* published an article revealing the existence of “black sites” where terrorism suspects were secretly detained and interrogated, but at the insistence of Bush Administration officials, the paper did not identify the names of the Eastern European countries that were participating in the program.²¹¹ The *Washington Post* explained that it had accepted the government’s argument that revealing those countries’ identities “might disrupt counterterrorism efforts in those countries and elsewhere and could make them targets of possible terrorist retaliation.”²¹² Like the publication of the NSA wiretapping story, the *Washington Post’s* black site revelations may have caused the United States some embarrassment in international circles, but there is no reason to believe that it has undermined its counterterrorism efforts.

There may be many reasons why the press is as cooperative as it is with the government. The press may be concerned that if it publishes stories that truly threaten national security, the government will have public support to go after the journalists themselves, particularly by subpoenaing them to reveal the identities of their sources. Some critics have suggested that reporters like to withhold national security secrets so that they can maintain status as “ultimate insiders” in the world of power.²¹³ In addition, the press may act responsibly out of their own economic self-interest; they do not want their consumers to perceive them as disloyal.

208. BEN BRADLEE, *A GOOD LIFE: NEWSPAPERING AND OTHER ADVENTURES* 474 (1995).

209. Association of American Law Schools, National Security Section Session (Jan. 5, 2007).

210. Instead, as James Risen said, “the real secret here was a political secret and a legal secret . . . not a national security secret.” James Risen, *Reporting National Security Under Threat of Indictment*, 2006 Annual Dinner of Media Law Resource Center, at 12 (transcript on file with the Indiana Law Journal).

211. Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST, Nov. 2, 2005, at A1.

212. *Id.*

213. TOM WICKER, *ON PRESS* 2 (1978).

So far, the government has never brought a prosecution against the press; instead, the Justice Department has focused on the leakers themselves. It is not clear whether the government would ever actually try to prosecute the press; it might be sufficient to have the threat of prosecution hanging over the heads of reporters and editors. As a CIA spokesman once said, “We don’t want to police the press We want the press to police itself.”²¹⁴ At a hearing before the Senate Judiciary Committee last May, Deputy U.S. Attorney Matthew W. Friedrich refused to rule out the possibility of prosecuting the press, but emphasized that the department’s “primary focus is on the leakers of classified information, as opposed to the press.”²¹⁵ Although the press can take some comfort in the government’s obvious reluctance to indict it for publishing sensitive national security information, the threat of prosecution remains very real. In addition, given that the internet permits individuals with no journalistic training to publish information to the world at large,²¹⁶ it is quite likely that the government will want to prosecute an individual publisher who has not been as responsible as the mainstream media has generally proven to be. The government’s willingness to prosecute the AIPAC lobbyists indicates that prosecutions against non-government actors may not be too far behind.

III. THE CURRENT STATUTORY REGIME

A review of the applicable statutes reveals that any of a number of provisions could be used against non-government actors. The United States lacks an equivalent to the United Kingdom’s Official Secrets Act, but it does have several statutes that criminalize the dissemination of particular types of information. Most of these provisions are contained in the Espionage Act. In addition, Congress has enacted several other laws that protect specific information or protect the government’s proprietary rights.

A. *No Official Secrets Act*

The United States does not have an act like the United Kingdom’s Official Secrets Act that punishes all unauthorized disclosures of classified information. In 2000, Congress passed legislation that would have criminalized the disclosure of classified information by U.S. officers or officials or any others with authorized access to such

214. Richard Zoglin, *Questions of National Security: The CIA tangles with the Washington Post and NBC*, TIME, June 2, 1986, at 67; see also James Kelly, *Shifting the Attack on Leaks: The CIA director hints at prosecutions of news organizations*, TIME, May 19, 1986, at 91 (quoting a Justice Department official as reporting that “we’re not hot to trot on [prosecuting the press]”).

215. Walter Pincus, *Silence Angers Judiciary Panel: Justice Official Mum on Possible Prosecution of Journalists*, WASH. POST., June 7, 2006, at A05.

216. Mary-Rose Papandrea, *Citizen Journalism and the Reporter’s Privilege*, 91 MINN. L. REV. 515, 521–32 (2007). For example, the website Wikileaks has published a variety of sensitive documents, including the Rules of Engagement for U.S. military forces in Iraq and operating procedures for Guantanamo Bay prison. See U.S. Rules of Engagement for Iraq, http://www.wikileaks.org/wiki/US_Rules_of_Engagement_for_Iraq; Camp Delta Standard Operating Procedure (2004), http://www.wikileaks.org/wiki/Camp_Delta_Standard_Operating_Procedure.

information, but it was vetoed by President Clinton. In his veto memo, Clinton explained that while he agreed that unauthorized disclosures of classified information are too frequent and can be “extraordinarily harmful” to the national security, the proposed legislation struck a poor balance between the two equally compelling needs to protect national security secrets and to promote the free flow of information that is essential to democracy.²¹⁷ In particular, Clinton expressed concern that the law would have a chilling effect on perfectly legitimate activities by serving to discourage government officials from appropriate discussions of public issues in press briefings or other legitimate activities, and by deterring former government officials from contributing to the public debate through teaching, writing, and public speaking.²¹⁸ In 2006, Senator Bond (R-MO) proposed very similar legislation to the bill Clinton vetoed.²¹⁹

B. The Espionage Act

While the proposed official secrets legislation applies only to those individuals who have authorized access to classified information, many provisions of the Espionage Act are potentially applicable to those who do not occupy a position of “trust” with the government, including the media.

In their famous *Columbia Law Review* article published shortly after the *Pentagon Papers* case, Benno Schmidt and Harold Edgar exhaustively detailed the history of this Act and examined its often vague and confusing language.²²⁰ The first iteration of the Espionage Act came in 1917 and was amended several times; the most recent amendments were made in 1950. As many commentators and judges have noted, the Espionage Act is one of the most confusing and ambiguous federal criminal statutes.²²¹

The foundation for the current Espionage Act lies in the Defense of Secrets Act of 1911,²²² which represented Congress’s first attempt to draft legislation specifically intended to protect the confidentiality of national defense information.²²³ Prior to this time, the government depended on generally applicable statutes barring treason,

217. H.R. Doc. No. 106-309, at 3–4 (2000).

218. *Id.* at 4.

219. S. 3774, 109th Cong. (2006). The bill proposed in 2006 differed from the 2000 legislation in two ways. First, it limited its application to information or material “properly” classified pursuant to the applicable statute or Executive Order. Second, the proposed legislation exempted the disclosure of classified information to an Article III judge, any member of Congress or committee or subcommittee of Congress, and agents of a foreign power when such disclosure has been authorized. *Id.*

220. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973).

221. See, e.g., *id.* at 934 (“[T]he legislation is in many respects incomprehensible”); Anthony Lewis, *National Security: Muting the “Vital Criticism,”* 34 UCLA L. REV. 1687, 1698 (1987) (“The espionage sections of the Federal Criminal Code are a singularly impenetrable warren of provisions originally passed by Congress under the stresses of World War I”); Stephen L. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL’Y REV. 219, 222 (2007) (noting that the Espionage Act contains “a number of seemingly overlapping and often ambiguous provisions”).

222. Act of Mar. 3, 1911, ch. 226, Pub. L. No. 470, 36 Stat. 1804-05 (1911).

223. Edgar & Schmidt, *supra* note 220, at 939–40.

unlawful entry onto military bases, and theft of government property.²²⁴ The Defense of Secrets Act prohibited the willful communication of knowledge concerning “anything connected with the national defense” to someone “not entitled to receive it.”²²⁵ The provisions of the Defense of Secrets Act were largely retained in the Espionage Act.²²⁶

The potential breadth and scope of the various provisions of the current Espionage Act are staggering. Many of its sections could, on their faces, apply to a media entity or reporter who obtains, retains, or publishes national defense information. Although it is not always clear whether this was Congress’s intent, the press plainly is vulnerable to indictment under these provisions.

1. Section 793

Section 793 restricts the gathering, retention, and dissemination of national security defense information. Subsection 793(a) criminalizes the entry onto any military installation “for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation.” Subsections 793(b) and (c) similarly punish anyone who copies or attempts to copy, or receives or obtains, or attempts to receive or obtain, “anything connected with the national defense,” provided that the offender has “the purpose of obtaining the information . . . with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation.” Although these provisions do not apply to the act of publication, they do relate to pre-publication activities, namely, the investigation and acquisition of national defense information.²²⁷

Subsections 793(d) and (f), which impose penalties for the dissemination of national security information on those in “lawful” possession of it, would generally not apply to the media, but subsection 793(e), which prohibits the dissemination or retention of such information by those in “unauthorized possession” of it, easily could be. This provision is particularly dangerous for the press with respect to tangible national security materials because the statute requires only that the offender disseminate or retain such materials “willfully.” With respect to “information pertaining to the national defense,” the government must also prove that the offender has “reason to believe [the information] could be used to the injury of the United States or advantage of a foreign nation.” Although this provision would provide some measure of protection for the press, it is unclear exactly how much.

Federal courts have imposed a number of limitations on the scope of “information relating to the national defense” to save it from being unconstitutionally vague and overbroad. Although the Espionage Act does not contain a definition of what constitutes “information relating to the national defense,” in *Gorin v. United States*, the Supreme Court held that the term “national defense” contained in a predecessor provision was a “generic concept of broad connotations, referring to the military and

224. *Id.* at 940.

225. *Id.*

226. The basic provisions of the Defense of Secrets Act were codified at 18 U.S.C. § 793(a)-(b) with some important modifications. *See* 18 U.S.C. § 793 (a)-(b) (2000).

227. Edgar & Schmidt, *supra* note 220, at 967–69.

naval establishments and the related activities of national preparedness.”²²⁸ In interpreting the predecessor provision, the Supreme Court held that the government does not have to provide any proof of injury or even potential injury to the United States; that the information could be advantageous to a foreign country is sufficient.²²⁹ The Court held that it was sufficient if the disclosed information be used “to the advantage of a foreign nation,” regardless of whether the nation is friend or foe.²³⁰ Furthermore, the Espionage Act is not clear whether the government must show *actual* injury to the national security of the United States (or actual advantage to a foreign power). Later courts have noted that the classification of the information is probative, although not conclusive, evidence that it is information relating to the national defense;²³¹ the classification scheme did not exist when *Gorin* was decided in 1941. To be constitutional, the courts have first required that the information at issue could not be publicly available,²³² and the information, if disclosed, must be “potentially damaging to the United States or useful to an enemy of the United States.”²³³ As one judge has noted, a “potentially damaging” standard has incredibly broad sweep because “[o]ne may wonder whether any information shown to be related somehow to national defense could fail to have at least some such ‘potential.’”²³⁴

228. *Gorin v. United States*, 312 U.S. 19, 28 (1941). Although this definition of national defense information is potentially limited to military information and tactical plans, lower courts have rejected such a limited construction. *See, e.g.*, *United States v. Truong Dinh Hung*, 629 F.2d 908, 918 (4th Cir. 1980) (rejecting the defendants’ attempt to limit “national defense” information to information concerning military matters); *United States v. Boyce*, 594 F.2d 1246 (9th Cir. 1979).

229. *Gorin*, 312 U.S. at 29.

230. *Id.* at 29–30. In *Gorin*, the defendant had disclosed to Russia information concerning the comings and goings of Japanese military and civilian officials on the West Coast. *Id.* at 23. Soon after *Gorin* was decided, the United States Attorney General issued an opinion stating that *Gorin* does not apply in cases where national defense information is provided to an allied nation with permission from the government. *See* 40 Op. Att’y Gen. 247 (1942). The Attorney General was responding to an inquiry from a factory desiring to communicate with allied nations about manufacturing methods and products. *Id.*

231. *United States v. Rosen*, 445 F. Supp. 2d 602, 623–24 (2006).

232. *Gorin*, 312 U.S. at 28 (explaining that if the information is not in fact secret, “there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government”). *See, e.g.*, *United States v. Heine*, 151 F.2d 813, 816 (2d Cir. 1945) (holding that compiling and disseminating to Germany publicly available information concerning the production of airplanes in the United States did not constitute a violation of the Espionage Act because none of the transmitted information was secret). The lower courts have interpreted the *Gorin* exception for national security information that is not in fact secret relatively narrowly. For example, the Fourth Circuit has held that the fact that some of the information at issue is publicly available is irrelevant if that information was not made publicly available by the government in an official document. *United States v. Squillacote*, 221 F.3d 542, 577–80 (4th Cir. 2000); *see also* *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972) (“Rumor and speculation are not the equivalent of prior disclosure, however, and the presence of that kind of surmise should be no reason for avoidance of restraints upon confirmation from one in a position to know officially.”).

233. *United States v. Morison*, 844 F.2d 1057, 1081 (4th Cir. 1988); *Rosen*, 445 F. Supp. 2d at 621–22.

234. *Id.* at 1086 (Phillips, J., concurring).

Most importantly, the Supreme Court held that the phrase “information relating to national security” was constitutional because it was limited by a scienter requirement that the offender had “reason to believe [that the information] could be used to the injury of the United States or to the advantage of any foreign nation.”²³⁵ By adding this requirement Congress hoped to provide some measure of protection to free debate on national security issues.²³⁶ The Congressional record contains little indication, however, of whether Congress meant by this “intent or reason to believe” requirement that the offender had to intend to harm the United States or benefit a foreign power, or whether it “is to be inferred from action when occurrence of the result is a virtual certainty.”²³⁷ Some lower courts have embraced a reading of *Gorin* suggesting this intent requirement required a showing of “bad faith.”²³⁸ In the AIPAC case, for example, Judge Ellis held that the government would have to prove not only that the defendants knew that the national defense information at issue could harm the United States, but also that they had a “bad faith purpose to either harm the United States or to aid a foreign government.”²³⁹ In other words, Judge Ellis explained, even if the defendants knew the disclosure of the information could harm the United States or help its enemies, they could not be convicted under the statute if they disclosed the information for “some salutary motive” or “as an act of patriotism.”²⁴⁰ The disclosure of the information must be *objectively* harmful to the United States, and the defendant must be *subjectively* intending to cause that harm.²⁴¹ If Judge Ellis’s interpretation of the “reason to believe” requirement stands, it would be very hard to satisfy this “bad faith” requirement in prosecutions against the press for the disclosure of “information relating to national security.”

Although it appears from the legislative history that Congress did not intend 18 U.S.C. § 793(e) to apply to the media, the plain language of the statute is by no means clear on that point. A media outlet, having “unauthorized possession” of any of the national security materials or information listed in the statute, from a leak, frequently “communicates” this information to “any person not entitled to receive it”—its readers. Such action would violate the plain language of § 793(e). Nothing in the statute carves out the press or publications to the public at large; instead, it simply applies to anyone who “communicates, delivers, or transmits” information to “others not entitled to

235. This scienter requirement applies only to the disclosure of “information relating to the national defense” and not to any of the other tangible materials listed in the statute. This premise is clear not only from the plain language of the statute, but also from the legislative history, where the report from the Senate Judiciary Committee, which added the scienter language to the statute, specifically stated that the phrase “which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation” modified only “information relating to the national defense.” S. REP. NO. 81-2369, pt. 1, at 9 (1950).

236. Edgar & Schmidt, *supra* note 220, at 941.

237. *Id.* at 942.

238. *Gorin*, 312 U.S. at 27–28; *see also* United States v. Troung Dihn Hung, 629 U.S. 908, 919 (1980) (approving a jury instruction that defined “bad faith” as “a design to mislead or deceive another. That is, not prompted by an honest mistake as to one’s duties, but prompted by some personal or underhanded motive”).

239. *Rosen*, 445 F. Supp. 2d at 626.

240. *Id.*

241. *Id.* at 640–41, 641 nn.55, 56.

receive it.” Although there is some evidence that Congress intentionally did not use the word “publish” in order to keep the press out of its scope, under the law, “publishing” information is a form of “communicating” it. In addition, as a realistic matter, publishing information necessarily involves some communication, typically between sources such as editors, copy editors, etc.²⁴²

Although the Supreme Court has not addressed the issue, lower courts have been unwilling to read these statutes as applying only to the classic espionage setting. The leading case on this issue is *Morison v. United States*, where the Fourth Circuit rejected the argument that 18 U.S.C. § 793(d) and 18 U.S.C. § 793(e) apply only to “classic spying and espionage activity by persons who, in the course of that activity, had transmitted national security secrets to agents of foreign governments with intent to injure the United States,” and not to the transmittal of information to a nationally recognized news organization.²⁴³ In that case, the defendant, Samuel Loring Morison, a military intelligence employee, had been doing some off-duty work for *Jane’s Defence Weekly*, a London-based publication that provided information on international naval operations. During his work there, Morison provided the publication with classified satellite photographs Navy intelligence had taken of a Soviet aircraft carrier in a Black Sea naval shipyard.²⁴⁴ His defense was not based on the actual words of the Espionage Act, but rather on the legislative intent of Congress.²⁴⁵ The Fourth Circuit also rejected Morison’s argument.²⁴⁶

Both statutes plainly apply to “whoever” having access to national defense information has under section 793(d) “willfully communicate[d], deliver[ed] or transmit[ted] . . . to a person not entitled to receive it,” or has retained it in violation of section 793(e). The language of the two statutes includes no limitation to spies or to “an agent of a foreign government,” either as to the transmitter or the transmittee of the information, and they declare no exemption in favor of one who leaks to the press. It covers “anyone.” It is difficult to conceive of any language more definite and clear.²⁴⁷

The more recent AIPAC case has extended the reach of subsections 793(d) and (e) to individuals who, unlike Morison, are not in a position of trust in the government.

2. Section 794

Section 794 also concerns the transfer of national defense information, but rather than prohibiting the disclosure of information to “one not entitled to receive it,” it

242. See Edgar & Schmidt, *supra* note 220, at 1036. Edgar and Schmidt suggest that there is a way to interpret the word “publish” to require making information generally known to the public, whereas “communicating” information requires a more intimate transaction. *Id.* at 943–44. This approach would ignore the well-established principle of media law that one “publishes” information even when communicating that information to just one other person.

243. *United States v. Morison*, 844 F.2d 1057, 1063–64 (4th Cir. 1988) (internal quotations omitted).

244. *Id.* at 1061.

245. *Id.* at 1063–64.

246. *Id.* at 1064.

247. *Id.* at 1063.

instead prohibits disclosure to an “agent . . . [of a] foreign government,” without regard to whether the foreign power is friend or foe.²⁴⁸ As with § 793, it is quite possible to construe certain provisions of this statute to apply to the media, although it is not at all clear that was Congress’s intent.

Subsection 794(a) sweeps broadly to impose criminal penalties on anyone who “communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit,” to any foreign government or agent “either directly or indirectly” any “document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense,” provided that the person has the “intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation.” Although the subsection does not define “information relating to the national defense,” it permits the imposition of the death penalty only if the offense resulted in a foreign power uncovering the identity of a United States secret agent, or if the information details major weapons systems, communications intelligence or cryptographic information, or any major element of defense strategy.²⁴⁹

It is possible to read this subsection as subjecting the press to punishment if it “indirectly” delivers national security information to foreign powers by publishing a newspaper, broadcasting on television or radio, or posting on an Internet site where agents of a foreign power might discover it. Edgar and Schmidt argue that the “direct or indirect” language is “better read as directed at communication between citizens when the transmitter realizes that his contact is but a link in the intended chain to a foreign recipient.”²⁵⁰ In addition, they point out that the drafters specifically avoided using the word “publish” in this provision, even though they used that word in § 794(b).²⁵¹ This is all well and good, but it is a slender defense for any media who are prosecuted under this provision. Publication is a form of communication, and publishing any information in the United States—particularly in the age of the Internet—is equivalent to “indirectly” publishing it to foreign powers. If a court could get past the plain language of the statute, the legislative history is somewhat more helpful to the press. When subsections 794(a) and (b) were passed in 1917, Congress rejected proposed legislation that would have authorized the President to issue regulations to prohibit the publication of specific national security information.²⁵² Those who argued against giving the President this power argued that 794(b) was sufficient; neither side mentioned subsection 794(a) as having any relevance to this issue.²⁵³

Subsection 794(b) is applicable only “in time of war.” It punishes anyone who “collects, records, publishes, or communicates, or attempts to elicit any information” concerning military matters “with the intent that the same shall be communicated to the enemy.” Unlike subsection 794(a), subsection 794(b) does not require that an offender have “intent or reason to believe” that the disclosed national defense information will be “used to the injury of the United States or to the advantage of a foreign nation”;

248. *Id.* at 1064–65 (discussing differences between 18 U.S.C. § 793 (1988) and 18 U.S.C. § 794 (1988)).

249. 18 U.S.C. § 794(a) (2000).

250. Edgar & Schmidt, *supra* note 220, at 943.

251. *Id.* at 943–44.

252. *Id.* at 944.

253. *Id.*

instead, it is sufficient that the offender have the intent that the information “shall be communicated to the enemy,” and it is sufficient if the information “might be useful to the enemy.” The Espionage Act fails to define who constitutes an “enemy,” and in the “war on terror,” this is an endlessly elastic concept.²⁵⁴

Significantly, subsection 794(b) punishes anyone who “publishes” military information. It is unclear from the plain language of the statute whether this provision was meant to apply to the press. The use of the word “publish” is an indication that it was intended to apply to the press; on the other hand, if that were Congress’s intent, it is odd that Congress would saddle the Department of Justice with the requirement that it prove the press specifically “intended” to communicate with the enemy, rather than with the general public.²⁵⁵ Trying to communicate with its readership and to make money would not be a sufficient basis for a prosecution against the press based on this provision.²⁵⁶ That said, § 793(b) could apply to “disloyal” papers—especially foreign-language papers that are suspected of having allegiance to the enemy.²⁵⁷ Indeed, the Trading with the Enemy Act of 1917, which required foreign language newspapers to submit translations before publication, indicates that Congress was indeed concerned with treasonous newspapers.²⁵⁸

3. Section 798

Section 798 specifically bans the dissemination of “classified information . . . concerning the communications intelligence activities of the United States.” Section 798 explicitly applies to anyone who “publishes” this specific category of national defense information.

The scope of this statute is staggering. Unlike many other Espionage Act provisions, this subsection does not require an offender to have “intent or reason to believe” that the publication would harm the United States or provide an advantage to a foreign power. The only intent requirement is that the publication be “knowingly and willfully,” which is easily satisfied in cases involving the media. In addition, section 798 does not require a showing that the information was properly classified,²⁵⁹ or that even if at one time it was properly classified, that classification is still appropriate. For example, the statute does not distinguish between communications intelligence information that was classified last year, and similar information that was classified during World War II. In addition, the statute’s definition of classified, which includes information or material “that the person knows or has reason to believe has been properly classified by appropriate authorities,” could sweep in information that

254. *Id.* at 944–45.

255. *Id.* at 946.

256. *Id.* at 965.

257. *Id.* at 965–66.

258. *Id.*

259. *United States v. Boyce*, 594 F.2d 1246, 1251 (9th Cir. 1979) (“Under section 798, the propriety of the classification is irrelevant. The fact of classification of a document or documents is enough to satisfy the classification element of the offense.”). Section 797, which prohibits the publication of photographs or any representation of a military installation or equipment that the President has declared “as requiring protection against the general dissemination of information relative thereto,” also lacks an intent requirement. 18 U.S.C. § 797 (2000).

has not actually been classified. Finally, the statute does not require any showing that the disclosure of the information would pose any harm whatsoever to the United States' national security interests. Although by referring to "classified" information the statute arguably incorporates any potential harm standard into the Executive's classification scheme, this scheme is constantly subject to change.

Gabriel Schoenfeld has argued that section 798 could be used to prosecute the *New York Times* reporters who revealed that the National Security Agency was conducting wiretapping outside the constraints of the Federal Intelligence Security Act.²⁶⁰ If section 798 can be reasonably interpreted to cover the NSA wiretapping program—which certainly seems plausible—the *New York Times* would face potential liability under this section unless it could show that the statute was otherwise unconstitutional.

C. Atomic Energy Act

The Atomic Energy Act of 1954 protects the secrecy of information relating to nuclear energy and weapons.²⁶¹ Because the secrecy provisions of this Act are identical to those contained in the Atomic Energy Act of 1946, it is essential to look at the legislative history of the 1946 Act for guidance.

Before August 5, 1944, when the atomic bomb was dropped on Hiroshima, neither Congress nor the general public was aware that atomic energy or atomic weapons were possible.²⁶² The atomic bomb had been developed in secret by scientists working under military supervision as part of the Manhattan Project.²⁶³ Although the bulk of the legislation passed to deal with the new problem of atomic energy and weapons concerned whether the administration and control of such technology should be in military or civilian hands,²⁶⁴ there was much debate over the provisions governing the dissemination of atomic weapons information. Indeed, one of the primary battlegrounds between scientists and government officials was whether scientific information concerning nuclear science would be openly available or tightly controlled by the Pentagon.²⁶⁵ Although few scientists argued for the complete declassification of atomic weapons information, many argued that scientists were in a much better position than government officials to tell what was truly a "secret," and that too much secrecy could undermine their ability to conduct research.²⁶⁶ Others argued that only

260. Gabriel Schoenfeld, *Has the "New York Times" Violated the Espionage Act?*, COMMENTARY, March 2006, at 26.

261. See 42 U.S.C. §§ 2011-2297h (2000).

262. Byron S. Miller, *A Law is Passed: The Atomic Energy Act of 1946*, 15 U. CHI. L. REV. 799, 801 (1948).

263. *Id.*

264. *Id.* at 817-19.

265. Howard Morland, *Born Secret*, 26 CARDOZO L. REV. 1401, 1402 (2005).

266. See, e.g., *Atomic Energy: Hearing on H.R. 4280 Before the H. Comm. On Military Affairs*, 79th Cong. 98 (1945) [hereinafter *Statement of Harold Anderson*] (Statement of Harold Anderson, Ph.D., of the University of Chicago, Santa Fe, N.M.) ("The greatest progress in understanding comes from research coupled with the fullest and most free discussion and dissemination of its results and the related ideas."); see also Miller, *supra*, note 262, at 810-13. Miller mentions that during the Manhattan Project an entire laboratory might have exploded had one group of scientists not illicitly leaked information to another. *Id.* at 811. Harold Anderson also argued that excessive secrecy could actually harm our national security interests by causing

government control could adequately protect our national security interests, suggesting that some atomic energy information had already been leaked from Oak Ridge National Laboratory.²⁶⁷ Secretary of Defense Patterson argued before Congress that atomic weapons information was more sensitive than any other kind of information, including information pertaining to bacteriological warfare.²⁶⁸ From the beginning of this debate, the American public was quick to accept the notion that keeping this information secret was essential to protect against nuclear warfare.²⁶⁹ A commentator, writing shortly after the Atomic Energy Act of 1946 was passed, noted that “an early propaganda coup was scored when the words ‘security’ and ‘secrecy’ became interchangeable in this field.”²⁷⁰

Because government and military officials convinced Congress that the Espionage Act offered an inadequate safeguard of atomic energy information and that the difficulties of amending the Espionage Act to cover all national security information appeared insurmountable without interfering with the First Amendment,²⁷¹ specific provisions prohibiting the communication and dissemination of such information were included in the Atomic Energy Act. The policy provisions of the Act governing the control of atomic information recognized the tension between “control[ling] the dissemination of restricted data in such a manner as to assure the common defense and security” and permitting the dissemination of atomic energy information “to provide that free interchange of ideas and criticisms . . . essential to scientific progress.”²⁷² The first draft of the Senate bill divided nuclear information into two categories: basic scientific information that was to remain in the public domain and technical data concerning the design and manufacture of bombs.²⁷³ The Senate ultimately rejected

foreign governments to become suspicious. *Statement of Harold Anderson, supra*, at 99 (“In the eyes of a foreign government, the enactment of legislation which shields possible military activities of a government behind a cloak of secrecy is itself an act of aggression” and is “fraught with just the dangers of mutual suspicion which we must endeavor from the beginning to wipe out”).

267. Miller, *supra* note 262, at 814–15.

268. *Atomic Energy Act of 1946: Hearings on S. 1717 Before the S. Spec. Comm. on Atomic Energy*, 79th Cong. 406 (1946) [hereinafter *Atomic Hearings*] (testimony of Secretary of War Robert Patterson) (“I don’t regard anything as important under present conditions as the atomic bomb.”).

269. Miller, *supra* note 262, at 810.

270. *Id.* This continues to be the modern public understanding. When the Court of Appeals for the Second Circuit asked Alexander Bickel—who was representing the *New York Times* in the *Pentagon Papers* case—to give an example of information that could be subjected to a prior restraint, he suggested a scenario in which “the hydrogen bomb turns up.” Transcript of Oral Argument at 44–45, *United States v. New York Times*, 444 F.2d 544 (2d Cir. 1971) (No. 71-1617), *reprinted in* 2 *THE NEW YORK TIMES COMPANY v. UNITED STATES, A DOCUMENTARY HISTORY*, at 929–30 (James C. Goodale ed., Arno Press 1971).

271. *See Atomic Hearings, supra* note 268, at 86–87 (testimony of Secretary of the Navy James Forrestal); 92 CONG. REC. 6096 (1946) (testimony of Secretary of War Robert Patterson) (expressing concern that the Espionage Act did not permit prosecution of government employees who disseminated national security information, rather than documents, without a specific level of intent). Specifically, some were concerned that the Espionage Act required employees disseminating “information” to do so with a specific level of intent. *Id.*

272. Atomic Energy Act, Pub. L. No. 79-585, § 10(a), 60 Stat. 755, 766 (1946).

273. Atomic Energy Act, S. 1717, 79th Cong. § 10(b) (1946). Congress also considered empowering the Atomic Energy Commission to issue regulations declaring what information

this distinction and instead created a special category of sensitive information called “Restricted Data,” which is defined as “all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy.”²⁷⁴ This definition does not distinguish between information generated by the government and information generated by private scientists, or between information that is obtained from publicly available sources and that obtained from classified sources,²⁷⁵ leading some to note that information concerning a nuclear bomb can be “born classified.”²⁷⁶

The Act subjects to criminal penalties anyone who “communicates, transmits, or discloses” documents or information “involving or incorporating restricted data” with the “intent to injure the United States” or advantage a foreign nation,²⁷⁷ or who has “reason to believe such data” would have that effect.²⁷⁸ Those who act with “intent” to advantage a foreign nation or harm the United States face possible life imprisonment and a \$100,000 fine, while those who act with merely “reason to believe” that the information could advantage a foreign nation face a maximum of ten years in jail and a \$50,000 fine; the legislative history does not indicate why Congress made this distinction. This section applies regardless of whether the offender obtained the documents or information at issue “lawfully or unlawfully.”²⁷⁹ Those who receive, attempt to receive, or conspire to receive documents or information “involving or incorporating Restricted Data” can also be prosecuted under another provision provided they act “with intent to injure the United States or with intent to secure an advantage to any foreign nation.”²⁸⁰ Government employees, contractors, and military officials can be punished for “knowingly” communicating Restricted Data to any person not authorized to receive it as long as the offender did so “knowing or having reason to believe that such data is Restricted Data.”²⁸¹ In such a case, it is not necessary that a person communicate Restricted Data with the intent to harm the United States or advantage a foreign nation, or with reason to believe the communication would have such effect. The Act also specifically authorizes the government to obtain injunctive relief to prevent any violations of its provisions.²⁸²

In *United States v. Progressive, Inc.*, a federal district court relied on the Atomic Energy Act to grant a preliminary injunction to prevent the publication of a magazine article describing a method of manufacturing and assembling a hydrogen bomb.²⁸³ *The*

could and could not be disseminated, but there were concerns that such an approach might threaten freedom of speech and press by permitting the Commission to act arbitrarily and requiring people to be aware of the constantly changing regulations. 92 CONG. REC. 6096 (1946).

274. 42 U.S.C. § 2014(y) (2000).

275. Roger Funk, *National Security Controls on the Dissemination of Privately Generated Scientific Information*, 30 UCLA L. REV. 405, 420–21, 434 (1982).

276. L.A. Powe, Jr., *The H-Bomb Injunction*, 61 U. COLO. L. REV. 55, 56 (1990).

277. 42 U.S.C. § 2274 (2000).

278. *Id.* § 2274(b).

279. *Id.* § 2274.

280. *Id.* § 2275.

281. *Id.* § 2277.

282. *Id.* § 2280.

283. 467 F. Supp. 990 (W.D. Wis. 1979). Unlike the Espionage Act, the Atomic Energy Act specifically authorizes the Attorney General to seek injunctive relief against someone who “has engaged or is about to engage” in any violation of its provisions. 42 U.S.C. § 2280. The district

Progressive was an anti-war and anti-militarism publication that had wanted to demonstrate two things: (1) the production of a hydrogen bomb was so complex and expansive that only large governments could afford to produce them; and (2) the basics of nuclear fission and the configuration of a hydrogen bomb were not, in fact, secret.²⁸⁴ The editors of *The Progressive* had commissioned Howard Morland to write an article about the hydrogen bomb, and when they received it, they decided to clear the article with the Department of Energy (DOE) before publishing it.²⁸⁵ The DOE claimed that Morland's article contained Restricted Data, as defined in the Atomic Energy Act, even though Morland had no access to classified information and instead had cobbled together publicly available information.²⁸⁶ *The Progressive* informed the DOE that it would publish the full article unless the DOE got an injunction.²⁸⁷ The DOE decided to do just that, and successfully convinced a federal district court to enter an injunction restraining the article's publication.²⁸⁸

In reaching its holding, the court concluded that the "communicates, transmits, or discloses" language of the statute encompasses publication in a magazine,²⁸⁹ and that the magazine had "reason to believe" that the publication could harm the United States or give an advantage to a foreign nation.²⁹⁰ In considering the damage to First Amendment rights, the district court concluded that there was "no plausible reason why the public needs to know the technical details about hydrogen bomb construction to carry on an informed debate on this issue."²⁹¹ The court accepted the government's argument that even though at least some of the information in the article had been declassified or was in the public domain, the article provided "vital information on key concepts involved in the construction of a practical thermonuclear weapon" that would enable other nations to develop a hydrogen bomb more quickly and thereby cause "direct, immediate and irreparable damage to the United States."²⁹²

The government ultimately abandoned its case against *The Progressive* because other publications revealed the same information while appellate review was pending.²⁹³ *The Progressive* eventually published its article, and none of the dire consequences the government had predicted occurred.²⁹⁴ Some commentators have

court held that it would have granted prior restraint even in the absence of an authorizing statute because of the likelihood of "grave, direct, immediate and irreparable harm to the United States." *Progressive*, 467 F. Supp. at 996.

284. Erwin Knoll, *The H-Bomb and the First Amendment*, 3 WM. & MARY BILL RTS. J. 705, 705-07 (1994). Erwin Knoll, the editor of THE PROGRESSIVE, said that the article was intended to counteract the popular belief "that there is an 'H-Bomb secret' that can be written down on the back of an envelope (or in a magazine article)," and that "[i]f that 'secret' were to fall into the wrong hands . . . we'd all be in a heap of trouble." *Id.* at 706.

285. HOWARD MORLAND, *THE SECRET THAT EXPLODED* 145 (1981).

286. Powe, *supra* note 276, at 56.

287. *Id.*

288. *Id.*

289. *United States v. Progressive, Inc.*, 467 F. Supp. 990, 994 (W.D. Wis. 1979) (quoting 42 U.S.C. § 2274 (1969) (amended 2000)).

290. *Id.* at 999.

291. *Id.* at 994.

292. *Id.* at 996.

293. Ian M. Dumain, *No Secret, No Defense: United States v. Progressive*, 26 CARDOZO L. REV. 1323, 1332 (2005).

294. Gregg Easterbrook, *The Atomic Club: If the Bomb Is So Easy to Make, Why Don't More Nations Have It?*, N.Y. TIMES, Jan. 4, 2004, at WK1.

pointed out that this is because the real obstacle to creating nuclear weapons is not the lack of knowledge of how to do it, but having access to the necessary materials.²⁹⁵ The *Progressive* case reveals that it is not always so clear that information concerning atomic weapons is as secret—nor as categorically deserving of secrecy—as the general public appears to assume.

D. Intelligence Identities Protection Act

The Intelligence Identities Protection Act of 1982 (IIPA) prohibits the identification of covert agents.²⁹⁶ This legislation was enacted after mounting concerns about the publication of the names of American agents in books and magazines designed to disrupt intelligence activities in foreign countries.²⁹⁷ For example, the *Covert Action Information Bulletin* had been publishing lists of names of covert agents.²⁹⁸ At the same time, revelations concerning the CIA's involvement in conducting drug experiments on unsuspecting people, intercepting American communications overseas, and spying on American citizens, as well as the FBI's counterintelligence covert action program directed against Americans (COINTELPRO), made the debate over criminalizing the unmasking of covert CIA agents more complex than it might have appeared at first blush. In addition, the identity of CIA agents is often easily discoverable from publicly available documents.²⁹⁹

Although in the government's view the Espionage Act already governed such activities, the Department of Justice wanted a statute that eliminated some of the intent requirements of that legislation, as section 798 of the Espionage Act did with respect to communications and cryptographic information, and that explicitly applied to publication in a newspaper, magazine, or book.³⁰⁰

The first two provisions of the IIPA are directed at past or present government employees, contractors, or military officials. They prohibit anyone with authorized access to classified information that identifies a covert agent from disclosing that

295. E.g., Anthony R. Klein, *National Security Information: Its Proper Role and Scope in a Representative Democracy*, 42 FED. COMM. L.J. 433, 449 (1989).

296. 50 U.S.C. §§ 421-26 (2000).

297. Charles Mohr, *Issue and Debate: Disclosing Intelligence Agents' Names*, N.Y. TIMES, Feb. 6, 1981, at A10 (noting that Congress began to consider the IIPA soon after an agent in Athens was killed and another in Jamaica was attacked following the disclosure of their identities).

298. *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. 54 (1980) [hereinafter *Proposals to Criminalize*] (questioning by Rep. Wyche Fowler) (“[A]nybody and everybody can call himself a journalist and publish anything they want to”); see also Mohr, *supra* note 297 (commenting on the disclosure of eight senior CIA officials in the *Covert Action Information Bulletin*).

299. John Crewdson, *Internet Blows CIA Cover*, CHI. TRIB., Mar. 12, 2006, at C1 (explaining how easy it is to discover the identity of CIA agents through the internet); Mohr, *supra* note 297 (noting that former CIA agent John Stockwell claimed that the agency was “flagrantly careless” about protecting the cover of its agents and protecting their security).

300. *Intelligence Identities Protection Legislation: Hearings on S. 2216, et al., Before the S. Select Comm. on Intelligence*, 96th Cong. 18–19 (1980) [hereinafter *S. 2216 Intelligence Hearings*] (testimony of Associate Deputy Attorney General Robert L. Keuch).

information to any individual not entitled to receive it. The discloser of information must have knowledge that the information identifies the agent and that the United States is taking affirmative steps to conceal the identity of that agent.³⁰¹ Individuals subject to this provision are likely to be government employees.

The third provision of the IIPA, § 421(c), prohibits anyone outside the government, “in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States,” from disclosing information identifying a covert agent to anyone not entitled to receive classified information.³⁰² This portion of the statute is not limited to the disclosure of classified information. As the committee report explained, a person could be prosecuted under this statute for publishing information obtained, for example, through a “comprehensive counterintelligence effort of engaging in physical surveillance, electronic surveillance abroad, and other techniques of espionage directed at covert agents.”³⁰³

During the debates surrounding this legislation, Congress repeatedly expressed its concern that any statute it passed regarding the identification of covert agents not cover any constitutionally protected speech, such as academic studies or reports in the media of intelligence failures.³⁰⁴ Earlier proposed versions required the government to prove that the disclosure of the identity of a covert agent was made “with intent to impair or impede foreign intelligence activities.”³⁰⁵ The government complained that such a standard would lead to several problems. On one hand, an intent requirement posed a possible conflict with the First Amendment because a “mainstream journalist”³⁰⁶ might fear that other stories he has written that are critical of the United States could be used as evidence of a bad intent.³⁰⁷ At the same time, the government argued, this intent standard could make it unduly difficult to prove beyond a reasonable doubt that a defendant intended to impede foreign intelligence activities, and it might facilitate defendants’ attempts to engage in “graymail” in trying to prove that the disclosure was made with an intent to reform the government rather than to impede it.³⁰⁸

301. 50 U.S.C. § 421(a)-(b) (2000).

302. 50 U.S.C. § 421(c) (2000).

303. Jerry J. Berman & Morton H. Halperin, *The Agents Identities Protection Act: A Preliminary Analysis of the Legislative History*, FIRST AMENDMENT AND NATIONAL SECURITY, May 1984, at 41, 51–52 (1984).

304. *Id.* at 41–55.

305. *Proposals to Criminalize*, *supra* note 298, at 156, 158; *see also* H.R. REP. NO. 96-1219, pt. 1, at 2, 6–7 (1980).

306. Floyd Abrams criticized the government for assuming that only “mainstream” journalists would be entitled to First Amendment protection. *Intelligence Identities Protection Act, S. 2216: Hearing Before the S. Comm. on the Judiciary*, 96th Cong. 117 (1980) [hereinafter *S. 2216 Judiciary Hearing*] (statement of Floyd Abrams).

307. *S. 2216 Intelligence Hearings*, *supra* note 300, at 22 (testimony of Associate Deputy Attorney General Robert L. Keuch); *see also Intelligence Identities Protection Act: Hearings on H.R. 5615 Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 96th Cong. 98 (1980) (written statement of Associate Professor Ford Rowan, Northwestern University) (noting that sometimes the media *wants* to “impair and impede” an intelligence activity that undermines the moral stature of the United States) (emphasis in original).

308. Berman & Halperin, *supra* note 303, at 43. Prosecutors who are “graymailed” may instead choose not to pursue a case. Floyd Abrams, a prominent First Amendment lawyer,

In an effort to avoid these problems, the bill was amended to provide what was seen as a more objective “reason to believe” intent requirement.³⁰⁹ Floyd Abrams argued that this change did little to protect journalists.³¹⁰ “Reason to believe” that the disclosure of a covert agent would “impair our intelligence efforts” could easily exist, Abrams argued, even when a reporter reveals agents who are spying on American citizens or committing assassinations in the United States.³¹¹ Perhaps in response to Abrams’s concerns, the conference report specifically noted that “[a] government warning to a news reporter that a particular intended disclosure would impair or impede foreign intelligence activities” could be submitted to the jury as evidence to prove the requisite intent, but the government would still have to provide “objective facts about likely harm.”³¹²

In addition, Congress required that individuals without a government affiliation would have to have exposed the identities of covert agents as part of a “pattern of activities” requirement—defined in the statute as “a series of acts with a common purpose or objective.”³¹³ Earlier versions of the IIPA provided simply that a defendant made such disclosures “in the course of an effort” to identify covert agents.³¹⁴ By changing the statute to require a “pattern of activities,” Congress attempted to limit the applicability of the statute to those who “make it their business to ferret out and publish the identities of agents,” without “affect[ing] the First Amendment rights of those who disclose the identities of agents as an integral part of another enterprise such as news media reporting of intelligence failures or abuses, academic studies of U.S. government policies and programs, or a private organization’s enforcement of its internal rules.”³¹⁵ The committee report also indicated that a reporter would “rarely” have the requisite intent to “identify and expose covert agents,” as the law requires.³¹⁶ The government’s proof that a reporter had that intent could be rebutted by evidence demonstrating an alternative, permissible intent, such as the intent to explain questionable government conduct.³¹⁷

The government has never prosecuted a member of the press under this statute. Recently Special Prosecutor Patrick Fitzgerald investigated a possible violation of this statute when Valerie Plame was identified as a CIA operative.³¹⁸

conceded that graymail was a possibility, but argued, “I think we are willing as a general matter to live with the proposition that guilty people might even get off because we think we are preserving some other very important rights.” *S. 2216 Intelligence Hearings, supra* note 300, at 82 (testimony of Floyd Abrams).

309. 50 U.S.C. § 421(c) (2000).

310. *S. 2216 Judiciary Hearing, supra* note 306, at 118 (statement of Floyd Abrams).

311. *Id.* at 117–18.

312. H.R. REP. NO. 97-580, at 10 (1982) (Conf. Rep.), as reprinted in 1982 U.S.C.C.A.N. 145, 175.

313. 50 U.S.C. § 426(10) (2000).

314. *The Intelligence Identities Protection Act: Hearing on H.R. 4, Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 97th Cong. 140 (1981).

315. Berman & Halperin, *supra* note 303, at 50–51.

316. *Id.* at 52.

317. *Id.* at 53.

318. In the course of this investigation, Fitzgerald successfully subpoenaed the testimony and notes of several reporters, including Judith Miller and Matthew Cooper. Miller served 85 days in jail before she revealed the identity of her source. David Johnston & Douglas Jehl, *Times Reporter Freed from Jail, She Will Testify*, N.Y. TIMES, Sept. 30, 2005, at A1.

E. Federal Larceny Statute

The federal larceny statute, 18 U.S.C. § 649, imposes criminal penalties not only on anyone who “embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof,” but also on anyone who “receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted.”³¹⁹ Although the statute, passed in 1875, does not explicitly mention classified information, and nothing in its legislative history indicates that Congress intended the statute to apply to government information,³²⁰ some lower courts have read the statute to apply to both tangible and intangible government information.³²¹ Whether the government has a legitimate, protectable property interest in its documents—or the information contained in its documents—is not an easy question.³²²

F. Inchoate Liability Provisions

The AIPAC case has reminded the press that it is not only vulnerable to prosecution under the Espionage Act, but it is also susceptible to “aiding and abetting” and conspiracy charges whenever it obtains information from a source who violates federal law by disclosing the information to the press.³²³ Under 18 U.S.C. § 2, “[w]hoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.” In addition, §§ 793(g) and 794(c) of the Espionage Act authorize prosecutions for conspiracies to violate the provisions in those subsections.

Notably, the IIPA specifically prohibits aiding and abetting or conspiracy charges in connection with a violation of the Act except when, “in the case of a person who acted in the course of a pattern of activities,” intended to expose covert agents with reason to believe the disclosure would impair or impede U.S. foreign intelligence activities.³²⁴

319. 18 U.S.C. § 649 (2000).

320. Michael E. Tigar, *The Right of Property and The Law of Theft*, 62 TEX. L. REV. 1443, 1463 (1984).

321. See, e.g., *United States v. Fowler*, 932 F.2d 306, 310 (4th Cir. 1991) (recognizing that because “information is a species of property and a thing of value,” and that “conversion and conveyance of governmental information can violate § 641”); *United States v. Morison*, 844 F.2d 1057, 1077 (4th Cir. 1988) (holding that § 641 applies to maps and photographs); *United States v. Girard*, 601 F.2d 69, 70–71 (2d Cir. 1979). Some courts have dodged the issue by holding that the use of government computers and copy machines to make copies constituted a violation of the statute, regardless of what information was contained in the documents. *United States v. DiGilio*, 538 F.2d 972 (3d Cir. 1976).

322. See Tigar, *supra* note 320, at 1466–68 (discussing the difficulties inherent in declaring a government property right in information).

323. Subsection 793(g) specifically criminalizes the conspiracy to commit any of the offenses listed in § 793. 18 U.S.C. § 793 (2000).

324. 50 U.S.C. § 422(b) (2000).

IV. CURRENT FIRST AMENDMENT DOCTRINE

Although the courts have not expressly addressed the constitutionality of prosecuting the press for publishing classified national security information or for aiding and abetting in the violation of any of the statutes mentioned above, current First Amendment jurisprudence suggests some constitutional limitations on the government's prosecutorial powers. The scope of these limitations is unclear, however, and the Court has indicated that no defense can be particular to the "press" as an institution.

A. Speech Concerning National Security Information is Protected Speech

In its brief in opposition to the defendants' motion to dismiss the indictment in the AIPAC case, the government argued that the disclosure of classified national security information fell completely outside the protection of the First Amendment.³²⁵ The district court correctly rejected this contention out of hand, emphasizing that the right to gather and disseminate information concerning United States foreign policy is a core value of the First Amendment.³²⁶ Judge Ellis noted that representative government requires open and well-informed discussions, particularly in the area of foreign policy, where often the only check on executive power is an informed citizenry.³²⁷ Simply invoking the need for secrecy to protect national security interests does not eliminate the need for constitutional scrutiny,³²⁸ Judge Ellis explained, especially given the government's tendency to over-classify and to withhold information it does not want the public to hear.³²⁹

Judge Ellis's analysis is undeniably correct. The government's asserted interest in protecting the national security of the country does not render the First Amendment inapplicable. National security information generally can be extremely high value speech, and its disclosure to the public often promotes a deliberative democracy. Furthermore, to permit the government to restrict any speech that involves national security would give the government too much power to hide its actions from public scrutiny. As the Fourth Circuit has said, "[h]istory teaches us how easily the spectre of a threat to 'national security' may be used to justify a wide variety of repressive government actions."³³⁰

325. Government's Supplemental Response to Defendants' Motion to Dismiss the Superseding Indictment at 22–30, *United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006) (No. 1:05cr225).

326. *United States v. Rosen*, 445 F. Supp. 2d 602, 630 (E.D. Va. 2006).

327. *Id.* at 633.

328. *Id.* at 630–34.

329. *Id.* at 633.

330. *In re Washington Post Co.*, 807 F.2d 383, 391 (4th Cir. 1986); *see also* Louis Henkin, *Foreign Affairs*, in 2 *ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION*, 747, 754 (Leonard W. Levy, Kenneth L. Karst & Dennis J. Mahoney eds., 1987) ("Nothing in the Constitution suggests that the rights of individuals in respect of foreign affairs are different from what they are in relation to other exercises of government power.").

B. The Pentagon Papers Case

The Supreme Court has explicitly addressed the intersection of the First Amendment rights of the press and the need to protect national security in only one case, *New York Times Co. v. United States*. In this case, the Court rejected the government's request for a prior restraint enjoining the publication of the Pentagon Papers, which consisted of volumes of documents detailing the history of the involvement of the United States in Vietnam.³³¹ Perhaps due to the speed with which the case was submitted to the Court, argued, and decided, a majority of Justices agreed on only one thing: that the government could obtain a prior restraint in only the most compelling circumstances. The Court held in a brief *per curiam* opinion that the government must bear the "heavy burden of showing justification" when seeking to enforce a prior restraint against the publication of classified national security information, and that the government had not met its burden in that case.³³²

In the nine separate opinions that followed the *per curiam* decision, many important issues concerning the scope of the First Amendment's protection for the publication of national security information were left unresolved. Most significantly, the Court did not reach the issue of whether the defendants could be punished after the fact for publishing the contents of the Pentagon Papers. Only Justices Black and Douglas would protect the press from criminal laws punishing the publication of classified information as well as prior restraints.³³³ They argued that the very purpose of the First Amendment was to protect the ability of the press to "bare the secrets of government and inform the people,"³³⁴ and that "[s]ecrecy in government is fundamentally anti-democratic, perpetuating bureaucratic errors."³³⁵ Justice Brennan, in contrast, rested his decision specifically on the disfavored status of prior restraints (as opposed to criminal prosecutions after the fact of publication). He stated he would permit a prior restraint on proof that publication would "inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea."³³⁶ Brennan drew this standard from dicta in the Court's prior opinion in *Near v. Minnesota*, in which the Court states that prior restraints are permissible in cases involving "actual obstruction to [the government's] recruiting service or the publication of the sailing dates of transports or the number and location of troops."³³⁷

Although Justice Brennan did not indicate what the government's burden would be for a criminal prosecution, the three remaining concurring Justices—Justices Stewart, White, and Blackmun—specifically noted that the government would not necessarily have to meet the same burden of proof to obtain a criminal conviction as it would to obtain a prior restraint.³³⁸ These votes, combined with the votes of the three dissenting

331. 403 U.S. 713 (1971) (*per curiam*).

332. *Id.* at 714 (quoting *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971)).

333. *Cf. id.* at 719 (Black, J., concurring) (agreeing with the Court's prior decision not to allow criminal punishment of a man who attended a Communist meeting).

334. *Id.* at 717 (Black, J., concurring).

335. *Id.* at 724 (Douglas, J., concurring).

336. *Id.* at 726–27 (Brennan, J., concurring).

337. 283 U.S. 697, 716 (1931).

338. *See New York Times*, 403 U.S. at 737–40 (White J., concurring) (noting that the procedures governing a criminal trial render criminal prosecution preferable to prior restraints); *id.* at 759 (Blackmun, J., dissenting) (agreeing with White's statement discouraging prior

Justices who would have allowed the prior restraint, have led some courts and commentators to conclude that the First Amendment is no obstacle to a subsequent criminal prosecution against the press.

The Court also left unclear whether it was at all relevant *how* the newspapers obtained the Pentagon Papers. The origin of these documents is left unstated, aside from a brief reference in Justice Harlan's dissenting opinion.³³⁹ The failure to address the origin of the materials is curious, especially given that Solicitor General Griswold emphasized their tainted origin throughout his oral argument before the Court.

Given all of this uncertainty, it is obvious that the press cannot be confident that the Supreme Court would hold that a criminal prosecution of the press for the publication of national security information is unconstitutional. But there is a possible reading of the Pentagon Papers case that would protect the press from most criminal prosecutions. Primarily, if in fact there is no good constitutional reason to distinguish between prior restraints and subsequent prosecution, the very high standard the Court set for prior restraints³⁴⁰ should apply equally to criminal prosecutions. Although the Supreme Court has continued to maintain that there is a meaningful distinction between prior restraints and subsequent punishments,³⁴¹ it is by no means clear how meaningful the distinction is or how much weight should be given to it.³⁴² Indeed, several Justices

restraints). Their statements appeared to warn the *New York Times* and *Washington Post* that the First Amendment would serve as no bar to criminal prosecutions against them after publication. *Id.* at 733 (White, J., concurring) ("That the Government mistakenly chose to proceed by injunction does not mean that it could not successfully proceed in another way."). Although the source of the Pentagon Papers, Daniel Ellsberg, was ultimately prosecuted (the prosecution was dismissed based on government misconduct), the government never attempted to indict the newspapers.

339. *Id.* at 754 (Harlan, J., dissenting) (mentioning that the documents at issue "were purloined from the Government's possession and that the newspapers received them with knowledge that they had been feloniously acquired"); Louis Henkin, *The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers*, 120 U. PA. L. REV. 271, 277 (1971) ("We are not told whether and how much it would matter were it determined that [the Pentagon Papers] were obtained without the Government's consent, that they were taken or copied in violation of such governmental 'title' or right.").

340. See ALEXANDER M. BICKEL, *THE MORALITY OF CONSENT* 61 (1975).

341. *Alexander v. United States*, 509 U.S. 544, 553–54 (1993) ("[O]ur decisions have steadfastly preserved the distinction between prior restraints and subsequent punishments. Though petitioner tries to dismiss this distinction as 'neither meaningful nor useful,' . . . we think it is critical to our First Amendment jurisprudence."). In at least one prior opinion, the Court had indicated that the government had to meet the same high burden to restrict speech whether it attempted to do so through a prior restraint or through penal sanctions. See, e.g., *Smith v. Daily Mail*, 443 U.S. 97, 101–02 (1979) (holding that even when a speech restriction is properly categorized as a penal sanction rather than a prior restraint, the government must still demonstrate "the highest form of state interest to sustain its validity").

342. Many commentators have questioned whether there is a meaningful distinction between prior restraints and subsequent criminal punishment. See, e.g., John Calvin Jeffries, Jr., *Rethinking Prior Restraint*, *FIRST AMENDMENT AND NATIONAL SECURITY*, May 1984, at 15, 26–27 (arguing that a directed injunction may in fact deter only the speech that is the subject of the injunction, while the threat of subsequent criminal prosecution might deter even more speech); Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"*, 58 B.U. L. REV. 685, 727 (1978) (noting that "[u]nchecked discretion, vague standards and incompetent administration, while frequently associated with the system of prior restraint, can just as easily exist in a system of subsequent punishment"); but see Vincent Blasi, *Toward a*

have rejected a “formalistic” distinction between prior restraints and subsequent criminal punishment because they both can raise exactly the same concerns: “the evils of state censorship and the unacceptable chilling of protected speech.”³⁴³

The biggest difference between a prior restraint and a subsequent prosecution is arguably the “collateral bar rule,” which prevents those held in contempt for violating an injunction from challenging its validity.³⁴⁴ But heavy criminal penalties for publishing national security information certainly could have a significant chilling effect. Although the government has rarely prosecuted the press for publishing classified information, the constitutionality of government action should not depend upon the judicious exercise of prosecutorial discretion. Indeed, it is by no means clear why the *New York Times* and the *Washington Post* were presumably willing to risk a criminal prosecution when they would not have been willing to violate an injunction.³⁴⁵ As Louis Henkin argued, “The distinction between prior injunction and subsequent publication is hallowed by history, but its application . . . would seem less than persuasive: while a criminal penalty more readily permits ‘civil disobedience,’ or reliance on the jury to acquit, stiff penalties will deter—and deny the right to know—almost as effectively as any injunction.”³⁴⁶

Given the slender difference between prior restraints and subsequent criminal punishment, particularly when it comes to information about our government that is at the heart of the First Amendment, the government should be required to carry the same “heavy burden” if it attempts to prosecute someone for publishing national security information as it would if it attempted to obtain a prior restraint against the publication of that same information. In other words, the government must show that the harm that the publication is likely to cause is grave, direct, and unavoidable.³⁴⁷

C. First Amendment Rights of Government Employees

Current First Amendment doctrine draws a sharp distinction between the First Amendment rights of those who have received access to classified information as a result of having a position of trust with the government—such as government employees and contractors—and everyone else. In a series of cases, the Supreme Court has endorsed the federal government’s authority to restrict the speech of its past and current employees, even when the employee reveals unclassified information or information that poses no actual harm to national security interests. At the same time, by emphasizing the trust relationship between the federal government and its

Theory of Prior Restraint: The Central Linkage, 66 MINN. L. REV. 11 (1981) (arguing that prior restraints are akin to licensing systems); Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 LAW & CONTEMP. PROBS. 648 (1955).

343. *Alexander*, 509 U.S. at 571–72 (Kennedy, J., dissenting).

344. See Stephen R. Barnett, *The Puzzle of Prior Restraint*, 29 STAN. L. REV. 539, 551–53 (1977) (explaining that those against whom an injunction is entered can challenge its validity only on direct appeal).

345. OWEN M. FISS, *THE CIVIL RIGHTS INJUNCTION* 71 (1978) (arguing that one could not generally expect ordinary citizens to be as willing to risk criminal prosecution).

346. Henkin, *supra* note 339, at 278.

347. See Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL. REV. 185, 202 (2007) (arguing that the difference between prior restraints and criminal prosecutions in the context of national security information has “less bite” than in cases involving obscenity and libel).

employees, the Court has indicated that a very different standard would apply to third parties who disclose classified information.

In *Snepp v. United States*, the Supreme Court held that the First Amendment does not invalidate non-disclosure agreements signed by a federal employee that require the employee to submit any manuscript to the government for pre-publication review to determine whether it contains any classified information.³⁴⁸ Frank Snepp was a former CIA employee who signed an agreement when he left the Agency agreeing that he would not publish any information relating to the Agency without obtaining prior approval.³⁴⁹ The CIA brought a lawsuit to enforce this contract when Snepp published a book about CIA activities in South Vietnam without first obtaining Agency approval, even though the Agency conceded for purposes of the litigation that the book did not in fact contain any classified information.³⁵⁰

The Court rejected Snepp's argument that the agreement amounted to an unconstitutional prior restraint, reasoning that through his employment Snepp had entered into a "trust relationship" with the government.³⁵¹ The Court held that even though the government could not constitutionally prohibit Snepp from publishing classified information, due to this trust relationship, the government had a right to review anything Snepp planned to publish about the CIA to make sure that nothing he said compromised national security information or sources.³⁵² The Court held that the agreement was a "reasonable means" of protecting the government's compelling interest in protecting national security information and the appearance of confidentiality essential for collecting foreign intelligence.³⁵³

Although *Snepp* made clear that the government would ultimately not be permitted to enjoin the publication of non-classified information, the Court has not made clear what standard the government must meet to enjoin the publication of classified information. Some lower court cases have suggested that the government must prove at a minimum that "the information was not already in the public domain and that the disclosure is potentially damaging to the national security."³⁵⁴ The "potentially damaging" standard is not a particularly onerous standard; it certainly does not rise to the level of the "imminent and grave threat to national security" standard that the Court set forth in the *Pentagon Papers* case.

Even outside of the national security context, the Supreme Court has accepted the government's argument that the ordinary rules of the First Amendment do not apply to its employees. In *Pickering v. Board of Education*, the Court held that the government

has interests as an employer in regulating the speech of its employees that differ significantly from those it possesses in connection with regulation of the speech of

348. 444 U.S. 507 (1980); *see also* *Haig v. CIA*, 453 U.S. 280 (1981) (holding that the Secretary of State can withhold the passport of a former CIA employee who revealed the identity of other CIA operatives); *United States v. Marchetti*, 466 F.2d 1309 (4th Cir. 1972) (upholding the constitutionality of secrecy agreement signed by former CIA employee requiring prior approval from the Agency for any publications).

349. *Snepp*, 444 U.S. at 508.

350. *Id.* at 510.

351. *Id.* at 510–11.

352. *Id.* at 511.

353. *Id.* at 510 n.3.

354. Stone, *supra* note 347, at 194.

the citizenry in general. The problem in any case is to arrive at a balance between the interests of the [public employee], as a citizen, in commenting upon matters of public concern and the interest of the [government], as an employer, in promoting the efficiency of the public services it performs through its employees.³⁵⁵

It is unclear what other limits there might be on the government's ability to restrict the speech of its employees. It is quite possible that a government employee has no duty to keep illegal activity confidential. Under the *Restatement of Agency*, "[a]n agent's duty of confidentiality is not absolute. . . . [A]n agent may reveal to law enforcement authorities that the principal is committing or is about to commit a crime."³⁵⁶ As Geoffrey Stone has pointed out, whether such a privilege exists in the context of government employment "is unexplored terrain."³⁵⁷ As a matter of constitutional interest balancing, when the program is in fact unlawful, the public's need to know outweighs the government's interest in secrecy. In addition, the classification scheme specifically prohibits the classification of illegal government practices.³⁵⁸ But even if a federal employee enjoys a privilege to reveal unlawful information, Stone argues, her whistle-blowing is not protected by the First Amendment if the employee is wrong and the government's conduct turns out to be legal.³⁵⁹

Whatever the scope of the government's power to restrict the First Amendment rights of its employees, the Court has been very explicit that a different First Amendment analysis applies to persons who have not voluntarily accepted a position of trust and a duty of confidentiality.³⁶⁰ Any prosecution against someone without a trust relationship with the government, therefore, must satisfy rigorous First Amendment standards.

D. Newsgathering Rights

The Court has never given a clear indication whether the First Amendment protects the right to gather information. In various cases the Court has defined the First Amendment as including the right to receive information,³⁶¹ but it has given very

355. 391 U.S. 563, 568 (1968).

356. RESTATEMENT (THIRD) OF AGENCY § 8.05 cmt. c (2006).

357. Stone, *supra* note 347, at 196.

358. *See* Exec. Order No. 13,292, § 1.7(a)(1), 68 Fed. Reg. 15,318 (Mar. 25, 2003) (forbidding classification for the purpose of concealing "violations of law, inefficiency, or administrative error").

359. Stone, *supra* note 347, at 196.

360. *See* *United States v. Aguilar*, 515 U.S. 593, 606 (1995) ("As to one who voluntarily assumed a duty of confidentiality, governmental restrictions on disclosure are not subject to the same stringent standards that would apply to efforts to impose restrictions on unwilling members of the public."); Stone, *supra* note 347, at 191 ("Unlike public employees, who have agreed to abide by constitutionally permissible restrictions of their speech, journalists and publishers have *not* agreed to waive their rights." (emphasis in original)).

361. *See, e.g.,* *Virginia Bd. of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976) (recognizing that the First Amendment protects both the right to impart as well as the right to receive a communication); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (noting that "[i]t is now well established that the Constitution protects the right to receive information and ideas"); *Martin v. Struthers*, 319 U.S. 141, 143 (1943) (explaining the freedom of speech press

mixed messages about whether the First Amendment protects the right to gather that information,³⁶² outside the context of certain criminal proceedings.³⁶³ Whatever the First Amendment right to gather information is, the Court has made one thing clear: the right belongs to the press and public equally.³⁶⁴

Some early First Amendment cases recognized the right of private entities to impart—and of the public to receive—information. For example, in *Grosjean v. American Press Co.*, the Court declared unconstitutional a state tax on the advertising revenues of newspapers.³⁶⁵ In reaching its holding, the Court explained that “informed public opinion is the most potent of all restraints upon misgovernment,” and that the tax, which was designed “to limit the circulation of information” to the public,³⁶⁶ went “to the heart of the natural right of the members of an organized society, united for their common good, to impart and acquire information about their common interests.”³⁶⁷ In other cases, the Court rejected a prohibition on door-to-door distribution of literature³⁶⁸ and the Postmaster’s detention of Communist propaganda.³⁶⁹ These cases recognized that the government cannot interfere with an individual’s constitutional right to receive information from a willing speaker. Although these cases emphasized the importance of an informed public in a democracy, none of them addressed whether the First Amendment gave the public the right to force the government to disclose information.

In other cases, the Court has indicated that the First Amendment does not invalidate generally applicable laws that interfere with newsgathering. In one of the first cases to address the First Amendment right to gather information, *Zemel v. Rusk*, the Court held that government restrictions on the right to travel to Cuba did not implicate any First Amendment right to gather information.³⁷⁰ Louis Zemel argued that he wanted to travel to Cuba to “satisfy [his] curiosity about the state of affairs in Cuba and to make [him] a better informed citizen.”³⁷¹ The Court rejected Zemel’s contention that the restrictions violated his First Amendment rights, reasoning that “to the extent that the Secretary’s refusal to validate passports for Cuba acts as an inhibition . . . it is an inhibition of action.”³⁷² The Court seemed particularly concerned about the ramifications of a contrary holding:

There are few restrictions on action which could not be clothed by ingenious argument in the garb of decreased data flow. For example, the prohibition of

“necessarily protects the right to receive [literature]”).

362. See *Zemel v. Rusk*, 381 U.S. 1, 17 (1965) (holding that government restrictions on travel to Cuba did not infringe the First Amendment rights of an educational tour group seeking information relevant to the debate on the Cuban embargo).

363. See, e.g., *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986); *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501 (1984); *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 581 (1980).

364. See Papandrea, *supra* note 216; Papandrea, *supra* note 66.

365. 297 U.S. 233 (1936).

366. *Id.* at 250.

367. *Id.* at 243.

368. *Martin v. Struthers*, 319 U.S. 141 (1943).

369. *Lamont v. Postmaster General*, 381 U.S. 301 (1965).

370. 381 U.S. 1 (1965).

371. *Id.* at 4.

372. *Id.* at 16.

unauthorized entry into the White House diminishes the citizen's opportunities to gather information he might find relevant to his opinion of the way the country is being run, but that does not make entry into the White House a First Amendment right. The right to speak and publish does not carry with it the unrestrained right to gather information.³⁷³

In *Branzburg v. Hayes*, journalists argued that they had a First Amendment privilege to refuse to reveal the identity of their confidential sources to a grand jury because compelling such testimony would deter future confidential sources from coming forward with information, "all to the detriment of the free flow of information protected by the First Amendment."³⁷⁴ The Court rejected the reporters' argument, at least in the context of grand jury proceedings, noting that the press "has no special immunity from the application of general laws."³⁷⁵ To confuse matters, the Court also noted that "without some [constitutional] protection for seeking out the news, freedom of the press could be eviscerated"³⁷⁶ and that "news gathering is not without its First Amendment protections."³⁷⁷

Justice Powell, who provided the crucial fifth vote for the majority, drafted a concurring opinion in which he appeared to endorse a case-by-case balancing test based on the First Amendment that would protect journalists from subpoenas at least in some instances. The dissenters expressly embraced the notion that the First Amendment provided the press with a right to gather information:

A corollary of the right to publish must be the right to gather news. The full flow of information to the public protected by the free-press guarantee would be severely curtailed if no protection whatever were afforded to the process by which news is assembled and disseminated. . . . [W]ithout freedom to acquire information the right to publish would be impermissibly compromised.³⁷⁸

Because four dissenting Justices would have recognized a privilege, some lower courts have read Powell's opinion as controlling and have at a minimum required "heightened scrutiny" of any subpoena to the press.³⁷⁹ Furthermore, almost every court has recognized that even if the privilege does not attach in grand jury proceedings, the constitutional balance tips in favor of recognizing the privilege in civil and administrative cases, where a defendant's countervailing Sixth Amendment rights are not at issue.³⁸⁰

In *Cohen v. Cowles Media Co.*, the Court again retreated from any notion that the press had any sort of First Amendment immunity from generally applicable laws.³⁸¹ In that case, Dan Cohen, a consultant to a political candidate, provided information concerning the criminal record of the opponent to two newspapers on the express

373. *Id.* at 16–17.

374. 408 U.S. 665, 681 (1972).

375. *Id.* at 683 (quoting *Associated Press v. NLRB*, 301 U.S. 103, 132 (1937)).

376. *Id.* at 681.

377. *Id.* at 707.

378. *Id.* at 727–28 (Stewart, J., dissenting).

379. *See Papandrea, supra* note 216, at 553.

380. *Id.* at 556–58.

381. 501 U.S. 663, 670 (1991).

condition that his identity remain confidential.³⁸² The two newspapers independently decided to include Cohen's identity in their story.³⁸³ Justice White, writing for a closely divided Court, held that the newspapers had no First Amendment immunity from Cohen's promissory estoppel claim. The Court rejected the media's contention that this case was governed by the *Daily Mail* line of cases (discussed below), which privileges the publication of truthful information when lawfully acquired. Instead, it held that this case was governed by "the equally well-established line of decisions holding that generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news."³⁸⁴ Justice White emphasized that this case did not involve a government restriction on what the press could publish but rather a contractual promise that the newspapers brought upon themselves.³⁸⁵ In addition, Justice White continued, "it is not at all clear that respondents obtained Cohen's name 'lawfully' in this case, at least for purposes of publishing it. Unlike the situation in *Florida Star*, where the rape victim's name was obtained through lawful access to a police report, respondents obtained Cohen's name only by making a promise that they did not honor."³⁸⁶ The Court concluded by noting that any restriction on the press's ability to publish newsworthy information was "no more than the incidental, and constitutionally insignificant, consequence of applying to the press a generally applicable law that requires those who make certain kinds of promises to keep them."³⁸⁷

Relying on cases like *Cohen*, the lower courts appear to be in general agreement that those in "the media have no general immunity from tort or contract liability."³⁸⁸ In reaching this conclusion, however, courts have emphasized that applying "run-of-the-mill" tort law to the press will have no more than an "incidental" effect on their newsgathering.³⁸⁹ Criminal prosecutions of the publication of national security information would have more than a mere "incidental" effect on newsgathering.

E. Protection for the Publication of "Lawfully Acquired" Information

In a series of cases, the Supreme Court has indicated that "state action to punish the publication of truthful information seldom can satisfy constitutional standards."³⁹⁰ Indeed, truthful speech on core matters of public concern is at the height of the hierarchy of speech the First Amendment protects.³⁹¹ The Court has carefully refrained from holding, however, that the First Amendment *always* protects the publication of

382. *Id.* at 665.

383. *Id.* at 666.

384. *Id.* at 669.

385. *Id.* at 670–71.

386. *Id.* at 671.

387. *Id.* at 672.

388. *Desnick v. Am. Broad. Cos.*, 44 F.3d 1345, 1355 (7th Cir. 1995).

389. *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 521 (4th Cir. 1999).

390. *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 102 (1979).

391. *See Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 773 (1976) ("[A] State may [not] completely suppress the dissemination of conceded truthful information about entirely lawful activity, fearful of that information's effect upon its disseminators and its recipients."); *New York Times Co. v. Sullivan*, 376 U.S. 254, 271–73 (1964) (holding that even false speech must be accorded some constitutional protection).

truthful information.³⁹² These cases therefore leave open the question whether a law prohibiting the publication of information relating to national defense can ever satisfy the high standards of the First Amendment.

The first of these cases was *Landmark Communications, Inc. v. Virginia*, which held that a state could not punish a third party who revealed information about confidential judicial misconduct proceedings.³⁹³ Under Virginia law, all proceedings of the state's judicial review commission were confidential, and anyone who divulged any such information was subject to criminal sanctions.³⁹⁴ The defendant newspaper had published the identity of a judge whose conduct was under investigation.³⁹⁵

The Court did not question the ability of Virginia to declare its judicial review proceedings confidential or to punish third parties who obtain information about the proceedings through illegal means or participants in the proceedings who leak information.³⁹⁶ Virginia claimed that its law had several purposes: (1) to encourage the filing of complaints and participation of witnesses who might otherwise fear recrimination or reprisal, (2) to protect the reputation of judges in cases involving complaints ultimately deemed frivolous or unfounded, and (3) to promote confidence in the judicial system by avoiding premature public disclosure of unexamined complaints.³⁹⁷ The Supreme Court also noted that the confidentiality provision reduces the workload of judicial review commissions by encouraging judges justifiably facing misconduct or disability allegations to resign or retire without the embarrassment of formal proceedings.³⁹⁸

Although the defendant asked the Court to hold that the First Amendment always prohibits the imposition of criminal sanctions for the truthful reporting about public officials, the Court held that it was "unnecessary" to make such a broad holding. Instead, it simply held that "the publication Virginia seeks to punish under its statute lies near the core of the First Amendment, and the Commonwealth's interests advanced by the imposition of criminal sanctions are insufficient to justify the actual and potential encroachments on freedom of speech and of the press which follow therefrom."³⁹⁹ The Court rejected Virginia's argument that it was necessary to restrict the speech of nonparticipants, in part because "much of the risk can be eliminated through careful internal procedures to protect the confidentiality of Commission proceedings."⁴⁰⁰

392. *E.g.*, *Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829, 840 (1978) (refusing to determine whether the First Amendment protects the publication of all truthful information and focusing instead on the particular circumstances of the case).

393. 435 U.S. 829 (1978).

394. *Id.* at 830–31.

395. *Id.* at 831.

396. *Id.* at 837.

397. *Id.* at 835.

398. *Id.* at 835–36.

399. *Id.* at 838.

400. *Id.* at 845. In a concurring opinion, Justice Stewart disagreed that it was unconstitutional for Virginia to punish third parties for divulging confidential information regarding the commission, but that the law was unconstitutional because Virginia had attempted to apply the law to a newspaper. *Id.* at 848–49. Justice White argued instead that even though the government may control access to information and punish the criminal acquisition of such information, the "government may not prohibit or punish the publication of that information

In *Cox Broadcasting Corp. v. Cohn*, the Court struck down a Georgia law that permitted a civil cause of action for invasion of privacy based on the publication of the identity of a rape victim.⁴⁰¹ A television reporter had learned the identity of the rape victim when the clerk of the court in the courtroom during the trial of the six defendants accused of the crime acquiesced to the reporter's request to see the indictments.⁴⁰² The reporter testified that neither the clerk nor anyone else made any attempt to conceal the name of the victim as revealed in the indictments.⁴⁰³ The press defendants urged the Court to reach a broad holding that the press could not be held criminally or civilly liable for publishing truthful information,⁴⁰⁴ but, as it did in *Landmark*, the Court rejected the invitation. Instead, the Court consciously chose to take a narrower approach and focus solely on the facts of the case.⁴⁰⁵ The Court concluded that "[o]nce true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it," and we must rely "upon the judgment of those who decide what to publish or broadcast."⁴⁰⁶

In *Smith v. Daily Mail Publishing Co.*, the Supreme Court struck down a West Virginia statute that made it a crime for any newspaper to publish the name of a juvenile offender without court permission.⁴⁰⁷ In this case, the defendant newspapers learned the name of a student who had allegedly shot and killed his classmate through interviews with the police, a prosecutor, and several witnesses.⁴⁰⁸ The State argued that protecting the identity of a juvenile offender helps serve its interests in promoting the rehabilitation of the juvenile, who might otherwise lose employment opportunities and be encouraged to engage in additional antisocial conduct.⁴⁰⁹ The Court once again reiterated that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."⁴¹⁰ The Court emphasized that the First Amendment protects the press when it relies "upon routine newspaper reporting techniques" because "[a] free press cannot be made to rely solely upon the sufferance of government to supply it with information."⁴¹¹ In addition, the Court attacked the statute for restricting only "newspapers" but not electronic media or other forms of publication, leaving many press outlets to publish with impunity.⁴¹² The Court noted that West Virginia was one of the only states to penalize the press for publishing the names of juvenile offenders.

once it falls into the hands of the press, unless the need for secrecy is manifestly overwhelming," as might exist in cases involving national defense information. *Id.* at 849. Justice Stewart's concurrence underscores that the Court did not rest its decision solely on the ground that Virginia was attempting to restrict the press.

401. 420 U.S. 469 (1975).

402. *Id.* at 472 & n.3.

403. *Id.* at 472 n.3.

404. *Id.* at 489.

405. *Id.* at 491.

406. *Id.* at 496 (citing *Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 258 (1974)).

407. 443 U.S. 97 (1979).

408. *Id.* at 99.

409. *Id.* at 104.

410. *Id.* at 103.

411. *Id.* at 103-04.

412. *Id.* at 104-05.

Florida Star v. B.J.F. struck down a judgment against the media for publishing the name of a rape victim, inadvertently disclosed by the police themselves, in violation of state law.⁴¹³ In this case, a sheriff's department had placed in its pressroom a copy of a police report detailing B.J.F.'s allegations that she had been robbed and sexually assaulted. This pressroom was open to the public; a *Florida Star* reporter-trainee viewed the report and copied down the information it contained verbatim, including the victim's name,⁴¹⁴ even though signs posted in the press room stated that names of rape victims were not to be published. The *Florida Star* later prepared a small article for its newspaper concerning the alleged crime. B.J.F. brought a civil lawsuit against the *Florida Star* based on a state law that made it unlawful to "print, publish, or broadcast . . . in any instrument of mass communication" the name of the victim of a sexual offense.⁴¹⁵ B.J.F. claimed that the publication of her name caused her to suffer emotional stress because, not only did her co-workers and acquaintances learn of the crime, but she had received threats from a man claiming that he would rape her again.⁴¹⁶

The Court once again refused to make a sweeping holding that the First Amendment prohibits any civil or criminal sanctions for the publishing of truthful information, this time noting explicitly that it was "mindful that the future may bring scenarios which prudence counsels our not resolving anticipatorily"⁴¹⁷ and citing, among other cases, *Near v. Minnesota*, which suggested that "publication of the sailing dates of transports or the number and location of troops" could be constitutionally subject to a prior restraint.⁴¹⁸ That said, the Court concluded that in *Florida Star*, the government had the ability to engage in other measures to protect privacy interests of victims of sex crimes; the Court noted the government "may classify certain information, establish and enforce procedures ensuring its redacted release, and extend a damages remedy against the government or its officials where the government's mishandling of sensitive information leads to its dissemination."⁴¹⁹ Furthermore, the Court was concerned that punishing the press for the publication of truthful information would lead to "timidity and self-censorship."⁴²⁰ To permit sanctions against *Florida Star* "would force upon the media the onerous obligation of sifting through government press releases, reports, and pronouncements to prune out material arguably unlawful for publication," even when the media simply wants to reproduce the government's own documents verbatim.⁴²¹

In *Florida Star*, the Court made clear that the decision in that case, as well as the other cases in the *Daily Mail* line, has application only in circumstances where the

413. 491 U.S. 524 (1989).

414. *Id.* at 527.

415. *Id.* at 526 (alteration in original) (quoting FLA. STAT. § 794.03 (1987)).

416. *Id.* at 528.

417. *Id.* at 532; *see also id.* at 533 ("We continue to believe that the sensitivity and significance of the interests presented in clashes between First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case.").

418. 283 U.S. 697, 716 (1931).

419. *Florida Star*, 491 U.S. at 534.

420. *Id.* at 535–36.

421. *Id.* at 536.

press has “lawfully obtained” the sensitive information.⁴²² The Court stated: “The *Daily Mail* principle does not settle the issue whether, in cases where information has been acquired *unlawfully* by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well. . . . We have no occasion to address it here.”⁴²³ In addition, the Court somewhat cryptically stated that “[e]ven assuming the Constitution permitted a State to proscribe *receipt* of information, Florida has not taken this step.”⁴²⁴

Another significant aspect of the *Florida Star* opinion was the Court’s conclusion that the confidentiality provision was “facial[ly] underinclusive[]” because it restricted the publication of a victim’s identity only in an “instrument of mass communication,” but seemingly would not apply to those who spread the identities of sex-crime victims in other ways, such as through “backyard gossip” to fifty neighbors. As the Court explained, “[a]n individual who maliciously spreads word of the identity of a rape victim is thus not covered, despite the fact that the communication of such information to persons who live near, or work with, the victim may have consequences as devastating as the exposure of her name to large numbers of strangers.”⁴²⁵

The most recent Supreme Court case addressing the constitutionality of laws prohibiting the publication of truthful information is *Bartnicki v. Vopper*.⁴²⁶ The question that *Bartnicki* resolved was a “narrower version” of the question left open in the *Daily Mail* line of cases:⁴²⁷ “Where the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully, may the government punish the ensuing publication of that information based on the defect in a chain?”⁴²⁸ In a six-Justice majority opinion, Justice Stevens said that the answer was no; however, a concurring opinion by Justice Breyer and joined by Justice O’Connor, two of the Justices in the majority, potentially places some limitations on Justice Stevens’ otherwise broad holding.

The facts of *Bartnicki* were as follows. A teachers’ union was engaged in collective bargaining with a school board, and the wiretap at issue concerned a telephone conversation between Gloria Bartnicki, who was serving as the union’s chief negotiator, and Anthony Kane, the union’s president. During their conversation, Bartnicki and Kane discussed various issues relating to the negotiations, including a proposed strike, the effects of public comment on negotiations, and how they could get the school board to respond to their demands. At one point, Kane said: “‘If they’re not gonna move for three percent, we’re gonna have to go to their, their homes To blow off their front porches, we’ll have to do some work on some of those guys.

422. *Id.* at 534, 541.

423. *Id.* at 535 n.8 (emphasis in original); *see also id.* at 541 (“We do not hold that truthful publication is automatically constitutionally protected We hold only that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order”).

424. *Id.* at 536 (emphasis in original).

425. *Id.* at 540.

426. 532 U.S. 514 (2001).

427. *See, e.g., Florida Star*, 491 U.S. at 535 n.8; *Landmark Commc’ns, Inc. v. Virginia*, 435 U.S. 829, 837 (1978).

428. *Bartnicki*, 532 U.S. at 528 (quoting *Boehner v. McDermott*, 191 F.3d 463, 484–85 (D.C. Cir. 1999) (Sentelle, J., dissenting)).

Really, uh, really and truthfully because this is, you know, this is bad news.”⁴²⁹ Defendant Jack Yocum, who was the head of a local organization opposed to the demands of the teacher’s union, found a tape with this conversation in his mailbox. He played the tape for some members of the school board and gave it to defendant Frederick Vopper (aka Fred Williams), a radio commentator, who played the tape on his talk show during a discussion concerning the ultimate settlement of the conflict between the school board and the teacher’s union.⁴³⁰ Bartnicki and Kane sued Yocum and Vopper under federal and state wiretapping laws, which prohibit the disclosure of any communications that the defendant knows or should know was obtained through an illegal wiretap.⁴³¹ Because the defendants had plainly violated the federal and state statutes barring the disclosure of illegally intercepted communications, the only issue for the Court was whether applying the statutes to the circumstances of this case violated the First Amendment.⁴³² At the outset, the Court expressly noted that it made no distinction between the media defendants and Yokum.⁴³³ Justice Stevens also accepted for sake of argument the plaintiffs’ contentions that the defendants knew or should have known that the interception was unlawful.⁴³⁴

The majority held that the Government proffered justifications for punishing the dissemination of illegally wiretapped information by third parties—to remove an incentive for wiretapping and to minimize the harm suffered by wiretapping victims—were constitutionally insufficient. The majority was barely tolerant of the Government’s first argument that the dissemination ban was necessary to “dry up the market” for illegally intercepted information. Justice Stevens said that the “normal method” of deterring illegal behavior would be to stiffen the penalty for engaging in such behavior, and that “[i]t would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party.”⁴³⁵ He noted that although the Court had permitted the suppression of a person’s speech to deter criminal conduct on “rare occasions,” in such cases the speech at issue was of *de minimis* value, such as child pornography.⁴³⁶ In a footnote, Justice Stevens rejected the dissenters’ analogy to laws that prohibit the receipt of stolen mail or property as inapposite on the ground that such laws did not involve speech and therefore were “not relevant to a First Amendment analysis.”⁴³⁷ Justice Stevens noted that there was no empirical evidence demonstrating that the

429. *Id.* at 518–19 (omission in original).

430. *Id.* at 519.

431. Federal law provides that any person who “intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; . . . shall be punished . . .” 18 U.S.C. § 2511(1) (2000).

432. *Bartnicki*, 532 U.S. at 525.

433. *Id.* at 525 n.8.

434. *Id.* at 525.

435. *Id.* at 529–30.

436. *Id.* at 530 & n.13. Stevens cited *Osborne v. Ohio*, 495 U.S. 103 (1990), and *New York v. Ferber*, 458 U.S. 747 (1982), which held that the First Amendment did not bar convictions for possession or distribution of child pornography. *Bartnicki*, 532 U.S. at 530 n.13.

437. *Bartnicki*, 532 U.S. at 530 n.13.

prohibition against third-party disclosures deterred the illegal interceptions. In almost all reported cases, the intercepting party was known and could be punished directly.⁴³⁸

The Court was slightly more sympathetic to the government's second argument that the dissemination ban was important to reduce the harm that wiretap victims suffer.⁴³⁹ Justice Stevens recognized that the right to privacy was an "important" interest, the ban on dissemination was a "valid" approach to protecting that right, and "the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself."⁴⁴⁰ Justice Stevens was willing to allow that in cases involving "disclosures of trade secrets or domestic gossip or other information of purely private concern,"⁴⁴¹ the anti-dissemination law might very well withstand constitutional scrutiny; however, "privacy concerns give way when balanced against the interest in publishing matters of public importance."⁴⁴²

Just as the Court had done before, the *Bartnicki* Court consciously limited its holding to the facts of the case before it, reiterating that it was "'mindful that the future may bring scenarios which prudence counsels our not resolving anticipatorily.'"⁴⁴³ In addition, the Court did not address whether it would be constitutional for a government to punish the knowing receipt of information that had been illegally obtained. There is currently no state or federal law under which Yokum or Vopper could have been charged for the mere receipt of illegally acquired information.⁴⁴⁴ In addition, according to the case record, the defendants passively received a tape of the intercepted conversation; there was no evidence that they solicited the tape in any way. In a footnote, the Court suggested that the First Amendment would not bar the punishment of any party who obtains the information unlawfully, such as through theft or illegal wiretapping.⁴⁴⁵

Justice Breyer's concurring opinion, joined by Justice O'Connor, limits the *Bartnicki* holding in important ways. Because Justices Breyer and O'Connor were two of the six Justices who joined Justice Stevens's majority opinion, this concurring opinion must be read together with the majority opinion to clarify the holding of the Court. Justice Breyer emphasized that in this case, the defendants had "acted lawfully

438. *Id.* at 530–31.

439. *Id.* at 532 (stating that the Government's second argument was "considerably stronger").

440. *Id.* at 533.

441. *Id.*

442. *Id.* at 534.

443. *Id.* at 529 (quoting *Florida Star v. B.J.F.*, 491 U.S. 524, 532 (1989)).

444. One commentator questioned why the failure of Congress to criminalize the receipt of illicit information had any bearing on the constitutionality of a law criminalizing the publication of that information:

[I]t is hard to see why this case should be decided differently if Congress had made the "receipt" of illegally intercepted information itself unlawful. Congress has made unlawful both the "interception" of certain electronic communications and the "disclosure" of that intercepted information. Why should the constitutionality of these provisions depend on whether an interim step between the unlawful interception and the unlawful disclosure is also explicitly made unlawful?

Paul Gewirtz, *Privacy and Speech*, 2001 SUP. CT. REV. 139, 160 n.73 (2001).

445. *Bartnicki*, 532 U.S. at 532 n.19.

(up to the time of final public disclosure),” and the information disclosed “involved a matter of unusual public concern, namely, a threat of potential physical harm to others.”⁴⁴⁶ Justice Breyer noted that “[n]o one claims that they ordered, counseled, encouraged, or otherwise aided or abetted the interception, the later delivery of the tape by the interceptor to an intermediary, or the tape’s still later delivery by the intermediary to the media,” and there is no law forbidding the mere receipt of illegally wiretapped communications.⁴⁴⁷ In addition, Justice Breyer believed that the plaintiffs in this case “had little or no *legitimate* interest in maintaining the privacy of the particular conversation,”⁴⁴⁸ while the public had a particularly high level of interest in this conversation because it concerned a threat of violence.⁴⁴⁹ He concluded his concurrence by noting that the Court should refrain from setting strict constitutional rules in this area and that the Court’s holding should be limited to the facts of the case.⁴⁵⁰

The three dissenting Justices argued that the Court should have applied intermediate scrutiny to uphold the statute. Chief Justice Rehnquist, joined by Justices Scalia and Thomas, distinguished the *Daily Mail* line of cases on the grounds that such cases were content-based;⁴⁵¹ the information at issue in those cases, aside from *Daily Mail* itself, had been obtained from the government,⁴⁵² which can be presumed to have concluded that disclosure served the public interest;⁴⁵³ the information was already “publicly available” such that restrictions on its dissemination would not serve to protect confidentiality; and there was a legitimate concern of self-censorship that is absent when the statute requires a “knowing” disclosure of confidential information.⁴⁵⁴

The dissenters appear to have recognized that the *Daily Mail* case itself serves as the biggest obstacle to upholding the conviction in *Bartnicki*. In *Daily Mail*, the defendants received the information not through the government but through consensual interviews with third parties. At one point Justice Rehnquist says that the *Bartnicki* defendants cannot be compared to the *Daily Mail* reporters because the *Daily Mail* reporters “lawfully obtained their information through consensual interviews or public documents,”⁴⁵⁵ while the transmission of information from the unknown wiretapper to the defendants was illegal.⁴⁵⁶ This distinction does not hold water because the defendants in *Daily Mail* and *Bartnicki* are equally innocent, regardless of whether their sources violated any civil or criminal laws against the transmission of information. And in *Landmark Communications*, the source of the information concerning the judicial misconduct proceedings violated the confidentiality rules

446. *Id.* at 535–36 (Breyer, J., concurring).

447. *Id.* at 538.

448. *Id.* at 539 (emphasis in original).

449. *Id.* at 539–40.

450. *Id.* at 541.

451. *Id.* at 545 (Rehnquist, C.J., dissenting).

452. *Id.* at 546 & n.3. *Daily Mail* involved a law that contained a blanket prohibition on information, no matter how obtained. *Id.* at 546 n.3.

453. *Id.* at 546.

454. *Id.* at 546–47.

455. *Id.* at 548.

456. *Id.*

governing such proceedings, and in *Florida Star*, the government itself violated the law.⁴⁵⁷

That said, the Court has been unclear on where it draws the line between “lawful” and “unlawful” acquisition of information.⁴⁵⁸ It cannot be enough that merely interviewing government employees is enough to constitute “solicitation.” After all, the reporters involved in the *Daily Mail* case learned the identity of the juvenile offender not through a government document but through interviews with witnesses. Nevertheless, the Court leaves open the possibility that the First Amendment would offer no protection to someone who aided and abetted or otherwise more actively encouraged another to divulge information.⁴⁵⁹

In some ways, the *Daily Mail* line of cases supports the argument that holding the press—or anyone else—liable for the disclosure of classified national security information would be unconstitutional. First, throughout these cases, the Court emphasizes that the government itself bears the burden of controlling the dissemination of sensitive information, and when it fails to guard that information, the public cannot be punished for repeating it. Thus, in *Cox*, the clerk of the court should not have given the press a copy of an unredacted indictment containing the name of the rape victim; in *Florida Star*, the sheriff’s pressroom should not have made available a copy of the unredacted police report containing the name of the rape victim; and in *Landmark Communications*, the source of information concerning confidential judicial misconduct proceedings should not have leaked details of those proceedings to the press. Under this aspect of these cases, it would be inappropriate to punish the press for publishing the contents of these leaks, especially since the government has unquestioned authority to punish the leakers themselves.

Second, in several opinions, the Court expresses concern that holding the press liable for republishing information it had lawfully acquired would cause the press to censor itself out of fears of being held liable. The Court does not expect the press to sift through material—especially information it obtains from the government—to determine whether it is permissible to publish that information. This expectation is true even if the law is very specific about what information cannot be published or whether the press knows that its source illegally obtained the information. All of the cases

457. Professor Paul Gewirtz has argued that the difference between the *Daily Mail* cases and *Bartnicki* is that in the *Daily Mail* cases, the information at issue was “not unlawfully obtained by the media or by anyone else,” as the wiretapped conversation in *Bartnicki* was. In cases such as *Bartnicki*, interests in preserving confidentiality and deterring illegal conduct warrant speech restrictions. Gewirtz, *supra* note 444, at 145–46. But in at least some of the prior cases, the source of the disputed information violated confidentiality rules (if not laws), and prohibiting third parties from publishing such material would reduce the damage such a breach can cause just as much as the federal wiretapping law barring disclosure of illegally intercepted communications.

458. William E. Lee, *The Unusual Suspects: Journalists as Thieves*, 8 WM. & MARY BILL RTS. J. 53, 56–57 (1999).

459. In *Boehner v. McDermott*, a minority of judges concluded that Representative McDermott crossed the magic line by disseminating a tape he had received from some constituents with the express knowledge that the tape had been illegally obtained. 484 F.3d 573, 577 n.1 (D.C. Cir. 2007). As Judge Sentelle persuasively explains in his dissenting opinion, however, “[t]here is no distinction of legal, let alone constitutional, significance between our facts and those before the Court in *Bartnicki*.” *Id.* at 584 (Sentelle, J., dissenting).

except *Bartnicki* involved statutes that barred the publication of very specific information, whether the name of a rape victim (*Cox, Florida Star*) or juvenile defendants (*Daily Mail*) or the proceedings of a judicial misconduct commission (*Landmark*). *Bartnicki* assumed that the defendants in that case either knew or should have known that the contents of the tape were illegally intercepted, and in *Landmark*, the newspaper probably knew that its source was not supposed to be leaking information concerning the proceedings of the judicial misconduct commission. Accordingly, it is not enough that the defendant knew or should have known that the third-party source of information obtained the information illegally or violated civil or criminal laws when it provided the defendant with that information.

Third, the Court has not permitted special liability rules to apply to the press alone. In *Florida Star*, the Court held that a statute holding only those using “instruments of mass communication” liable for the disclosure of a rape victim’s identity was unconstitutional because it was underinclusive. In *Bartnicki*, the Court explicitly stated that it would treat the media and non-media defendants exactly the same. The harm caused by a non-press defendant can be just as great, if not greater, than the harm caused by a traditional media entity, particularly in the age of blogs and the Internet.

Fourth, the *Daily Mail* line of cases emphasizes that the press cannot be held liable for disseminating information that is of public concern. The recent debate involving the publication of confidential information concerning black sites and wiretapping are certainly matters of public concern, especially since they involve potentially illegal activity. It may follow that the government could restrict the dissemination of national security information that does little to advance public debate but causes a lot of harm, but the other cases in the *Daily Mail* series undermine this argument. For example, it is by no means clear how the identity of a rape victim advances the public debate. The harm to the rape victim is tremendous—in *Florida Star*, the victim was receiving threats that she would be raped again—and the public interest in knowing her identity, at least under the circumstances of that case, were minimal. In contrast, government information at the very least can be termed “political” information, which lies at the heart of the First Amendment.

The *Daily Mail* line of cases does not definitively answer the question of whether it would be constitutional to prosecute the press for the publication of classified information. The biggest open issue is what it means to acquire information “unlawfully.” Based on the Court’s precedent, merely asking a potential source questions must not be enough to cross the line into “unlawfully acquired,” while engaging in affirmatively illegal actions, such as stealing or wiretapping, does.⁴⁶⁰ Justice Breyer’s concurring opinion in *Bartnicki* also leaves open the possibility that legislatures could pass laws punishing the knowing receipt of illegally acquired information.⁴⁶¹ These cases do suggest, however, that a high level of protection for the publication of national security information is in order, especially given the tools the

460. See Rodney Smolla, *Information as Contraband: The First Amendment and Liability for Trafficking in Speech*, 96 NW. U. L. REV. 1099, 1128–29 (2002). In the AIPAC case, the defendants are accused of encouraging their source to reveal information by taking him to baseball games and nice dinners, which are not typically considered illegal acts. See *United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006).

461. See *Bartnicki*, 532 U.S. at 538 (Breyer, J., concurring).

government has at its disposal to prevent disclosure of such information in the first place.

F. Constitutional Analysis in United States v. Morison and United States v. Rosen

Most Espionage Act prosecutions have involved classic spy situations. Only one case, *United States v. Morison*, involved the prosecution of a government employee for disclosing classified national security information to the press.⁴⁶² *United States v. Rosen*, the recent AIPAC case, is the first case to apply the Espionage Act to individuals who are not in a position of trust with the government.⁴⁶³

1. *United States v. Morison*

United States v. Morison, was the first case in which a government employee was indicted under the Espionage Act and related statutes for disclosing classified national security information to the press, rather than to a foreign power or its agents. The defendant argued that the prosecution violated the First Amendment. The Fourth Circuit rejected this argument, holding that “we do not perceive any First Amendment rights to be implicated here.”⁴⁶⁴ The court first noted that the prosecution did not involve a prior restraint and therefore did not fall within the scope of the *Pentagon Papers* case.⁴⁶⁵ In addition, the court held that under Supreme Court precedent such as *Branzburg*, it was plain that the press was not immune from generally applicable criminal laws, and in any event, this case implicated “the right of an informer, who had clearly violated a valid criminal law, and not a newsman in issue.”⁴⁶⁶ Under *Marchetti* and *Snepp*, the court explained, a government employee has no First Amendment right to transmit information to anyone “not entitled to receive it,” even if the recipient is the press.⁴⁶⁷

The court upheld Morison’s conviction under § 641 for similar reasons, explaining that

The mere fact that one has stolen a document in order that he may deliver it to the press, whether for money or for other personal gain, will not immunize him from responsibility for his criminal act. To use the first amendment for such a purpose would be to convert the first amendment into a warrant for thievery.⁴⁶⁸

The court also noted that in the circumstances of *Morison*, the defendant “was not fired by zeal for public debate into his acts of larceny of government property”; instead, he was acting out of self-interest as he attempted to “ingratiate” himself with a potential employer.⁴⁶⁹

462. 844 F.2d 1057 (4th Cir. 1988).

463. 445 F. Supp. 2d 602 (E.D. Va. 2006).

464. *Morison*, 844 F.2d at 1068.

465. *Id.*

466. *Id.* at 1068–69 & n.18 (emphasis omitted).

467. *Id.* at 1069–70.

468. *Id.* at 1077.

469. *Id.*

In a concurring opinion, Judge Wilkinson emphasized the seriousness of the First Amendment rights implicated in the case. He expressed concern that prosecuting press sources “threaten[s] the ability of the press to scrutinize and report on government activity,”⁴⁷⁰ especially because the government has a tendency “to withhold reports of disquieting developments and to manage news in a fashion most favorable to itself.”⁴⁷¹ He noted that the First Amendment’s interest in informed public debate “does not simply vanish at the invocation of the words ‘national security.’”⁴⁷² He explained that issues of peace and war are fundamental issues for any government, affect every member of a society, and frequently play a key role in elections.⁴⁷³ At the same time, Judge Wilkinson recognized the importance of secrecy for sensitive government operations.⁴⁷⁴ In the end, he concluded that when balancing the need for an informed democracy against the need for some national security secrets, the courts must defer to the executive and legislative branches’ power and expertise in the conduct of foreign affairs.⁴⁷⁵

In rejecting the defendant’s overbreadth argument, Judge Wilkinson contended that the hypothetical applications of the statute to reports of “corruption, scandal, and incompetence” were not real enough to invalidate it.⁴⁷⁶ In addition, he suggested that in such circumstances it would be difficult to find a jury that would render a conviction, and “the political firestorm that would follow prosecution of one who exposed an administration’s own ineptitude would make such prosecutions a rare and unrealistic prospect.”⁴⁷⁷ Ultimately, Judge Wilkinson concluded that despite the constitutional issues the case raised, “it is important to emphasize what is *not* before us today. This prosecution was not an attempt to apply the espionage statute to the press for either the receipt or publication of classified materials. Neither does this case involve any prior restraint on publication.”⁴⁷⁸

2. *United States v. Rosen*

In the AIPAC case, the district court explicitly rejected the defendants’ argument that with respect to leaked national security information, the government has the power to punish only those in a position of trust with the government—typically government employees, military personnel, or contractors—but not those who receive the information from these individuals. The court notes that the authority addressing this issue “is sparse,” but concludes that “both common sense and the relevant precedent point persuasively to the conclusion that the government can punish those outside of the government for the unauthorized receipt and deliberate retransmission of information relating to the national defense.”⁴⁷⁹

470. *Id.* at 1081 (Wilkinson, J., concurring).

471. *Id.*

472. *Id.*

473. *Id.*

474. *Id.*

475. *Id.* at 1082–83.

476. *Id.* at 1084.

477. *Id.*

478. *Id.* at 1085 (emphasis in original).

479. *United States v. Rosen*, 445 F. Supp. 2d 602, 637 (E.D. Va. 2006).

Although Judge Ellis engages in a lengthy dissection of the *Pentagon Papers* case—concluding that the various opinions of the Court indicate that a majority of Justices would support a criminal prosecution under § 793(e)⁴⁸⁰—he never considers the relevance or applicability of the Court’s *Daily Mail* line of cases. Although the defendants argued in their brief in support of their motion to dismiss the indictment that under *Bartnicki* this case could not constitutionally stand, the district court never mentions *Bartnicki* in its lengthy opinion.

Given that the prosecution in the AIPAC case implicated core values of the First Amendment, Judge Ellis applied strict scrutiny. He concluded that the government had a “compelling interest” in protecting the security of the country,⁴⁸¹ and that § 793 was “narrowly drawn” because it applies only to information that is potentially harmful to the national security and that the defendants know is potentially harmful.⁴⁸² One clear misstep Judge Ellis made in his application of the strict scrutiny standard is that he required the government to show merely that information is “potentially” harmful. Although this might be the appropriate standard in cases involving the disclosure of government information by government actors, who are obligated contractually and otherwise to maintain government secrets, it is not an appropriate standard to apply to third parties. The government does not have a compelling interest in silencing information that possesses only potential to harm the national security interests of the United States. Accordingly, the government should be required to prove at a minimum that any such threatened harm is serious, direct, and imminent.

V. STRIKING THE BALANCE: REQUIRE INTENT AND ELIMINATE INCHOATE LIABILITY

In light of the complicated relationship between the press and the executive branch and the consummate control the executive branch exercises over national security information, courts should require the government to prove not only that the publication of the information at issue caused immediate, serious, and direct harm to the national defense, but also that the offender intended to harm the United States or to aid a foreign country, or acted with reckless indifference to the same. This requirement would help the First Amendment strike a proper balance between the public’s right to know and the executive branch’s need for secrecy in certain circumstances.

A. Requiring Intent to any Prosecution for the Disclosure of National Security Information

As other commentators have noted, any prosecution for the publication of national security information must demonstrate that the disclosure posed an immediate, serious, and direct threat to national security.⁴⁸³ In addition, the government should be required

480. *Id.* at 637–39.

481. *Id.* at 633–34.

482. *Id.* at 634–41.

483. *E.g.*, Blasi, *supra* note 14, at 521 (arguing that criminal prosecutions should be possible only if there is proof that the disclosure “in fact caused serious harm to the government’s ability to implement a legitimate and authorized policy”); Melville B. Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 STAN. L. REV. 311, 331–32 (1974) (arguing that no criminal prosecution could stand unless “‘serious injury’ to the state can be proven to be both likely and imminent as a result of [the] public disclosure”).

to demonstrate that the offender acted with the intent to harm the United States or advantage a foreign power, or with reckless indifference to the harm his disclosure would cause.

This proposed intent requirement is similar to the “bad faith” intent requirement the Court required in *Gorin* to avoid a vagueness problem with a prohibition against the disclosure of “information relating to national security.” This Article argues, however, that the intent requirement should apply in all cases involving the disclosure of national security material, including documents, maps, photographs, and the like. In addition, the standard proposed here would permit liability based on “reckless indifference” to the harm to the United States caused by the disclosure. This slightly broader intent requirement would allow the government to prosecute publications that may not have specifically formed an intent to harm the United States when the information published poses a clearly imminent and grave threat to the United States’ national security interests.

The appeal of an intent requirement in any prosecution concerning the publication of national security information by non-government actors is that it permits the restriction of speech in some cases without unduly chilling legitimate speech. It would protect those who disseminate information based on a good-faith desire to foster public debate. In this way, adding an intent requirement would have somewhat of the same effect as Geoffrey Stone’s suggestion that the government be required to demonstrate that the publication “would not meaningfully contribute to public debate.”⁴⁸⁴ For example, a publisher would not have to correctly guess whether a government practice it reports is illegal to obtain the protection of this test; it would be sufficient that the publisher has a good-faith belief that public scrutiny of the government action would be beneficial.

In addition, this intent requirement would help encourage open and honest conversations between the government and those seeking to disclose classified information. As discussed in Part II, the press has routinely demonstrated a willingness to discuss its publication decisions with the Executive branch, and these efforts should be applauded and encouraged. In return, the burden falls on the government to explain to the press why it is necessary for the information to remain secret. When the government provides nothing more than vague and generalized reasons to justify continued secrecy, it cannot reasonably expect the press to withhold publication. In such cases, the press has every reason to suspect that publishing the information in question would not in fact harm national security and would instead serve the public interest. On the other hand, if the government has instead provided a defendant with a specific and concrete explanation of how the disclosure of classified information could cause imminent and grave danger to our nation’s national security, the government would be permitted to introduce this fact into evidence to demonstrate the defendant’s reckless indifference to harming the United States or aiding a foreign power.⁴⁸⁵ Of course such evidence would not be conclusive; a defendant could argue that he published the national security information despite the government’s warnings because

484. Stone, *supra* note 347, at 204.

485. In some cases, defendants may not have even attempted to consult with government officials about the potential harm that the disclosure of national security information could cause. Such a failure would also be probative, although not conclusive, evidence of the requisite intent.

he believed the value to the public debate outweighed any harm government officials had forecasted. The debates surrounding the Intelligence Identity Protection Act reveal the issues surrounding an intent requirement. Ultimately, Congress required the government to prove that the offender had “reason to believe” that “the pattern of activities in which he engaged would impair or impede the foreign intelligence service activities of the United States,”⁴⁸⁶ but a better approach would be to require actual subjective intent or recklessness to injure the national defense of the United States or to give advantage to a foreign nation.

Requiring the government to prove intent (or recklessness) is preferable to trying to define certain categories of information that the government should be automatically entitled to keep secret. As Congress understood when passing the Intelligence Identities Protection Act, there are times when it is entirely legitimate for the media, academics, or other speakers to reveal otherwise top-secret and sensitive information (in that case, the names of CIA operatives).⁴⁸⁷ In the same vein, although the Supreme Court in *Near v. Minnesota* suggested in dicta that there were other categories of military information that fall outside the sphere of First Amendment protection, such as the publication of “the sailing dates of transports or the number and location of troops,”⁴⁸⁸ it is by no means clear that this is—or should be—the case, absent an additional showing that the publication of such information causes harm. During the Iraq war, newspapers and television shows have been full of stories concerning the movements of troops and ships, and virtually none of them have undermined our national security interests. The same can be said for cryptographic information and atomic energy information, both of which are subjects of specific statutory provisions. The government lacks a compelling interest to maintain the secrecy of these broad categories of information absent an additional showing of harm and causation in a particular case. That said, when the government can demonstrate harm as well as intent to harm or reckless indifference to the harm, the intent standard this Article proposes would still permit prosecutions in the very worst and obvious cases.

Finally, an intent requirement would also help alleviate concerns about defining who and what constitutes the press. Although the First Amendment protects the rights “of speech, and of the press,” the Court has never given the Press Clause any real meaning,⁴⁸⁹ and the creation of the Internet has brought into high profile the difficulties of defining the press in any meaningful way.⁴⁹⁰ Indeed, any approach that limited its protections to members of the press would be problematic. With an intent requirement, only those who intend to harm the United States or help a foreign power—or who recklessly disregard the dangers of disclosure—could be punished for communicating national security information. The government’s ability to prove this element would not turn on the medium of publication. For example, a magazine publishing lists of CIA operatives in the hopes of disrupting intelligence activities—the very kind of publication that provided the impetus for the passage of the Intelligence

486. *See supra* Part III.D.

487. *Id.*

488. 283 U.S. 697, 716 (1931).

489. It is worth noting that in *Bartnicki*, the Court did not distinguish between the individual who disclosed the tape he had received anonymously to radio stations and the radio stations who in turn disclosed the information to their listening public. *Bartnicki v. Vopper*, 532 U.S. 514, 525 n.8 (2001).

490. *See Papandrea, supra* note 216, at 523–32.

Identities Protection Act of 1982—would be subject to prosecution. Although in some cases a publication's tradition for providing relevant information for public debate might make it more difficult for the government to prove the requisite level of intent, an intent requirement would not amount to a *per se* bar to prosecutions against the mainstream media and would not make the viability of a prosecution dependent upon the medium of communication.

Requiring a showing of intent is consistent with the Court's First Amendment jurisprudence.⁴⁹¹ In *Brandenburg v. Ohio*, the Supreme Court set forth the test for incitement: "the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."⁴⁹² In order to constitute "incitement," the speaker must have intended to bring about the imminent lawless action.⁴⁹³ Similarly, "fighting words" is a category of unprotected speech consisting of words "which by their very utterance inflict injury or tend to incite an immediate breach of the peace."⁴⁹⁴ In *Cohen v. California*, the Court appeared to embrace an intent requirement in holding that the speech on defendant's jacket was not fighting words because there was "no showing of an intent to incite disobedience to or disruption of the draft."⁴⁹⁵ And most recently, in *Virginia v. Black*, the Court made clear that the First Amendment permits the banning of cross burnings as long as they are performed with the intent to intimidate.⁴⁹⁶

The Court's clearest discussion on intent to cause harm can be found in *New York Times Co. v. Sullivan*, where it considered whether the First Amendment presented any bar to defamation claims brought by public officials.⁴⁹⁷ At common law, libel was considered below the plane of constitutional concern. Instead, disputes were over whether truth was a defense and whether the jury was limited to deciding the mere fact of publication.

In *Sullivan*, the Court emphasized that absolute liability for the publication of false, defamatory speech was inappropriate given "a profound national commitment to the

491. Some scholars have questioned whether the speaker's intent should be a relevant factor under the First Amendment. See, e.g., Larry Alexander, *Free Speech and Speaker's Intent*, 12 CONST. COMMENT. 21 (1995); Frederick Schauer, *Intentions, Conventions, and the First Amendment: The Case of Cross-Burning*, 55 SUP. CT. REV. 197 (2004).

492. 395 U.S. 444, 447 (1969).

493. Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 B.U.L. REV. 685, 724–25 (1978) (discussing intent requirement of *Brandenburg* test); e.g., *Cohen v. California*, 403 U.S. 15, 18 (1971) (holding that Cohen's jacket stating "Fuck the Draft" could not constitute incitement because "there [was] no showing of an intent to incite disobedience to or disruption of the draft").

494. *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942); see also Kent Greenawalt, *Insults and Epithets: Are They Protected Speech?*, 42 RUTGERS L. REV. 287, 298 (1990) (arguing that fighting words that are not intended to provoke an immediate breach of the peace should be protected speech).

495. *Cohen*, 403 U.S. at 18; see also *id.* at 20 (there was "no showing that anyone who saw Cohen was in fact violently aroused or that [Cohen] intended such a result").

496. 538 U.S. 343, 362–63 (2003). The Court made clear, however, that it is not necessary to demonstrate that the speaker intends to carry out the threat. *Id.* at 359–60.

497. 376 U.S. 254 (1964).

principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials.”⁴⁹⁸ The majority was concerned that permitting strict liability for the publication of false information would have a severe chilling effect on the press, who would be sure to make only statements that “steer far wider of the unlawful zone.”⁴⁹⁹ The Court explained that “erroneous statement is inevitable in free debate, and that it must be protected if the freedoms of expression are to have the ‘breathing space’ that they need . . . to survive.”⁵⁰⁰

After a careful balance of the public’s interest in a free and open debate and the plaintiff’s interest in protecting his reputation, the Court determined that a public figure plaintiff must demonstrate by clear and convincing evidence that the press published false, defamatory statements with “actual malice”—that is, “with knowledge that it was false or with reckless disregard of whether it was false or not.”⁵⁰¹ Actual malice is not demonstrated by showing what a reasonably prudent person (or even journalist) would have published or would have investigated before publishing.⁵⁰² Instead, the plaintiff must show that the defendant “in fact” entertained serious doubts about the veracity of the publication.⁵⁰³ As the Court has noted in subsequent cases, “[t]he phrase ‘actual malice’ is unfortunately confusing in that it has nothing to do with bad motive or ill will.”⁵⁰⁴ Instead, a defendant may have acted with actual malice when the story is fabricated by the defendant, the story is the product of the defendant’s imagination, the story is so inherently improbable that only a reckless person would have put them in circulation, or there are obvious reasons to doubt the veracity of the information or the accuracy of the source or sources.⁵⁰⁵

New York Times Co. v. Sullivan and its treatment of defamation claims by public officials does not offer a perfect analogy for cases involving the restriction on national security information. After all, the disclosure of national security information is dangerous precisely because it is *truthful*. But if a high level of intent—“actual malice”—is required before false defamatory speech can be restricted, surely the disclosure of truthful national security information warrants at least as much protection.

Critics might respond that the leak of information to the press can be equally damaging to the national security interests as the transfer of information to the traditional spy, and that the motivation for the leak, such as informing a democracy in the case of the press, or giving an advantage to the enemy, is irrelevant when determining the harm that particular sort of information causes.⁵⁰⁶ Rather, the likelihood of harm depends on the slender hope that our enemies do not read American publications.⁵⁰⁷ But much the same thing can be said of libel of public officials,

498. *Id.* at 270.

499. *Id.* at 279 (citing *Speiser v. Randall*, 357 U.S. 513, 526 (1958)).

500. *Id.* at 271–72 (citing *NAACP v. Button*, 371 U.S. 415, 433 (1963)).

501. *Id.* at 279–80.

502. *Harte-Hanks Commc’ns, Inc. v. Connaughton*, 491 U.S. 657, 688 (1989).

503. *St. Amant v. Thompson*, 390 U.S. 727, 731 (1968).

504. *Harte-Hanks*, 491 U.S. at 666 n.7.

505. *St. Amant*, 390 U.S. at 732.

506. *E.g.*, *Edgar & Schmidt*, *supra* note 220, at 934.

507. *Id.* Although this is unlikely in the current day and age, during World War II the *Chicago Tribune* revealed that the U.S. government had broken the Japanese code, but the

incitement, and fighting words. In all of these cases, the harm is done regardless of the intent of the speaker. Here, requiring the government to prove intent to harm or reckless indifference to harm in any case involving the publication of information by a non-government actor will result in slightly more truthful but potentially harmful information from entering the marketplace.

Incorporating an intent requirement is not meant to replace the requirement that the government demonstrate that the publication of the information posed an immediate, serious, and direct threat to national security. Instead, an intent requirement would be an additional element of any prosecution. In addition, any revelation of even arguably illegal or immoral behavior by the United States should be immune from prosecution, regardless of the intent. For example, when 60 Minutes II came into possession of the Abu Ghraib photographs, the government argued that they should be not broadcast because they would likely cause some to retaliate against our soldiers.⁵⁰⁸ Bare assertions that leaks undermine our relationships with foreign countries, without regard to the actual content of the leak, would similarly be insufficient.

B. Drawing the Line Against Inchoate Liability

The only remaining issue is whether the press can be criminally prosecuted for inchoate crimes such as aiding and abetting the disclosure of national security information, conspiring to break laws governing the control of national security information, or knowingly receiving such information. If the Fourth Circuit permits the government's aiding and abetting charges in the AIPAC case to stand, there is nothing stopping the Department of Justice from using similar charges against the press. Although current statutory law authorizes such prosecutions, the First Amendment should stand as an absolute bar.

At first blush, holding the press liable for commanding, inducing, or procuring the leak of classified national security information would be "merely an application of the traditional crime of receiving stolen property."⁵⁰⁹ Aiding and abetting liability is consistent with other theories of criminal law that aim to deter criminal activity by punishing all of those involved in it in any way. As Paul Gewirtz has noted, applying the law of aiding or abetting, or punishing the receipt of stolen property, would be theoretically similar to applying the exclusionary rule in criminal cases. As he explained, "[t]he exclusionary rule in criminal cases rests precisely on the belief that police misconduct can be deterred by barring prosecutors and others from using the unlawfully seized evidence."⁵¹⁰

The most famous case holding the press liable under an aiding-and-abetting claim is *Rice v. Paladin Enterprises, Inc.*, which held a book publisher civilly responsible for aiding and abetting murder.⁵¹¹ Lawrence Horn hired James Perry to kill his ex-wife, his handicapped son, and his son's nurse in order to collect the two million dollars that

Japanese apparently never read the article. LLOYD WENDT, CHICAGO TRIBUNE: THE RISE OF A GREAT AMERICAN NEWSPAPER 627–36 (Rand McNally & Co. 1979).

508. Scott Pelley, *Reporting National Security Under Threat of Indictment*, 2006 Annual Dinner Media Law Resource Center at 22.

509. Stone, *supra* note 347, at 205 n.65.

510. Gewirtz, *supra* note 444, at 148.

511. 128 F.3d 233 (4th Cir. 1997).

his son had received in a settlement for the injuries that rendered him a quadriplegic.⁵¹² Perry carefully followed the instructions on how to commit murder like a professional killer outlined in *Hit Man: A Technical Manual for Independent Contractors*.⁵¹³ Representatives for the three victims filed wrongful death charges against the book's publisher Paladin Enterprises, alleging that Paladin had aided and abetted the three murders through the publication of the book. Paladin stipulated for purposes of summary judgment that (1) Perry had followed the book's instructions; (2) when marketing the book, Paladin had "intended to attract and assist criminals and would-be criminals who desire information and instructions on how to commit crimes," (3) Paladin "intended and had knowledge" that its book "would be used, upon receipt, by criminals and would-be criminals to plan and execute the crime of murder for hire," and (4) the publication of the book actually did assist Perry in his commission of the murders.⁵¹⁴ Paladin rested its defense entirely on the First Amendment. Although the district court had ruled in the publisher's favor, the Fourth Circuit reversed, holding that "long-established caselaw provides that speech—even speech by the press—that constitutes criminal aiding and abetting does not enjoy the protection of the First Amendment"⁵¹⁵

The *Rice* court recognized that the First Amendment required the plaintiffs to meet a higher intent standard than in the ordinary tort case. The court stated:

Even if the First Amendment imposes a heightened intent-based limitation on the state's ability to apply the tort of aiding and abetting to speech . . . we are confident that, at the very least, the aiding and abetting of a *malum in se* crime such as murder with the specific purpose of assisting and encouraging another or others in that crime would satisfy such a limitation.⁵¹⁶

The Supreme Court declined to review the controversial decision in *Rice*, but even assuming the Fourth Circuit's constitutional analysis was correct, the difference between aiding and abetting murder and aiding and abetting the leak of national security information are vastly different in degree and kind. Part of the reason for this dichotomy is that, unlike aiding and abetting murder, the aiding and abetting of a leak is not a *malum in se* crime. The leaks of information by government employees or contractors are not necessarily bad. As discussed earlier in this article, most leaks come from high-ranking officials, and a surprising number of leaks are authorized, frequently unbeknownst to the reporter. Unlike the government's easily recognizable interest in tangible property, the government's property rights to information is dubious. The Freedom of Information Act contains a presumption that all government information belongs to the people, and it must be turned over to the people when requested, unless it falls within one of the listed exemptions.⁵¹⁷

Furthermore, the Court's current jurisprudence has created a peculiar wrinkle whereby a government employee could be punished for disclosing national security information even when a non-government person could not be held liable for

512. *Id.* at 239.

513. *Id.*

514. *Id.* at 241.

515. *Id.* at 242.

516. *Id.* at 252.

517. 5 U.S.C. § 552 (2000).

publishing that same information. Certain federal statutory provisions directly applicable to government employees, and only through inchoate liability applicable to the press, do not require the disclosure of the information to pose a true threat to the nation's security interests. Instead, as discussed in Part IV.B.,⁵¹⁸ the Supreme Court has held that government employees have very limited First Amendment rights to disclose information that they obtained by virtue of their employment. Given this, using inchoate liability laws to prosecute press would permit the government to punish the press for encouraging the leak of information in cases when it could not constitutionally punish the press for publishing that same information.

Extending inchoate liability to reporters and journalists would be particularly harmful because it would permit the government and courts to interfere with the relationship between sources and the press. To prove that a journalist aided and abetted a leak, the government would certainly investigate the journalist's phone records and billing records. In the course of any investigation, the government would inevitably uncover information about many of the journalist's other sources. In this way, the government could substantially chill the free flow of information that is so essential to our democracy.

CONCLUSION

If the government seeks to prosecute the press for publishing classified national security information, it should be required to prove not only that the disclosure caused immediate, serious, and direct harm to the United States, but also that the defendant disclosed the information with the intent to harm the United States, or with reckless indifference to the harm the disclosure would cause. An intent requirement would offer a large measure of protection to those who publish national security information in good faith while permitting the government to punish the dissemination of such information in the most egregious cases. Such a requirement is consistent with the Supreme Court's First Amendment jurisprudence, which demands that a defendant's intent be proven before conviction. The application of this standard may occasionally lead to the publication of information that might threaten national security, but this small risk is necessary to balance the conflicting interest between the need for a deliberative democracy and national security.

518. *See supra* text accompanying note 331.