# PROTECTION OF INFORMATION TO PRESERVE NATIONAL SECURITY: IS WIKILEAKS REALLY THE ISSUE?

*Wendy J. Keefer*[*]

I. INTRODUCTION ..... 457
II. THE STATE SECRETS DOCTRINE AS A FOUNDATION FOR INFORMATION POLICY ..... 459
III. THE FIRST AMENDMENT DISTRACTION ..... 462
IV. THE INTERNET IS HERE TO STAY ..... 465
V. NOT ALL BAD ACTS ARE CRIMINAL ..... 466
VI. WITH ACCESS COMES RESPONSIBILITY ..... 471
VII. CLASSIFICATION AND DECLASSIFICATION ..... 472
VIII. KEEPING THE CAT IN THE BAG: WHERE DO WE GO FROM HERE? ..... 477

## I. INTRODUCTION

The government's response to the activities of Julian Assange and WikiLeaks seems universally to include threats of criminal punishment. Democratic Senator Dianne Feinstein provided the following opinion:

"When WikiLeaks founder Julian Assange released his latest document trove—more than 250,000 secret State Department cables—he intentionally harmed the U.S. government. The

---

[*] I currently practice law with the firm of Keefer & Keefer, LLC in Charleston, South Carolina. In addition to legal practice, I serve as an adjunct professor of law at the Charleston School of Law teaching national security law, separation of powers and legal writing courses. Prior to forming Keefer & Keefer with my husband, and in addition to working at other private law firms in Charleston, I served as senior counsel and chief of staff in the Office of Legal Policy of the U.S. Department of Justice (2001-2003) and worked at the law and public policy firm of Bancroft Associates, PLLC (2005-2006), both in Washington, D.C. From 1997-98, I was law clerk to the Honorable J.L. Edmondson, Circuit Judge, United States Court of Appeals for the Eleventh Circuit. I would like to thank Sean Keefer, Jessica Graham and Renee Anderson for their help and support in writing this article.

release of these documents damages our national interests and puts innocent lives at risk. He should be vigorously prosecuted for espionage."[1] Republican Senator Mitch McConnell described Assange as a "high-tech terrorist."[2] And Attorney General Eric Holder stated unequivocally that the "[n]ational security of the United States has been put at risk" by the publication of thousands of United States documents.[3]

No doubt the release of classified information through the WikiLeaks website causes concern for the government. That said, and despite any negative feelings and beliefs this author and others may have about Assange and his conduct personally, the government leaker is the proper focus of concern and criminal action. The spotlight has, in large part, found Mr. Assange and WikiLeaks but has been somewhat less attracted to Private Bradley Manning and his motive and actions in leaking the classified government information entrusted to him.[4]

The reasons for this misguided attention are several: (1) focus on WikiLeaks permits academic and policy debates to focus on the press protections of the First Amendment rather than the more difficult question of whether the Constitution guarantees citizens access to government information in the first instance;[5] (2) it is more comfortable to focus attention upon an outsider, a non-citizen located abroad, as the enemy, rather than to acknowledge that the real harm came from someone here;[6] and

1. Dianne Feinstein, Op-Ed., *Prosecute Assange Under the Espionage Act*, WALL ST. J. (Dec. 7, 2010), http://online.wsj.com/article/SB10001424052748703989004575653280626335258.html.

2. *McConnell: WikiLeaks Head a High-Tech Terrorist*, CBS NEWS (Dec. 5, 2010), http://www.cbsnews.com/stories/2010/12/05/politics/main7119787.shtml.

3. Sara Sorcher, *Assange Arrested; What Will U.S. Do Now?*, NAT'L J. (Dec. 7, 2010, 8:10 AM), http://nationaljournal.com/nationalsecurity/assange-arrested-what-will-u-s-do-now--20101207. Holder further stated: "The lives of people who work for the American people have been put at risk. The American people themselves have been put at risk by these actions that I believe are arrogant, misguided and ultimately not helpful in any way. We are doing everything that we can." *Id.*

4. *See* Scott Shane, *Accused Soldier in Brig as WikiLeaks Link Is Sought*, N.Y. TIMES (Jan. 13, 2011), http://www.nytimes.com/2011/01/14/world/14manning.html?_r=2.

5. *See infra* Part II.

6. *See infra* Part V.

(3) the Army's prosecution of Private Manning is underway with numerous fairly straightforward charges pending, including "aiding the enemy,"[7] and thus, is somewhat anti-climactic.

This Article uses the interest in WikiLeaks, and to a lesser extent Private Manning, as a platform for briefly summarizing key laws and legal concepts related to classified information. It then discusses some of the public rhetoric about WikiLeaks. The article concludes by identifying some red herrings, which red herrings distract from the real issues surrounding any system of information security, and acknowledges that no such system can wholly guarantee the protection of information or wholly guarantee that only information dangerous to national security is protected. The real questions are how the government might discourage dangerous information leaks and how it should react on those occasions when such leaks do occur.

## II. THE STATE SECRETS DOCTRINE AS A FOUNDATION FOR INFORMATION POLICY

Though the state secrets doctrine relates typically to questions of access to evidence in civil and criminal court actions, a review of that doctrine elaborates on the tension that often exists—highlighted by the WikiLeaks disclosures—between protecting against national security risks and providing access to government information.[8] The state secrets doctrine further recognizes that where disclosure of information may create a likely risk of harm to the country at large, secrecy may trump other constitutional requirements and protections.[9]

The concept of state secrets dates back to the country's formation and its earliest governors.[10] Its modern recognition

7. Charlie Savage, *Soldier Faces 22 New WikiLeaks Charges*, N.Y. TIMES (Mar. 3, 2011), http://www.nytimes.com/2011/03/03/us/03manning.html?_r=1.

8. *See* United States v. Reynolds, 345 U.S. 1, 10 (1953).

9. *See id.* at 9–10.

10. U.S. CONST. art. I, § 5. President Washington withheld information related to negotiation of the Jay Treaty. United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320–21 (1936). In response to congressional requests for information, the Court explained the following:

> [I]nquiry within the international field must often accord to the

stems from the Supreme Court's decision in *United States v. Reynolds*.[11]

In that case, an Air Force plane crash that killed several civilians resulted in their widows' filing wrongful death claims.[12] The litigants sought discovery of witness statements and an official incident report that the Air Force refused to produce by asserting the state secrets privilege.[13] Though the lower courts ordered production of the documents, the Supreme Court reversed those decisions.[14]

Recognizing the state secrets privilege, the Court established a procedure for courts to follow when faced with a government assertion of the privilege.[15] This procedure requires a "formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer."[16] This requirement attempts to ensure that the privilege is "not to be lightly invoked."[17] Once this formal assertion is made, "[t]he court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege

> President a degree of discretion and freedom from statutory restriction which would not be admissible were domestic affairs alone involved. Moreover, he, not Congress, has the better opportunity of knowing the conditions which prevail in foreign countries, and especially is this true in time of war. He has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials. Secrecy in respect of information gathered by them may be highly necessary, and the premature disclosure of it productive of harmful results.

*Id.* at 320.

11. 345 U.S. 1 (1953). In addition to *Reynolds*' recognition of a state secrets privilege, the Court recognized that cases that "would inevitably lead to the disclosure of matters which the law itself regards as confidential" are generally nonjusticiable, a concept that leads to near complete nonjusticiability of certain national security cases. Totten v. United States, 92 U.S. 105, 107 (1876); *see also* Tenet v. Doe, 544 U.S. 1, 11 (2005) (reaffirming the principle of *Totten*).

12. *Reynolds*, 345 U.S. at 3.

13. *Id.* at 3–4.

14. *Id.* at 12; *see* Reynolds v. United States, 192 F.2d 987 (3d Cir. 1951).

15. *Reynolds*, 345 U.S. at 8–11.

16. *Id.* at 7–8.

17. *Id.* at 7.

is designed to protect."[18]

Using this procedure, the issue is whether disclosure of the information presents a reasonable danger of harm to the national security of the United States.[19] In making this determination, however, "[t]oo much judicial inquiry into the claim of privilege would force disclosure of the thing the privilege was meant to protect, while a complete abandonment of judicial control would lead to intolerable abuses."[20]

The Court cautioned lower courts, once satisfied that the privilege is valid, not to "jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers."[21] How much scrutiny the court should afford the privilege claim, including possible judicial review of the information, may depend upon how crucial the information is to the relevant litigation.[22] That said, the recognition of the state secrets privilege further acknowledges the authority of the government, specifically the Executive Branch, to keep such secrets from the public and even from another branch of government.[23] Also, the secrets being kept may not always be the government's own.

State secrets may include information from foreign nations.[24] Often discussion of information that may injure national security focuses on whether that information discloses strategies, weaknesses, and the like, such that the information may be directly used against the United States to harm its troops, citizens, or property.[25] Not to be overlooked is the fact that much of the information gathered or obtained by the government comes from friendly foreign nations or foreign agents.[26] The continued

18. *Id.* at 8.
19. *Id.* at 10.
20. *Id.* at 8.
21. *Id.* at 10.
22. *Id.* at 11.
23. *Id.* at 6.
24. *See* Snepp v. United States, 444 U.S. 507, 512 (1980) (per curiam).
25. *E.g.* Reynolds, 345 U.S. at 10.
26. *See Snepp*, 444 U.S. at 512 (footnote omitted) ("In addition to receiving intelligence from domestically based or controlled sources, the CIA obtains information from the intelligence services of friendly nations and from agents

access to these external sources of information is crucial to the country's international relations and operations:

> Every major nation in the world has an intelligence service. … The CIA (or its predecessor the Office of Strategic Services) is an agency thought by every President since Franklin D. Roosevelt to be essential to the security of the United States and—in a sense—the free world. It is impossible for a government wisely to make critical decisions about foreign policy and national defense without the benefit of dependable foreign intelligence.[27]

In order to obtain this foreign intelligence, secrecy may be necessary. Secrecy does not directly implicate the First Amendment, but where secrecy is not maintained, and publication of the secret information is at issue, the First Amendment is often invoked.[28]

## III. THE FIRST AMENDMENT DISTRACTION

"Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."[29] Despite this restriction upon the government's ability to regulate speech or the press, nothing in this limitation upon government requires that it actually provide the information to be disseminated through speech or the press.[30]

---

operating in foreign countries.").

27. *Id.* at 512 n.7 (*citing* THOMAS POWERS, THE MAN WHO KEPT THE SECRETS: RICHARD HELMS & THE CIA (1979)).

28. *Id.* at 509–10.

29. U.S. CONST. amend. I.

30. *See* Houchins v. KQED, Inc., 438 U.S. 1, 15 (1978) ("Neither the First Amendment nor the Fourteenth Amendment mandates a right of access to government information or sources of information within the government's control."); Branzburg v. Hayes, 408 U.S. 665, 684 (1972) ("[T]he First Amendment does not guarantee the press a constitutional right of special access to information not available to the public generally."). The only area in which courts provide greater access to government information is in connection with the press and the public's right to observe certain proceedings. *See* Press-Enterprise Co. v. Superior Court (*Press-Enterprise II*), 478 U.S. 1, 8–9 (1986); Globe Newspapers Co. v. Superior Court, 457 U.S. 596, 604 (1982). But even in granting access to such things as criminal court proceedings, secrecy may be permissible where the "closure is essential to preserve higher values [such as national security] and is narrowly tailored to serve that interest." *Press-*

Indeed, that some information would be secret and that some balance must be struck regarding what the public can know and what it cannot are obvious from the Constitution itself.

In describing the requirements placed upon Congress, that founding document provides that "[e]ach House shall keep a Journal of its Proceedings, and from time to time publish the same, *excepting such Parts as may in their Judgment require Secrecy* . . . ."[31] The Supreme Court also expressly recognizes the right of the government—specifically the Executive Branch—to maintain secret information.[32] The Court noted: "[The President] has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials. Secrecy in respect of information gathered by them may be highly necessary, and the premature disclosure of it productive of harmful results."[33]

What amount of information should then be kept secret is highly debated but not strictly legally dictated.[34] In a representative government like the United States, access to information should be the rule not the exception. "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power knowledge gives."[35]

---

*Enterprise II*, 478 U.S. at 9 (quoting Press-Enterprise Co. v. Superior Court (*Press-Enterprise I*), 464 U.S. 501, 510 (1984)).

31. U.S. CONST. art. I, § 5 (emphasis added).

32. *See* United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936).

33. *Id.*

34. With rising distrust in the government following the Vietnam War, Congress made efforts to provide greater access for citizens to government information with legislation such as the Freedom of Information Act, 5 U.S.C. § 552 (2006), and the Privacy Act of 1974, 5 U.S.C. § 552a (2006). Even those statutes, however, include exceptions to required disclosures for certain information relating to national security. Freedom of Information Act, 5 U.S.C. § 552 (2006); Privacy Act of 1974, 5 U.S.C. § 552a (2006).

35. Letter from James Madison to W. T. Barry (Aug. 4, 1822) *reprinted in* THE FOUNDERS' CONSTITUTION Vol. 1, Ch. 18, Doc. 35 (Philip B. Kurland & Ralph Lerner eds., 2000).

"If a nation expects to be ignorant and free, in a state of civilization, it expects what [it] never was and never will be."[36] It is the American condition, then, to seek more, not less access to information. Indeed, in his concurring opinion in *New York Times Co. v. United States*,[37] Justice Black highlighted the importance not only of access to information but specifically the importance of the role the press plays, in part through First Amendment protections. In checking the actions of the government, "[t]he Government's power to censor the press was abolished so that the press would remain forever free to censure the Government. The press was protected so that it could bare the secrets of government and inform the people. Only a free and unrestrained press can effectively expose deception in government."[38]

In this ever-changing communication world, however, it is often the government condition to seek to control and withhold more information, not less, from the press and the public. This struggle requires constant reassessment of the balance struck in recent decades between access and secrecy. In that struggle, the First Amendment is not the real battlefield.

The First Amendment protects the publication of information legally obtained by ensuring, in most instances, that its publication may occur.[39] It may not necessarily protect the publisher from punishment for an otherwise criminal publication.[40] However, punishing the organized, traditional press would undoubtedly be politically unpopular. Punishment of any global Internet media, like WikiLeaks, would also be fraught with legal hurdles that—if not overcome by the government—could cause greater harm to the country than the original leak of

36. Letter from Thomas Jefferson to Col. Charles Yancey (Jan. 6, 1816) *reprinted in* 11 THE WORKS OF THOMAS JEFFERSON, 497 (Paul Leicester Ford ed. 1905).

37. 403 U.S. 713 (1971).

38. N.Y. Times Co. v. United States, 403 U.S. 713, 717 (1971) (Black, J., concurring).

39. U.S. CONST. amend. I.

40. *N.Y. Times Co.*, 403 U.S. at 733 (White, J., concurring) ("Prior restraints require an unusually heavy justification under the First Amendment; but failure by the Government to justify prior restraints does not measure its constitutional entitlement to a conviction for criminal publication.").

information.[41] Nonetheless, the publication and receipt of information via the Internet or other electronic means creates new issues for which the government must account in its handling of information.[42]

## IV. THE INTERNET IS HERE TO STAY

Many of the articles and discussions surrounding the WikiLeaks disclosures view the problem arising from a new type of media—a media that does not have a traditional editorial review process and does not seek to cooperate with governmental bodies:

> The great democratization of information on the Internet, notably in the form of WikiLeaks, means there is no responsible party to negotiate with on the other side. For better or worse, we [The New York Times] held back the warrantless wiretapping story, in part because we consulted with, and were persuaded by, things the government was telling us. We may have made the wrong decision, but it wasn't for want of trying to get it right, trying to strike the balance correctly. That doesn't seem to be the case in many quarters on the Internet today. So, we live in a new world.[43]

Similarly, others commenting on the WikiLeaks situation focus on the distinctions between news sources like WikiLeaks (blogs or other Internet postings) and the traditional media:

---

41. In the case of WikiLeaks and its founder, the government first must successfully orchestrate extradition to the United States. Once here, current criminal laws, as summarized in this article, may not provide for easy prosecution. In terms of national security, a failed prosecution is worse than no prosecution. *See* Jack Goldsmith, Op-Ed., *Why the U.S. Shouldn't Try Julian Assange*, WASH. POST (Feb. 10, 2011, 7:14 PM), http://www.washingtonpost.com/opinions/why-the-us-shouldnt-try-julian-assange/2011/02/10/ABpiIrQ_story.html (describing the harm that could result from pursuing any legal recourse unsuccessfully).

42. *Id.*

43. *Some Insights on WikiLeaks and First Amendment Protection*, ABSBLOG (Dec. 1, 2010, 1:27 PM), http://www.acslaw.org/taxonomy/term/651 (quoting Adam Liptak, Moderator, National Security, Government Transparency, and the First Amendment (Nov. 15, 2010) (video *available at* http://www.americanconstitutionsociety.org/node/17666)).

> The Times goes through, as you would, a process of making a determination whether they would publish a particular document with a particular legend on it, for example or revealing how long it takes for a particular weapon to fire. Material like that [is] the sort of thing the Times wouldn't publish, you wouldn't publish.
>
> . . . .
>
> When you get a Wikileaks organization, I don't think they're going through a fa[ç]ade of reading the material through [the] 92,000 documents and making some judgment that, well, maybe we shouldn't release that one.[44]

No doubt exists as to whether WikiLeaks and likely thousands if not millions of other Internet users may not have the same self-imposed editorial principles as the traditional news media.[45] Indeed, many of these computer users purporting to provide news and information may actually intend harm to persons, organizations, or even whole countries. However, not all unsavory actions are—or should be—criminalized. More importantly, such criminalization would be ineffective given the scope of the Internet.

## V. NOT ALL BAD ACTS ARE CRIMINAL

Criminal offenses related to the improper handling, disclosure, and use of classified information[46] provide legal prohibitions for the wrongful gathering of such information,[47] for

44. Interview by Alan Murray with Floyd Abrams, (full interview *available at First Amendment Guru Floyd Abrams on the WikiLeaks Situation*, WALL ST. J. (July 28, 2010), http://blogs.wsj.com/law/2010/07/28/first-amendment-guru-floyd-abrams-on-the-wikileaks-situation).

45. *Id.*

46. This Article focuses on disclosure, possession, and publication of "classified information" as that term is used and defined in Executive Order 13,526. Exec. Order No. 13,526, 3 C.F.R. 298 (2009). Often when discussing secret information the term sensitive information is used. Under the law, reference to sensitive information is scant. *See e.g.*, 18 U.S.C. § 793(e) (2006). Sensitive information is not a category within the Executive Branch's classification scheme.

47. 18 U.S.C. § 793 (2006) (prohibiting the gathering, transmitting or

providing such information to a foreign government or groups within a foreign country,[48] and for the unauthorized disclosure of classified information.[49] These crimes target those who legally access but wrongfully distribute such information or those who illegally gather the information in the first instance.[50] As the mere recipient of information, WikiLeaks falls into neither category.

WikiLeaks provides a mechanism for those in possession of certain material voluntarily to submit it to WikiLeaks for further dissemination:

> Wikileaks will accept restricted or censored material of political, ethical, diplomatic or historical significance.
>
> . . . .
>
> Wikileaks has an anonymous electronic drop box if you wish to provide original material to our journalists. Wikileaks accepts a range of material, but we do not solicit it. If you are going to send in material it should be done as securely as possible. That is why we have created our novel method of submission based on a suite of security technologies designed to provide anonymity. We have put a great deal of technical and design work into the drop box because we take the journalist-source relationship very seriously.[51]

Cries for the prosecution of WikiLeaks invoke the Espionage Act of 1917[52] (Act) as the statutory framework under which such a prosecution should commence.[53] The language and purpose of that Act, however, is the criminal prohibition of traditional spying, primarily through restrictions placed on those who

losing of defense information with the intent or reason to believe it will be used to injure the United States or aid a foreign nation).

48. 18 U.S.C. § 794 (2006).

49. 18 U.S.C. § 798 (2006).

50. *Id.*

51. *Submissions*, WIKILEAKS, http://213.251.145.96/Submissions.html (last visited Mar. 6, 2011).

52. 18 U.S.C. §§ 793–98 (2006).

53. *See, e.g.*, Feinstein, *supra* note 1.

"lawfully" have possession of the information at issue.[54] In other words, criminal prohibitions properly focus upon the government leaker or traditional thief (or spy) rather than the recipient of information.

Within the Act, only section 793(c) criminalizes receipt of documents or other tangible items related to national defense.[55] No successful prosecution of those outside the government is known to exist, and no successful prosecution appears to exist for mere receipt of information.[56] Instead, prosecutions, consistent with the language and primary purpose of the Act, focus on the government leaker, not the recipient.[57] After all, the government leaker is the one with a legal obligation to protect classified information.

When enacting the Act, Congress explicitly rejected language that would have permitted prosecution for mere publication of information and instead focused on traditional acts of spying (i.e. acts intended to harm the Country).[58] On many occasions since, Congress rejected broad prohibitions on any public dissemination of national defense information.[59] "[N]obody other than a spy, saboteur, or other person who would weaken the internal

54. *E.g.*, 18 U.S.C. § 793(d), (f) (2006).

55. Technically, anyone—regardless whether a government agent—may be imprisoned or fined for publishing or otherwise making classified information available to those not authorized to receive it where that information relates to codes, cryptography and communications intelligence. 18 U.S.C. § 798 (2006). That statutory provision, however, covers a very limited type of information and does not apply to all classified information. *See id.*

56. Letter from John Ashcroft, at 9 ("Clearly, that only a single non-espionage case of an unauthorized disclosure of classified information has been prosecuted in over 50 years provides compelling justification that fundamental improvements are necessary and we must entertain new approaches to deter, identify, and punish those who engage in the practice of unauthorized disclosures of classified information.")

57. *See, e.g., id.*

58. *See* Harold Edgar & Benno C. Smith, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 940–41 (1973); *see also* Laura Barandes, *A Helping Hand: Addressing New Implications of the Espionage Act on Freedom of the Press*, 29 CARDOZO L. REV. 371, 383 (2007).

59. *See, e.g.*, S. DOC. NO. 79-244, at 252–531 (1946) (rejecting blanket prohibition on disclosure of classified information); *see also* H.R. REP. NO. 81-1895, at 2 (1950), *reprinted in* 1950 U.S.C.C.A.N. 2297, 2298–99; 108 CONG. REC. 23140-41 (1962).

security of the [n]ation need have any fear of prosecution."[60]

One of the more recent considerations of a broad criminal prohibition on the unauthorized disclosure of all classified information by those within or outside the government occurred in 2000.[61] President Clinton vetoed that legislation, explaining that it would create a "chilling effect on those who engage in legitimate activities . . . . Incurring such risks is unnecessary and inappropriate in a society built on freedom of expression and the consent of the governed and is particularly inadvisable in a context in which the range of classified materials is so extensive."[62] Though debate exists as to whether some interpretation of existing statutes permits broader prosecutions than those undertaken to date, efforts continue to enact more sweeping legislation.[63] But, such proposals generally still focus (or should focus) on the government leaker, not the recipient of information.

This legislative and prosecutorial history makes clear, despite the Act's sometimes potentially broad language, the limited nature of the Act's purpose.[64] However, it does not

60. 95 CONG. REC. 9749 (1949) (statement of Tom C. Clark, Att'y Gen. of the U.S.).

61. Intelligence Authorization Act for Fiscal Year 2001, H.R. 4392, 106th Cong. § 303, (2d Sess. 2000).

62. Message on Returning Without Approval to the House of Representatives: Intelligence Authorization Act for Fiscal Year 2001, 3 PUB. PAPERS 2466, 2466–67 (Nov. 4, 2000).

63. "The time has come for a comprehensive law that will make it easier for the government to prosecute wrongdoers and increase the penalties, which hopefully will act as a deterrent for people thinking about disclosing information." Pete Hoekstra, *Secrets and Leaks: The Costs and Consequences for National Security*, HERITAGE FOUND. (July 29, 2005), http://www.heritage.org/Research/HomelandDefense/wm809.cfm.

64. *See, e.g.*, United States v. Abel, 258 F.2d 485 (2d Cir. 1958) (permitting relatively broad application of the Espionage Act during criminal prosecution); *see also* United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010), *petition for cert. filed* (Mar. 11, 2011). Note also that despite the legislative history's more narrow focus on acts of classic espionage, even the majority of Justices viewed as a possibility the criminal prosecution of even the traditional press in New York Times Co. v. U.S., 403 U.S. 713 (1971). That said, Justice Douglas rejected the argument that the statute's use of the term "communicate" included acts of publication, relying on legislative history suggesting Congress rejected efforts to reach publication rather than communication. *Id.* at 721–22.

provide a clear answer for the WikiLeaks situation, nor could the drafters of this legislation or the drafters of revisions in later years foresee the WikiLeaks media model.

September 11 complicated the handling of information because the attacks resulted in a realization that, even within the government, an insufficient sharing of information existed that created national security risks.[65] Thus, in the decade following those attacks, the government took two potentially adverse actions: increasing the sharing of information within the government (i.e., among various government branches, levels, and agencies)[66] while also increasing the amount of information deemed in need of secrecy and protection.[67] As any child who shares a secret knows, the more people who know your secret, the greater the jeopardy to its secrecy. Yet, as the United States government and its people now know, the failure to share secrets with each other may endanger the country itself.[68] Information must be more widely spread while still protected against general disclosure to the media,[69] including sites like WikiLeaks. This means that the real attention remains on the conduct of those with access to it: government employees.

65. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 79–80, 91–92, 267, 355–56, 416–19 (2004), *available at* http://www.gpoaccess.gov/911/index.html (outlining the "vastly complicated information sharing" occurring prior to the attacks of September 11 and providing recommendations for the improvement of information sharing).

66. *See id.*

67. *See* FED. R. CRIM. P. 6(e)(3)(D)–(F) (as amended by the USA PATRIOT Act providing for sharing of grand jury information); 50 U.S.C. § 1825 (2006); *see also* Scott Shane, *Increase in the Number of Documents Classified by the Government*, N.Y. TIMES (July 3, 2005), www.nytimes.com/2005/07/03/politics/03secrecy.html.

68. *See* THE 9/11 COMMISSION REPORT, *supra* note 65.

69. Much of the public discourse surrounding WikiLeaks attempts to elevate the traditional press by describing the editorial process undertaken by members of that medium before publishing any potentially sensitive government information and the cooperation and communication that often exists between that press and government officials prior to any determination on publication. Though that cooperative process is certainly preferred by government officials over the total lack of cooperation from WikiLeaks, such cooperation is not required and never ensured prevention of the publication of information the government did not want disclosed. *See* Liptak, *supra* note 43; Abrams, *supra* note 44.

## VI. WITH ACCESS COMES RESPONSIBILITY

Less controversial than the access of a litigant—including criminal defendants or the press—to particular information is that where one voluntarily agrees to work for the government in a position in which access to key information exists, the government may impose restrictions upon that individual in terms of disclosure of the information learned.[70] In a government where it is clear that some information may remain secret, it is equally clear that the government may mandate that its agents maintain such secrecy.

The legal obligation of government employees to protect classified information differs from that of the general public or the press.[71] For many in the intelligence community, this legal obligation is spelled out contractually.[72] In those situations, improper disclosure of information may subject those employees not only to criminal sanctions, but also to other legal penalties resulting from breaches of their contracts.[73] Furthermore, unlike government efforts to impose prior restraints on the speech of the general public, when focused on government employees, such efforts survive any First Amendment challenge.[74]

Government employees, particularly those who are provided access to classified information, hold positions of trust.[75] Private Manning was such an individual.[76] Rather than the actions of information recipients like WikiLeaks, actions of those like Private Manning should be the focus of any efforts to maintain the secrecy of information related to national security. In

70. Snepp v. United States, 444 U.S. 507, 507–08 (1980) (per curiam).

71. One obvious issue when seeking to prevent classified information leaks is how to evaluate treatment of intentional leaks (i.e., those authorized by the government without formal declassification of the information leaked). This article does not discuss the issue of intentional leaks, which issue is itself a complicated one worthy of more in-depth, separate discussion.

72. *E.g. Snepp*, 444 U.S. at 508.

73. *Id.*

74. *See*, *e.g.*, *id.*; United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972).

75. *Snepp*, 444 U.S. at 510 ("Snepp's employment with the CIA involved an extremely high degree of trust.").

76. *See* Savage, *supra* note 7.

addition to preventive measures, including but not limited to the threat of criminal sanctions, civil sanctions, or the loss of one's security clearance or employment, questions arise about the motivation for one who improperly discloses classified information.

One claimed potential motivation is over-classification: that so much information is classified that an employee may believe he is acting for the good of the public in disclosing information which he does not believe is properly classified.[77] Though over-classification may indeed be an issue, a review of classification procedures identifies areas where greater attention may be needed to prevent future leaks by better training of employees on the means for questioning the classification status of particular information.[78]

## VII. CLASSIFICATION AND DECLASSIFICATION

Though both Congress and the President play roles in creating and protecting information that could endanger the country's national security, the majority of information likely to impact that security is compiled within the Executive Branch. Thus, the primary classification system for government information rests within that branch.[79] Since 1940, classification procedures exist pursuant to executive order.[80]

Though the first such Roosevelt's executive order invoked statutory authority, the President's authority to establish a procedure for classification exists without such authorization:

> The President, after all, is the "Commander in Chief of the Army and Navy of the United States." U.S. Const., Art. II, § 2.

77. *See generally* Hoekstra, *Secrets and Leaks*, *supra* note 63.

78. Exec. Order No. 13,526 § 1.3, 3 C.F.R. 298, 299–300 (2009).

79. *Id.*

80. President Franklin D. Roosevelt issued the first executive order outlining the means for protecting information regarding military installations. Exec. Order No. 8,381, 3 C.F.R. 117, 117–18 (1940). Prior to that time, military regulations controlled such classification. *See* Harold Relyea, *The Presidency and the People's Right to Know*, *in* THE PRESIDENCY AND INFORMATION POLICY 1, 16–18 (1981). Since Roosevelt, every President other than President Kennedy issued his own executive order governing classification.

> His authority to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant.[81]

Congress may also participate in classification procedures and does so through a number of statutory enactments.[82] For most information, executive orders establish the classification process.[83] As such, classification procedures change with administrations—sometimes only slightly and other times by completely reversing prior policies related to the classification of information.[84]

Current classification procedures exist in Executive Order No. 13,526 issued by President Obama in 2009.[85] As with past executive orders, this Order identifies who may classify information, what may be classified, what levels of classification may be used,[86] who may access information once classified, and how and when information will be declassified.[87]

---

81. *See* Dep't of the Navy v. Egan, 484 U.S. 518, 527 (1988) (citing Cafeteria & Rest. Workers Union v. McElroy, 367 U.S. 886, 890 (1961)).

82. *See, e.g.*, Atomic Energy Act, 42 U.S.C. § 2011 *et seq.* (2006) (creating a separate process for protection of nuclear "Restricted Data"); 50 U.S.C. § 435 *et seq.* (2000) (requiring background checks be performed prior to any person's accessing classified information). Congress formalized the tradition of executive control over classification procedures by defining classified information in a number of statutes as including information designated as such, pursuant to, and among other things, an executive order. *See* 50 U.S.C. § 426(1) (2000); *see also* 18 U.S.C. § 798(b) (2006); 50 U.S.C. § 438(2) (2006).

83. *E.g.*, Exec. Order No. 13,526, 3 C.F.R. 298 (2009).

84. *See* DANIEL PATRICK MOYNIHAN, CHAIRMAN, REPORT OF THE COMM'N ON PROTECTING AND REDUCING GOVERNMENT SECRECY, S. DOC. NO. 105-2, at 11 (1997).

85. Exec. Order No. 13,526, 3 C.F.R. 298 (2009).

86. *Id.* at § 1.2(a), 3 C.F.R. at 298–99. Currently, three levels of classification exist: "Top Secret" for information reasonably expected to cause exceptionally grave damage to national security if disclosed; "Secret" for information reasonably expected to cause serious damage to the national security if disclosed; and "Confidential" for information reasonably expected to cause damage to the national security if disclosed. *Id.*

87. *See infra* note 111.

Those with authority may classify information concerning a number of matters falling within the scope of national security, including the following: military plans, weapons systems, or operations;[88] foreign government information;[89] intelligence activities, sources, methods, or cryptology;[90] foreign relations activities;[91] scientific, technological, or economic matters relating to national security;[92] federal programs for safeguarding nuclear materials or facilities;[93] national security system vulnerabilities or capabilities;[94] or information related to weapons of mass destruction.[95] For the most part, these categories seem appropriate for secrecy and information protection.

Determining when information falls within these categories may be difficult. Over time—after being properly classified—the same information may cease to present any reasonable danger to national security by its disclosure. President Obama's Order embodies a policy against classification in the first instance where significant doubt exists as to the risk posed by disclosure and that policy provides methods for targeted and automatic declassification.[96]

Decisions as to what and how to classify bring questions about how to prevent unnecessary classification. Though the executive orders governing classification all purported to discourage over-classification,[97] those making classification decisions face difficult decisions. Classification is to occur for information that could reasonably be expected to damage national security if disclosed.[98] What constitutes national

88. Exec. Order No. 13,526 § 1.4(a), 3 C.F.R. 298, 300 (2009).
89. *Id.* at § 1.4(b), 3 C.F.R. at 300.
90. *Id.* at § 1.4(c), 3 C.F.R. at 300.
91. *Id.* at § 1.4(d), 3 C.F.R. at 300.
92. *Id.* at § 1.4(e), 3 C.F.R. at 300.
93. *Id.* at § 1.4(f), 3 C.F.R. at 300.
94. *Id.* at § 1.4(g), 3 C.F.R. at 300.
95. *Id.* at § 1.4(h), 3 C.F.R. at 300.
96. *Id.* at § 1.1(b), 3 C.F.R. at 298.
97. For example, the current executive order directs the classifying official, where significant doubt exists about whether to classify, either to leave the information unclassified or to classify it at the lowest appropriate level. *Id.* at § 1.1–1.2, 3 C.F.R. at 298–99.
98. *Id.* at § 1.2, 3 C.F.R. at 298.

security or what constitutes damage is unclear, as neither of these terms is defined. Thus, likely out of necessity, interpretation of the terms is left to individual classifying officials.

In the matter of a former CIA employee's publication of information without prior review by the government as required by contract, the Supreme Court identified another problem inherent in one's independent classification decision making: "When a former agent relies on his own judgment about what information is detrimental, he may reveal information that the CIA—with its broader understanding of what may expose classified information and confidential sources—could have identified as harmful."[99] Classification in error may keep a piece of information from the public, but failure to classify when necessary may directly cost American lives. Thus, it is no surprise that, despite policy instructions to the contrary, classification may be the rule rather than the exception. That situation undoubtedly leads to over-classification.[100]

Over-classification lessens respect for properly classified information. Concerns about over-classification or classification that extends beyond its necessary temporal limit result in the classification system's provision for declassification. Additionally, it is probably through declassification procedures that over-classification is best addressed. In other words, the best system may be one where the concern is not whether information is properly classified in the first instance, but whether a timely and adequate method exists and is being used

99. Snepp v. United States, 444 U.S. 507, 512 (1980) (per curiam).

100. Over the years, accusations exist that classification decisions were made to protect officials from embarrassment or for other improper reasons. Though certainly this author does not contend that such classification never occurs, such classification would be impermissible under the various classification systems established by each President. President Reagan, for example, prohibited classification "to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security." Exec. Order No. 12,356 § 1.6, 3 C.F.R. 166, 170 (1982). The current executive order contains similar prohibitions. Exec. Order No. 13,526 § 1.7, 3 C.F.R. 298, 302–03 (2009).

to review classification decisions.

The classification system also provides—perhaps most importantly for those who posit that government employees may disclose information because it was improperly classified—a process for challenging classification.[101] Where an employee has a "good faith" belief that something should not be classified, the employee is "encouraged and expected" to challenge the classification using this process.[102]

In the interest of limiting classification of information in terms of time of classification, a default timeframe exists for how long information will remain classified.[103] That default generally provides that information remain classified for ten or twenty-five years, depending on the information and absent an affirmative decision by the classifying agency that it be declassified earlier.[104] Moreover, executive-created classification procedures provide for declassification of previously classified information automatically after twenty-five years and through a mandatory declassification review.[105]

Realizing the importance for a declassification process, Congress enacted the Public Interest Declassification Act of 2000.[106] This legislation created the Public Interest Declassification Board, to advise the President and others on issues of declassification.[107] The most recent executive order establishing classification (and declassification) policy also focused on speeding up review of classified information for possible declassification.[108]

Congress most recently passed the Reducing Over-Classification Act in 2010.[109] The purpose of this act is to

101. Exec. Order No. 13,526 § 1.8, 3 C.F.R. 298, 303 (2009).

102. *Id.*

103. *Id.* at § 1.5, 3 C.F.R. at 300–01.

104. *Id.* at § 1.5(b)–(c), 3 C.F.R. 300–01; *see also* Exec. Order No. 13,292 § 1.5, 3 C.F.R. 196, 198–99 (2004) (President Bush's prior order).

105. Exec. Order No. 13,526 §§ 3.3, 3.5, 3 C.F.R. 298, 307–10, 311–12 (2009).

106. Public Interest Declassification Act of 2000, Pub. L. No. 106-567, § 701, 114 Stat. 2856, 2856 (2000) (codified as amended at 50 U.S.C. § 435 (2006)).

107. *Id.* at § 703, 114 Stat. at 2856.

108. *See* Exec. Order No. 13,526 § 1.9, 3 C.F.R. 298, 303–04 (2009).

109. H.R. 553, 111th Cong. (2d Sess. 2010).

"prevent federal departments and agencies from unnecessarily classifying information or classifying information at a higher and more restricted level than is warranted, and by doing so to promote information sharing across departments and agencies and with State, local, tribal and private sector counterparts, as appropriate."[110]

To these ends, the statute also authorizes the inspectors general of the various agencies to conduct assessments of whether their agencies are complying with current policies on classification.[111] Declassification is a slow process[112] and does not directly reach the issue of what to do once information that is still classified is improperly disclosed.

## VIII. KEEPING THE CAT IN THE BAG: WHERE DO WE GO FROM HERE?

The government can create contractual obligations and provide employment to encourage obligations of secrecy, while the law—specifically the Executive Branch's classification system—can create other legal obligations. However, once publicly disclosed, protecting the information is no longer the primary concern. Instead, the way in which the government reacts to a particular leak may do as much harm as good in protecting national security.

110. S. COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, REDUCING OVERCLASSIFICATION ACT, S. REP. NO. 111–200, at 1 (2d Sess.).

111. Pub. L. No. 111-258 § 6(b) (2010).

112. President Obama directed the National Declassification Center (NDC) to review all classified records more than twenty-five years old, more than 400 million pages. Memorandum on Implementation of the Executive Order, "Classified National Security Information", 75 Fed. Reg. 733 (Dec. 29, 2009). The NDC was to work with the various agencies to review these documents and determine whether they should remain classified. *Id.* The agencies, however, are classifying new documents and information at a faster rate than declassification is occurring—NDC estimates for every 11 million pages that go through the declassification process each year, 15 million new pages reach the National Archives and Records Administration, where the agencies send classified documents reaching this age for declassification review. Sheryl J. Shenberger, Director, National Declassification Center, *The National Declassification Center*, at 12.

Again, childhood playground rules are apropos. So much of what is done by bullies or others whose goals may be less than honorable is to embarrass and harass (i.e., to get a reaction and gain control).[113] The greater the reaction from the person or entity from whom or about whom the information is, the more information likely will be noted and disseminated.[114]

The goal should be for the government to react quickly and effectively. First and foremost, investigation into the source of the leak must ensue. Once identified and sufficient evidence is obtained, criminal prosecution—or, where more appropriate, civil sanctions or employment termination—should begin against any and all government leakers. However, this type of deterrence is not the first line of attack.

The ultimate goal is to prevent the leak in the first place. Ways to account for proper classification, proper information sharing (also crucial for national security), and proper declassification are numerous; no one solution will be perfect. Thus, to function at their peaks, these policies must be clear, concise, consistent, and known throughout government. Ensuring training of employees on these procedures, including how to challenge classification internally where one believes information is being kept secret from the public without justification, can only help avoid a government employee's perceived need to leak the information externally.

Tighter control over access to information once classified could also aid in preventing leaks. Not only does more restricted control of access—not necessarily more restricted access—limit the number of people with information and, thus, the number of potential leakers, but it also aids in identifying the source of any leaks.

Finally, a clear post-leak protocol wherein each agency and employee understands what to do and what will be done in the

113. *Tips for Dealing with Bullies for Students, Teachers, and Kids*, THE FREE RESOURCE, http://www.thefreeresource.com/tips-for-dealing-with-bullies-resources-about-bullying.

114. DAN OLWEUS, BULLYING AT SCHOOL: WHAT WE KNOW ABOUT BULLYING 35 (1933); *see also* KIDSHEALTH, http://kidshealth.org/kid/feeling/emotion/bullies.html.

event of a leak may provide a deterrent effect earlier in the chain of events than formal criminal prosecution.

No solution will guarantee a leak-free government, nor does a solution exist that can guarantee against over-classification. The gathering, analyzing, and maintaining of information is a delicate business. It requires balancing the need for information, which need requires the trust of the sources of information, with the need to share information at times with the public and at times with other levels of governments or other nations. Moreover, any policy controlling access to information must balance any restriction to that information against the benefits gained by an open government where information is available to the public to inform its policy and voting preferences.

Ultimately, WikiLeaks is not the problem. The Internet now permits the instant transfer of information around the world by anyone to everyone. With advanced technology comes a need for new considerations when drafting policies on how to handle information that is so easily and instantly communicated. And, most important is perhaps ensuring full understanding of such policies by those who must actually put them to work.